11:11 Systems Service Schedule

The terms and conditions set out in this 11:11 Systems Service Schedule (this "Schedule") shall apply to each Service Order executed by the Provider and the Customer (each, a "Order"), and shall be deemed to be incorporated, the necessary changes having been made, into each Order.

1. Section 1: Definitions

In this Schedule: Any capitalized terms used but not defined in this Schedule or the remainder of the Agreement shall have the meanings set out in the relevant Order.

1. "11:11 Autopilot Managed Recovery for DRaaS" shall refer to a managed service offering provided by the Provider to the Customer for the purpose of managing the on-boarding, technical design, testing and operational support elements of an 11:11 Secure DRaaS for Zerto, 11:11 Secure DRaaS for Veeam, or 11:11 DRaaS for Cohesity service contract.
2. "11:11 Cloud" shall refer to an environment that contains the Provider's basic cloud infrastructure features without any level of encryption or security attributes integrated into the environment and its underlying storage and/or shared Cloud Resources. Features associated with 11:11 Cloud environment are only available to Customers that elect to have those services provided to them on their Order.
3. "11:11 Cloud Console" or "Cloud Console" shall refer to the cloud-based management portal in which the Customer accesses and administers the Services.
4. "11:11 Cloud Object Storage" shall mean the public Internet service delivered by the Provider that allows the Customer to store and manage data as objects, as opposed to other storage architectures like file systems and block storage. Features associated with 11:11 Cloud Object Storage environment are only available to Customers that elect to have those services provided to them on their Order.
5. "11:11 Co-Managed Firewall" shall refer to the service that allows the Customer the ability to make configuration changes to supported firewall devices while the Provider provides monitoring, support, and visibility in accordance with the selected Basic and Advanced Managed Appliance service level.
6. "11:11 DRaaS for Zerto" shall refer to an environment that contains the Provider's basic cloud infrastructure features without any level of encryption or security attributes integrated into the environment and its underlying storage and/or shared Cloud Resources. Features associated with 11:11 DRaaS for Zerto environment are only available to Customers that elect to have those services provided to them on their Order.
7. "11:11 DRaaS for Zerto Cloud-to-Cloud" shall refer to a DRaaS environment where both the Primary Site and Recovery Site are in two (2) different Provider's physical locations as specified in the Order. Features associated with 11:11 DRaaS for Zerto Cloud-to-Cloud environment are only available to Customers that elect to have those services provided to them on their Order.
8. "11:11 Managed Migration" shall mean the Provider's process and service that assists the Customer with the migration of Virtual Machines and/or Physical Servers

from the Customer’s Primary Site into a Provider’s Virtual Data Center, and the connectivity setup and configuration that it entails.

9. “11:11 Secure Cloud” shall refer to an environment that contains the Provider’s advanced security and encryption features and attributes integrated into the environment and its underlying storage and shared Cloud Resources. Features associated with 11:11 Secure Cloud environment are only available to Customers that elect to have those services provided to them on their Order.

10. “11:11 Secure Cloud Backup for Veeam Cloud Connect” shall mean the public Internet service delivered by the Provider that allows the Customer to backup Machine’s virtualized data into Cloud Resources. Features associated with 11:11 Secure Cloud Backup environment are only available to Customers that elect to have those services provided to them on their Order.

11. "11:11 Secure DRaaS for Veeam" shall refer to an environment where the Customer uses Veeam Cloud Connect software to replicate from the Primary Site to the Provider's Recovery Site and its underlying storage and shared Cloud Resources. Features associated with 11:11 Secure DRaaS for Veeam environment are only available to Customers that elect to have those services provided to them on the Order.

12. “11:11 Secure DRaaS for Zerto” shall refer to an environment that contains the Provider’s advanced security and encryption features and attributes integrated into the environment and its underlying storage and shared Cloud Resources. Features associated with 11:11 Secure DRaaS for Zerto environment are only available to Customers that elect to have those services provided to them on their Order.

13. “11:11 Secure Private Cloud” shall refer to an environment that contains the Provider’s advanced security and encryption features and attributes integrated into the environment and its underlying storage and dedicated Cloud Resources. Features associated with 11:11 Secure Cloud environment are only available to Customers that elect to have those services provided to them on their Order.

14. “11:11 Secure Private DRaaS for Zerto” shall refer to an environment that contains the Provider’s advanced security and encryption features and attributes integrated into the environment and its underlying storage and dedicated Cloud Resources. Features associated with 11:11 Secure Private DRaaS for Zerto environment are only available to Customers that elect to have those services provided to them on their Order.

15. “11:11 Support” shall refer to the Provider’s technical support department, which acts as the primary contact for all Customer’s requests for help and assistance once the initial deployment has been completed.

16. “Accelerated Storage” shall mean encrypted storage resources provided on a blend of traditional shelves of disks and flash storage.

17. "Acceptable Use Policy" or "AUP" shall mean the Provider's document that stipulates constraints and practices that the Customer must adhere to when utilizing any of the Provider's Services. The current AUP can be accessed

at https://1111systems.com/legal/acceptable-use-policy/ provided, however, that the AUP may be modified from time to time at the Provider's sole discretion.

18. “Account Management Application” is the primary resource for Customers to access and manage information including, but not limited to, account profile, contact management, contracts, service and maintenance status of services and regions, and support tickets.
19. “Active Virtual Machine” shall mean a Virtual Machine that is turned on within the Virtual Data Center.
20. “Advanced Storage” shall mean storage resources provided on traditional shelves of disks.
21. “Appliance” shall mean a physical or virtual device or equipment designed to perform a specific IT task.
22. “Archive Storage” shall mean storage resources provided on traditional shelves of disks.
23. “Availability Zone” shall mean one or more AWS discrete Data Centers with redundant power, networking, and connectivity in an AWS region. Availability Zones are physically separated by a meaningful distance, many kilometers, from any other Availability Zone, although all are within 100 km (60 miles) of each other, and are designed to handle concurrent device failures by quickly detecting and repairing any lost redundancy, and they also regularly verify the integrity of your data using checksums.
24. “Backup Groups” shall mean the groups of Virtual Machines defined in Advanced Backups. These groups define what Virtual Machines are backed up and how they are backed up by the applied Backup Policy.
25. “Backup Policies” shall mean the policies that define the Advanced Backup schedule of how often and when to take a backup and the retention timeframe for that backup. The policies also define how often full backups should be taken and how often to retry in the event of backup failure.
26. “Backup Testing” shall mean the operational mode in which the data of the Machines are validated leveraging Target Site restore points during a predetermined process. “Tested Backup” shall have a correlative meaning.
27. "Bare Metal Device" shall mean a physical computer system without a base operating system (OS) or installed applications. It is a computer's hardware assembly, comprised of structure and components, that is installed with either the firmware or basic input/output system (BIOS) software utility or no software at all. The Provider service includes the colocation of this device, but no OS.
28. "Broadcom White Label Program" shall refer to the licensing and resell framework established by Broadcom under the VMware Cloud Service provider (VCSP) program, enabling authorized partners to resell VMware Cloud Foundation licenses and related add-ons.

29. “Brownfield” shall mean an IT environment or deployment where the design, installation, and configuration is an upgrade or addition to an existing infrastructure using legacy components.
30. “Burst Resources” shall mean Cloud Resources that are not dedicated to the Customer but which, if available, the Customer may use to exceed its committed Reserved Resources. These are billed in arrears and are calculated by multiplying a usage over the Reserved Resources by the monthly or hourly burst rate as specified in the Order.
31. “Carrier” shall mean an organization that provides services accessing and using the Internet or any other telecommunications service that operates on its proprietary network infrastructure.
32. “CASB” shall mean Cloud Access Security Broker.
33. “CDN” shall mean Content Delivery Network.
34. “Change Management” shall mean making controlled and informed changes to the operation and functionality of an eligible service or Equipment provided by the Provider.
35. “Cloud Resources” shall mean compute (CPU), memory (RAM), storage, IP address and network bandwidth that comprises a Virtual Data Center as described in the Order.
36. “Cloud Storage” shall mean storage resources within the Target Site, provided on traditional shelves of disk, accessed from the Machines.
37. “Colocation” shall mean the Provider's service related to placing and maintaining the Customer's Equipment within the same Data Center where the Provider hosts its Cloud Resources.
38. “Colocation Area” shall mean the area within the Data Center in which the Colocation Rack Space is located.
39. “Colocation Rack Space” shall mean the physical space within a rack or other location(s) within the Colocation Area of the Data Center designated by the Provider for the Customer to colocate the Equipment.
40. “Colocation Specifications” shall have the meaning set out in the relevant Colocation Order or, if no such definition is set out in the Colocation Order, the Provider's standard specifications for colocation space in the Colocation Area.
41. “Commencement Notification” shall mean an email communication from the Provider to the Customer indicating the formal hand-off of Cloud Resources and the commencement of billing under the Order.
42. “Connectivity Services” shall mean, collectively, Dark Fiber, Lit Services, Managed Firewall, SD-WAN, and Managed Connectivity.
43. “Cross Connects” shall mean physical cables that allow direct connections between two different termination locations within a Data Center.

44. “Customer-Owned Telecommunications Circuit” shall mean a telecommunications circuit contracted by Customer with a third-party telecommunications provider.
45. “Customer Premises Equipment” or “CPE” shall mean any Equipment owned and/or used by Customer, including Provider-Supplied Equipment, that is used to connect to the Services.
46. “Customer-Provided Equipment” shall mean any equipment owned by the Customer and listed in the Hybrid Colocation Order as equipment that may be colocated in the Colocation Rack from time to time.
47. “Dark Fiber” shall mean all connectivity circuits with dark optical fiber strands in a particular network configuration supplied by Provider to Customer pursuant to an Order.
48. “Dark Fiber Specifications” shall mean those specifications set forth in section 3.33.5 below.
49. “Data Center” or "Datacenter" shall mean the facility operated by the Provider designated as the Datacenter in the relevant Order.
50. “Data Seeding” or “Seed Data” shall mean the process of exporting Virtual Machine data to removable media at the Primary Site and/or Source Site, shipping the removable media to Recovery Site and/or Target Site and importing Virtual Machine data into a Virtual Data Center at Recovery Site and/or Target Site.
51. “DDoS” shall mean Distributed Denial of Service.
52. "Dedicated Resources" shall mean Cloud Resources dedicated to a single tenant or Customer.
53. “Demarcation Point” shall mean the point located in the Data Center at which the extension from the Carrier infrastructure ends and connects with the Provider’s on-premises wiring, where Provider hands off the Connectivity Services to Customer;
54. “Deployment” shall mean the period beginning once the Provider has acknowledged receipt of the signed Order and ending when the Provider satisfies all deliverables within the initial scope.
55. “Deployment Engineer” shall refer to an engineer, who is an employee of the Provider with technical knowledge and training of use and best practices of the Provider’s services, that is responsible for deploying the environment in the Provider’s infrastructure used by the Customer.
56. “Disaster” shall mean the Customer’s inability to send or receive data at the Primary Site due to unavailable compute, storage, or network resources.
57. “Disaster Recovery Runbook” shall mean a collection of Recovery Groups that are combined into a single list to simplify management of the DRaaS environment when testing failover, or in the case of performing a live failover of the environment.
58. “DLP” shall mean Data Loss Prevention.
59. “DNS” shall mean Domain Name Services.

60. “DRaaS” shall mean Disaster Recovery as-a-Service.

61. “DRaaS Testing” shall mean the operational mode in which the functions of the Virtual Machines in the Primary Site are validated on the Virtual Machines in the Recovery Site. Testing is a non-service impacting event and does not include modification of Primary Site resources including Virtual Machines and networking. “Tested” shall have a correlative meaning. Testing is a fully autonomous function and can be triggered by the Customer at any time.

62. “Electricity Fee” shall mean the amount to be charged by the Provider to the Customer based upon the Customer's usage of electricity in the Colocation Area during the relevant period and the then-current standard prices charged by the Provider to its Customers for electricity, which shall be calculated on a breakered-amp-load basis, and which shall be subject to increase from time to time if the power utility or primary electricity vendor used by the Provider increases the price paid by the Provider for power provided to the Colocation Rack.

63. “Emergency” shall mean an urgent, sudden, and serious event that requires immediate action to remedy the situation.

64. "Equipment" shall mean physical computer, network and/or communications devices.

65. “Failback” shall mean the return of operational mode of the Virtual Machines in the Recovery Site back to the Virtual Machines in the Primary Site after originally becoming unavailable through either failure or scheduled downtime.

66. “Failover” shall mean the backup operational mode in which the functions of the Virtual Machines in the Primary Site are assumed by the Virtual Machines in the Recovery Site due to the Virtual Machines in the Primary Site becoming unavailable through either failure or scheduled downtime.

67. “Greenfield” shall mean an IT environment where the design, installation, and configuration is totally new and requires development from a clean state.

68. “GSS” shall mean Broadcom Global Support Services which provide additional support services for VMware license providers.

69. “ICMP” shall mean Internet Control Message Protocol, more commonly known as ping.

70. “Image-based Backup” shall mean a point-in-time copy of a defined collection of data.

71. “Insider Protection” shall mean the optional feature for the 11:11 Cloud Backup for Veeam Cloud Connect service delivered by the Provider that provides an off-repository storage folder into which all deleted files will be retained for a short time allowing for the restoration of those files by the Provider based on the Customer’s request. The length of time these files are stored is set in the Order.

72. “IOPS” shall mean Input/Output Operations Per Second and is a common performance measurement used to benchmark computer storage devices.

73. “i-Tech” or “iTech” shall refer to the Provider’s i-Tech Services Schedule where services, fees, and rates are defined for when remote, on-site, and/or Telco carrier support is required that was not part of the original scope on an Order. It can be accessed at https://1111systems.com/i-tech-services-schedule

74. “Letter of Authorization” or “LOA” is a document from the Customer or Carrier authorizing the Provider to act on their behalf.

75. “Lit Services” shall mean the services provided by Provider to Customer to enable the transmission of data using one of the following methods as indicated on an Order:

a. Domestic optical (lit) Wavelength and Ethernet Private Line (“EPL”) connectivity circuits—these services are a point-to-point, dedicated electrical or optical data transmission that provides a fixed capacity of bandwidth between two (2) points, specified by the Customer, for the transport of Customer’s digital communications traffic over a physical circuit;

b. Ethernet Private LAN (“EPLAN”) connectivity circuit, Multi-Cloud Connect, Layer 3 VPN (L3VPN) — these services are dedicated electrical or optical data transmission that provides a fixed capacity of bandwidth between two (2) or more points, specified by the Customer, for transporting the Customer’s digital communications traffic over a physical circuit;

c. Domestic Direct Internet Access — this connectivity circuit provide the Customer with connectivity to the Internet, including routing services based upon the Internet Protocol, and are typically comprised of a network Internet Port at a Provider provided POP, and a dedicated network connection between 11:11 Systems POP and the Customer location (these services do not include Internet Over Broadband or Internet Over Wireless);

d. Internet Over Broadband (Broadband) — these connectivity circuits provide the Customer with connectivity to the Internet and include:

i.Digital Subscriber Line (“DSL”),

ii.Ethernet Over Copper (“EOC”),

iii.Internet Over Broadband (“IOB”),

iv.Internet Over Cable (“IOC”),

v.Internet Over Fiber (“IOF”),

vi.Internet Over Wireless (“IOW”),

vii.Internet Over Fixed Wireless (“IOFW”), and

viii.Internet Over Satellite (“IOS”);

e. AWS Direct Connect (AWS DX) On-ramp — this connectivity is between a Provider POP and AWS Direct Connect on-ramp, offered in a 50 Mbps – 5 Gbps hosted connection, or a 1 Gbps or 10 Gbps dedicated direct connect connection.

i. An AWS Direct Connect Dedicated On-ramp connection is a physical network port that allows customers to establish a dedicated and private network connection between the Customer’s on-premises networks and the AWS cloud, and

ii. An AWS Direct Connect Hosted On-ramp connection allows Customers to establish a network connection between their on-premises networks and the AWS cloud on a shared Provider port. Unlike a Direct Connect dedicated port, which requires Customers to manage the physical network port themselves, a Hosted Connection simplifies the process by allowing Customers to connect to AWS using connectivity provided and managed by the Provider; and

f. IP Bandwidth – This connectivity service provides the Customer with connectivity to the internet via diverse upstream internet peering providers.

g. Fabric Connect - This connectivity service provides the Customer with layer 2 or layer 3 connectivity between the source and destination locations specified in the Order.

h. Fabric Multi-Service Connect – This connectivity service provides the Customer with layer 2 or layer 3 full mesh connectivity between all Multi-Service Connect source locations specified in the Order.

i. Colo Multi-Service Connect – This connectivity service provides the Customer with a single-mode cross connect and network port on Provider's infrastructure.

76. "Local Monitoring Probe" shall mean an Appliance deployed within a specific Customer's location, such as an on-premises facility or a remote site, whose primary purpose is to collect, analyze, and report data on the performance and health of the local network or systems.

77. "LUR" shall mean License Usage Report, which is provided in conjunction with Broadcom's Usage Meter.

78. "Machine" shall mean the computing equipment on which the Customer is running the Veeam Cloud Connect software and the computing equipment used by the Customer to access the Cloud Resources (but excluding the Cloud Resources).

79. "Managed Security Portal" shall mean the site that is accessed as part of the Continuous Risk Scanning offering providing the customer visibility into the vulnerabilities within their environment, which can be accessed at https://assess.grncld.com/

80. "Microsoft 365" shall mean a Microsoft 365 end-user account that, because it is being backed up using the Provider's services, requires an 11:11 Secure Cloud Backup for Microsoft 365 license. A Microsoft 365 user account can use one or many applications such as Exchange Online, OneDrive for Business, SharePoint Online, and Microsoft Teams.

81. "Microsoft SPLA" shall refer to the licensing provided under the Microsoft Service Provider Licensing agreement.

82. "mTLS" shall mean mutual transport layer security.

83. "Network Support" shall mean the Provider's process and service that assists the Customer with the initial implementation and ongoing support of Customer's virtual network appliances and their configurations.

84. "NGFW" shall mean a next-generation firewall, which is a security appliance that uses context-aware features to process network traffic and applies rules to protect against modern cyber threats.

85. “NOC” or “Network Operation Center” shall mean a centralized function within the Provider’s organization composed of people, processes, and technologies that continuously shall mean any Connectivity Service designated as having redundancy of route and facilities and power and card protection. In the event of an equipment failure or a fiber cut, the service will automatically be re-routed to a “protected” path. Customer hand-off protection is limited to Connectivity Services delivered over a four (4) fiber hand-off connection.

86. “Object Storage Access Credentials” are comprised by a pair of text strings (Key and Secret) used in an 11:11 Cloud Object Storage environment that the Customer generates through the 11:11 Cloud Console.

87. "Offsite Backup" shall mean an archive copy of computer data stored at another remote Data Center different to the one where the source of that data resides.

88. “On-boarding Provisioning Form” shall mean a document used by the Provider for information gathering and collection of all Customer specific technical and infrastructure related details for the sole purpose of the Provider providing the on-boarding service, integration, and management services to the Customer as part of an 11:11 Secure DRaaS for Zerto or 11:11 Secure DRaaS for Veeam service contract.

89. "Onsite Backup" shall mean an archive copy of computer data stored at the same Data Center location where the source of that data resides.

90. "OSI Model" shall mean Open Systems Interconnection model.

91. “Playbook” shall mean a set of configured instructions within the Managed Endpoint Detection and Response (EDR) service that outlines the automated steps taken following a specific alert condition.

92. “Primary Site” shall mean the Customer’s physical location in which the Customer’s Virtual Machines function in normal, non-Failover scenarios in a DRaaS environment.

93. “Product Compatibility Matrix” shall identify the requirements that the Customer's systems and software must meet in order for them to be compatible with the Provider's offerings. The Customer can access the Matrix by accessing our Success Center at https://success.1111systems.com/.

94. “Provider-Supplied Equipment” shall mean any equipment or licenses that the Customer obtains from the Provider for the Customer’s exclusive use and control.

95. “RBI” shall mean Remote Browser Isolation.

96. "Recovery Group" shall mean one or more Virtual Machines grouped together for replication purposes.

97. “Recovery Plan” shall mean the detailed steps involved in how a Customer’s Virtual Machines will be recovered into the Provider’s Recovery Site.

98. “Recovery Point Objective” or “RPO” shall mean the maximum acceptable amount of data loss, measured in time, between the last point-in-time that IT services (applications and data) can be restored to during a Disaster.

99. “Recovery Site” shall mean the Provider’s physical location as specified in the Order to which the Virtual Machines located in the Primary Site will be replicated.

100. “Recovery Time Objective” or “RTO” shall mean the maximum desired length of time allowed between an unexpected failure or Disaster and the recovery of the IT services (applications and data).

101. “Replica Seeding” or “Seed Replica” shall mean the process of exporting Virtual Machine data from an 11:11 Secure Cloud Backup Target Site repository and importing Virtual Machine data into a Virtual Data Center at Recovery Site and in the same Data Center location.

102. “Reserved Resources” shall mean Cloud Resources that are dedicated to the Customer.

103. “RMA” shall mean Return Merchandise Authorization, which is a form of approval issued to Customers who have requested to return or exchange an appliance after experiencing a failure and validated by the Provider.

104. “SD-WAN” or “Software-Defined Wide Area Network” shall mean a virtual WAN architecture that allows communication between networks over the Internet using software-defined technology and encryption.

105. “Shared Resources” shall mean a pool of Cloud Resources shared across multiple Customers in a multi-tenant environment.

106. “Site Environmental Specifications” shall mean the requisite space, racks, power, security and other facilities and other environmental conditions necessary to support and operate the Provider Network and telemetry to support out of band management. Unless specified in the Order, Customer shall be responsible for providing the conditions set forth above.

107. “SNMP” shall mean Simple Network Management Protocol.

108. “SOC” or “Security Operation Center” shall mean a centralized function within the Provider’s organization composed of people, processes, and technologies that continuously monitor and improve the Customer’s security posture by detecting, analyzing, and responding to cybersecurity incidents.

109. “Source Site” shall mean the Customer’s physical location from which the Customer’s Virtual Machines will be backed up in an 11:11 Secure Cloud Backup environment.

110. “SSD Storage” shall mean storage resources provided on Solid State disks.

111. “Statement of Work” or “SOW” shall mean a document defining the project specific activities, requirements, considerations, deliverables and timelines between the Customer and the Provider, in conjunction with the specifications of the relevant Order.

112. “Success Center” shall refer to the digital site provided by the Provider that consists of a knowledge base that contains product documentation, user guides, and technical articles related to the Provider’s portfolio of services located at https://success.1111systems.com/.

113. “Target Site” shall mean the Provider’s physical location as specified in the Order to which the Machines will be backed up in an 11:11 Secure Cloud Backup environment.

114. "Tunnel” shall mean an encrypted tunnel between an origin server and Cloudflare’s nearest Data Center.

115. “UM” or “Usage Meter” shall mean Broadcom’s Usage Meter, which is a virtual appliance provided by Broadcom used to monitor VMware software usage and report license usage back to Broadcom.

116. “Unified Threat Management” or “UTM” is an information security term that refers to a single hardware or software installation that provides multiple security functions at a single point on the network.

117. “Users Authorized to Declare Disasters” shall mean users defined on the Customer Contact form which have the Customer’s authorization to declare a Disaster. If Cloud Resources are available at the time-of-Disaster, the Customer pre-authorizes Users Authorized to Declare Disasters the option to expand its Reserved Resources up to the Disaster Resource Limit specified in the Order. These resources are billed on a monthly basis with a minimum of one-month commitment. The Customer’s Resource Burst Limit will not be modified. At the end-of-Disaster, the Customer has the option to revert to the original Reserved Resource quantity.

118. “vApp” shall mean a collection of pre-configured Virtual Machines that combine applications with the operating systems that they require allowing them to work together in a stack as an application.

119. “VCF" or "VMware Cloud Foundation" shall mean VMware Cloud Foundation software by Broadcom.

120. “Virtual Data Center” shall mean self-contained infrastructure including, compute, memory, and storage that is pooled, aggregated, virtualized, and delivered as-a-service.

121. “Virtual Machine” or '"VM" shall mean a guest operating system such as Windows or Linux that can run or be stored as an isolated entity on a host and is separated from the physical resources it uses such that the host environment is able to dynamically assign those resources among several Virtual Machines.

122. “VMWaaS” shall mean VMware as a Service wherein the Provider manages the VMware layer on a Bare Metal cluster.

123. “vSAN” shall mean Virtual SAN (Storage Area Network).

124. “WAF” shall mean Web Application Firewall.

125. “WARP” shall mean the Cloudflare WARP client.

126. “Workload” shall mean a logical Virtual Machine or physical server instance used for the purposes of hosting one or more applications and / or data set instances.

127. "Zerto Journal" or "Journal" shall mean the collection of replicated data and checkpoints defined as part of the Virtual Protection Group (VPG) configuration. The Journal lives in the Recovery Site and it determines the maximum amount of history, in hours or days, that can be saved and leveraged during a failover event.

128. "Zone" shall mean a unique apex domain such as example.com.

2. Section 2: Universal Service Terms (Applicable to All Services)

    1. **Service Commencement Date.** For all the Provider's Services, the Service Commencement Date of services shall be defined on the applicable Order.

    2. **Provider's Obligations.** The Provider is responsible for the following in accordance with industry best practices:

        1. Providing 24x7x365 global technical support via our different contact methods located at https://1111systems.com/support/contact-support/ or via our Account Management Application. The technical ticket response SLOs are available at https://1111systems.com/legal/sla.

        2. Testing and placing into production any software updates on the Provider's systems in relation to the third-party software on the Provider's then-current Product Compatibility Matrix, which is updated from time to time to reflect new software updates that have been placed into production. The Provider shall not be liable to the Customer and the Customer can neither cancel nor withhold payment for an Order outside of the requirements set forth in the Master Service Agreement, Service Schedule, or Order if the Customer's systems or software were not compatible with this Matrix prior to the commencement of an Order or if the Customer installs a software update before that update is reflected in the Provider's then-current Product Compatibility Matrix. In addition, while the Provider may test third-party software updates before listing them on the Provider's then-current Product Compatibility Matrix, those tests are solely designed to ensure that the third-party software updates will not have a negative effect on the Provider's ability to provide agreed upon services to the Customer and the Provider presents those updates listed as being compatible "as is" with no warranties of any kind, express or implied, including, but not limited to, warranties for fitness of purpose in regard to the third-party software.

    3. **Customer's Obligations.** The Customer is responsible for the following in accordance with industry best practices:

        1. Supplying the Provider with information reasonably required to fulfill its obligations;

        2. Promptly notifying the Provider if the Cloud Resources are compromised, accessed by a person lacking permission to access the Cloud Resources, or infected with a virus, worm or similar malicious code;

        3. Reviewing the Provider's then-current Product Compatibility Matrix before procuring the Provider's services and before installing any software updates in order to ensure that the Customer's systems are compatible with the

Provider's system. The Provider shall not be liable to the Customer and the Customer can neither cancel nor withhold payment for an Order outside of the requirements set forth in the Master Service Agreement, Service Schedule, or Order if the Customer's systems or software were not compatible with this Matrix prior to the commencement of an Order or if the Customer installs a software update before that update is reflected in the Provider's then-current Product Compatibility Matrix. In addition, while the Provider may test third-party software updates before listing them on the Provider's then-current Product Compatibility Matrix, those tests are solely designed to ensure that the third-party software updates will not have a negative effect on the Provider's ability to provide agreed upon services to the Customer and the Provider presents those updates listed as being compatible "as is" with no warranties of any kind, express or implied, including, but not limited to, warranties for fitness of purpose in regard to the third-party software;

4. Configure the appropriate organization access including the creation, modification, and deletion of end-user 11:11 Cloud Console account(s).

5. If the Customer is providing operating system or application licenses:

    1. If used in conjunction with the Services, Customer is solely responsible for compliance with the applicable license terms. At any time during the term of an Order, Provider may request Customer to provide proof of software assurance for the licenses or subscriptions deployed on Provider's hardware;

    2. Adhering to the relevant software vendor's licensing agreements, as well as the Microsoft Licensing Policy stated at https://microsoft.com/licensing/spur, as applicable;

    3. Implicitly consenting to the transferring of limited Customer data (i.e. such as Customer contact information) by the Provider to third-party licensors providing licenses to the Customer for the purpose of verifying and monitoring compliance and usage with the terms associated with those licenses, and

    4. Maintaining, updating, and keeping current license information (as interruption of services may result if such licenses are not maintained). This includes ensuring that the quantity and type of licenses do not exceed the Customer-provided licenses. If the Provider determines (in its sole discretion) that the Customer has exceeded the Customer-provided quantity of licenses, the Provider will (1) notify the Customer of such usage, (2) advise the Customer to upgrade its Order in order to reflect the additional license usage, and (3) invoice the Customer for the costs associated with the additional license usage during the corresponding period. If the Provider advises the Customer to upgrade its Order in the preceding sentence and the Customer does not upgrade its Order within 30 days after receiving that notice, the Provider reserves the right to

unilaterally increase the number of licenses on the Customer Order in order to true up the licensed endpoints. The Customer agrees to pay any invoices or charges for any additional licenses or back charges allowed under this Section;

5. Building Virtual Machine templates using Customer-provided operating system licenses;

6. Not utilizing Microsoft operating system original equipment manufacturer (OEM) licenses as they are not allowed; and

7. Adhering to the Provider's then-current Acceptable Use Policy as defined in the Definitions Section 1 at all times.

6. If the Customer is consuming Provider-supplied licenses:

    1. Such software is subject to the terms of a separate license from the applicable Third-Party software vendor. Customer will comply with all such applicable license agreements as well as the Microsoft Licensing Policy stated at https://microsoft.com/licensing/spur, as applicable;

    2. Implicitly consenting to the transferring of limited Customer data (i.e. such as Customer contact information) by the Provider to third-party licensors providing licenses to the Customer for the purpose of verifying and monitoring compliance and usage with the terms associated with those licenses;

    3. Maintaining, updating and keeping current license information (as interruption of services may result if such licenses are not maintained). This includes ensuring that the quantity and type of licenses do not exceed the contracted amount as described in the Order. If the Provider determines (in its sole discretion) that the Customer has exceeded the contracted quantity of licenses, the Provider will (1) notify the Customer of such usage, (2) advise the Customer to upgrade its Order in order to reflect the additional license usage, and (3) invoice the Customer for the costs associated with the additional license usage during the corresponding period. If the Provider advises the Customer to upgrade its Order in the preceding sentence and the Customer does not upgrade its Order within 30 days after receiving that notice, the Provider reserves the right to unilaterally increase the number of licenses on the Customer Order in order to true up the licensed endpoints. The Customer agrees to pay any invoices or charges for any additional licenses or back charges allowed under this Section; and

7. If both 2.3.5 and 2.3.6 above, if Provider is audited by the Third-Party vendor or owner of such software, then in addition to Provider's rights under the Agreement, Provider will promptly notify Customer and Customer agrees to participate in such audit, at its own expense, and to provide all reasonably requested information to Provider in a complete and timely manner. If

Customer does not comply with the foregoing, without limited any other remedy available to Provider, Provider will have the right to terminate the applicable the Services and/or revoke Customer's license(s) immediately upon written notice to Customer.

8. Resource additions via Console. The Customer acknowledges and agrees that any additions, modifications, or adjustments to the Services or resources made by or on behalf of the Customer through the Console, whether or not such actions result in a formal contract amendment, shall be deemed authorized by the Customer. The Customer shall be fully responsible for all associated fees, obligations, and usage relating to such actions. All resource additions or changes made via the Console shall be governed by, and subject to, the same terms and conditions as set forth in the original Order, including pricing, billing periods, and usage restrictions, unless otherwise expressly agreed by the parties in writing.

4. **Customer Data.**

    1. By purchasing the Provider's Services, the Customer acknowledges that the Provider could potentially be exposed to Customer data which shall not be utilized by the Provider for any purpose other than the purpose of carrying out the Provider's Obligations specified under Sections 2 and 3 of this Service Schedule. By purchasing Provider Services, the Customer expressly acknowledges that it understands and accepts this possibility and the Customer further agrees to not hold the Provider liable in the event that such an exposure occurs.

    2. After the signing of an Order, the Customer and the Provider may mutually agree to move or redirect the Customer's data from the Data Center identified on an Order to a different Data Center located in the same country. In the event that the Customer and the Provider come to such an agreement, the Customer shall not be required to sign a replacement Order in order to effect that change and the Provider shall not be in breach of the Agreement or any Order if it moves or redirects the Customer's data in accordance with that agreement.

5. **Service Level Agreement.** Infrastructure and Service Availability, Service Performance, and Response times are available on the Service Level Agreement accessible at https://1111systems.com/legal/sla

6. **Disabling Cloud Resources.** If the Cloud Resources get infected, hacked, or are compromised in any way, or if it is determined by the Provider that there is a potential threat to the Provider's network or any of the Provider's other customers, the Provider will make commercial best efforts to notify the Customer and may in its sole discretion disable the Cloud Resources until the Customer can take the appropriate actions to resolve the issue or contact the Provider to resolve the issue. The Provider may disable the Cloud Resources at any time if the Provider reasonably believes that the Customer has violated the Provider's then-current Acceptable Use Policy.

7. **Beta Service Participation.** This section describes the terms and conditions under which the Customer may access certain services or features available by the Provider that are not considered Generally Available. Services or features labeled "beta" (each, a "Beta Service"), or access and use of the Provider's Services available in Data Centers that are also labeled as "Beta Location".

    1. Customer may access the applicable Beta Service used in a generally available Data Center, or in a Beta Location during the term specified by the Provider;

    2. Customer shall not grant access to any Beta Service by any third-party other than the Customer's employees and contractors that have executed written non-disclosure agreements with the Provider;

    3. Customer shall not advertise or publicly disclose any of the features, services or performance of the Beta Services without the written approval from the Provider;

    4. The Customer shall utilize the applicable Beta Service used in a generally available Data Center, or in a Beta Location only for internal evaluation purposes or to provide feedback to the Provider;

    5. The Customer shall comply with the Provider's then-current Acceptable Use Policy when accessing and using the Beta Service or the Provider's Services in a Beta Location;

    6. The Provider may suspend or terminate Customer's access to or use of Beta Service or the Provider's Services available in Beta Locations;

    7. The Customer shall provide reasonably-requested information related to access, use, testing, or evaluation results of the Beta Services to the Provider;

    8. The Customer agrees that the Provider does not guarantee any Service Level, performance or stability of the Beta Service or any of the Provider's Services in Beta Locations;

    9. Access or use of the applicable Beta Services or the Provider's Services in the Beta Location will automatically terminate upon the release of a generally available version;

    10. The Customer agrees that after termination of

        1. The applicable Beta Service, or

        2. Access to a Provider's Service in a Beta Location,

there will be a decommissioning process that will include the erasure of all the Customer's data;

    11. The Customer agrees that the Provider does not guarantee that any Beta Service or the Provider's Services in any Beta Location will ever be made generally available, or that the generally available version will be the same or similar as the version made available by the Provider during the term of the Beta Service or Beta Location, as applicable; and

12. THE PROVIDER EXCLUDES ALL WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, WITH RESPECT TO ANY SERVICE PROVIDED AS PART OF THE BETA SERVICE OR BETA LOCATION, AS APPLICABLE, INCLUDING WARRANTIES FOR MERCHANTABILITY, FITNESS FOR ANY PARTICULAR PURPOSE, OR SATISFACTORY QUALITY OR WHETHER AT COMMON LAW OR CONTRACT OR TORT OR BY STATUTE, OR OTHERWISE. THE BETA SERVICES AND THE PROVIDER'S SERVICES IN ANY BETA LOCATION ARE OFFERED ON AN AS-IS, WHERE IS BASIS, WITH ALL FAULTS, AND ARE NOT SUBJECT TO ANY OF THE WARRANTIES SET OUT IN THE AGREEMENT.

8. **Inbound and Outbound Shipping Policy to/from any of the Provider's Data Center.** The terms and conditions of this Section 2.8 shall be applicable if the Customer-Provided Equipment needs to be shipped from the Customer to the Provider or from the Provider to the Customer.

    1. Responsibility and Liability. It is the Customer's sole responsibility to arrange the packaging and shipping of the Customer-Provided Equipment, as the Provider does not provide those services. Because the Provider does not provide those services, the Provider accepts no liability or responsibility in regard to the Customer-Provided Equipment being damaged or mishandled in the packaging and shipping process. Any Customer-Provided Equipment or property not removed within thirty (30) days after the expiration or termination of service agreement(s) will be deemed abandoned and become the property of the Provider. The Customer will be liable for all costs incurred by the Provider as a direct result of removal and disposal of any abandoned Customer-Provided Equipment.

    2. Usage of Carriers. Should the Customer utilize a Carrier for this service, the Customer shall coordinate with that Carrier directly in order to address the variables that arise during shipping, such as shipping internationally or any applicable tax or tariff related requirements; and

    3. Provider's Shipping Process. The Customer is required to contact the Provider's project manager for specific details on the Provider's Inbound and Outbound Shipping Process. The Customer shall be charged the applicable Remote Hands and/or i-Tech fees for the Provider's assistance.

9. **Statement of Work (SOW).** The terms and conditions of this Section 2.9 are applicable to all Statement of Work documents that shall be required prior to the Deployment of a Provider’s specific Service.

    1. **Provider’s Obligations.** The Provider is responsible for the following in accordance with industry best practices:

        1. Providing the Customer with a team to ensure the successful completion of the project. This team will include a project manager and a qualified deployment engineer to perform the services purchased; the Provider’s standard support will be available upon completion of the project;

2. Ensuring that resources are available to complete the tasks and hold meetings per the project timeline;
3. Providing all deliverables described in the SOW;
4. Providing written communication and documents through the project tickets;
5. Adhering to the project schedule and milestone projections. The Provider will notify the Customer as soon as possible if a need to reschedule should arise; and
6. Providing a method of feedback for each project.

2. **Customer's Obligations.** The Customer is responsible for the following in accordance with industry best practices:
    1. Designating one Technical Contact as the primary contact who will be responsible for the project, acting as the Customer's project manager;
    2. Reviewing all the documentation the Provider shares with the Customer and asking for clarification when needed;
    3. If required, ensuring that there is enough bandwidth at the Primary Site to enable initial replication of data and successive incremental changes of data to the Recovery Site;
    4. Reviewing the Provider's online product documentation and user guides located on the Provider's Success Center;
    5. Providing ample time for the Customer's project manager to maintain communication with the Provider's project manager to complete the project requirements;
    6. When possible, providing at least one (1) business day written notice to reschedule any meeting. The Provider understands that emergency circumstances come up as is the nature of the IT services business and that, as a result, one day advance notice is not always possible; and
    7. Missed meetings are defined as being absent from a scheduled meeting by 15 minutes or more after the start time without notifying the Provider in writing in advance. If three (3) meetings are missed, then the project may be placed "On Hold" at the Provider's sole discretion, and a project placed on "On Hold" status will be rescheduled to the Provider's next availability. There is no guarantee that a project rescheduled due to "On Hold" status will be assigned to the same Provider's project manager.

3. **Risks.** The SOW and Order were designed and built according to specific information identified during the discovery phase. If that information is incorrect or has changed, the timeline and cost of this project could change.

1. Compatibility. The Provider publishes the Product Compatibility Matrix which details the current requirements for a Customer's system and its compatibility with the Provider's system as specified under Section 2.3.3 of this Service Schedule. For DRaaS and/or Migration Services, the Provider makes every effort to ensure that the Customer's Primary Site or Source Site meets the requirements during the pre-sales process, but in the event something in the Customer's environment is not compatible with the Provider's solution, the Provider shall make every reasonable effort to provide assistance to accommodate the Customer. The most common incompatibilities are:
    1. Customer is running VMs with a VM hardware version which is not supported by the Provider,
    2. Customer is running a version of the replication software that the Provider does not support,
    3. Customer is using Guest Operating Systems that the replication software does not support;
2. Storage. Storage requirements can change quickly. During the kick-off call, the Provider's project manager will confirm the amount of storage you need and the amount of storage you purchased. If more storage is needed, the Provider's project manager will work with the Provider's sales representative to increase storage;
3. Bandwidth. If required, the amount of bandwidth the Customer allocates for replicating the data directly correlates with how long replication will take. The Provider recommends providing as much bandwidth as possible during and after the Customer's office hours. This will ensure the Customer's data is replicated as quickly as possible without affecting the Customer's day-to-day operations;
4. Shared Disks. For DRaaS and/or Migration Services, the Customer understands that any shared disks used across multiple VM's need to be converted to a single VMDK and used from a single VM. Clustered servers or shared disks are not supported within this SOW Section and would require alternate planning. This solution only supports SCSI based disks. CIFS, IDE, or any other disk types are not supported; and
5. Active Directory replication. For DRaaS, the Customer understands that in some cases a live Active Directory server is needed for replication and should be connected to the Customer's internal network for quicker and more seamless recovery of the solution.

3. Section 3: Service-Specific Terms
    1. **11:11 Cloud.** The terms and conditions of this Section 3.1 are applicable to each Order that includes 11:11 Cloud services.

1. **Resources.**

    1. Storage;

        1. Public. These Cloud Resources are available as Shared Resources with Advanced and/or SSD Storage types as specified in the Order,

        2. Dedicated. These Cloud Resources are available as Dedicated Resources with Accelerated and/or SSD Storage types as specified in the Order with varying parameters:

            1. Capacity. Dedicated Storage is sold in preconfigured sizes, each size providing different usable capacity as specified in the Order, which is determined by the maximum recommended usable capacity for the underlying storage component that accounts for the average deduplication and compression ratios.

            2. Performance. Performance for each preconfigured size is specified in the Order.

            3. Interoperability. Dedicated Storage resources are only supported under Private Virtual Data Centers, which should only be comprised of resources with similar capacity and performance. Mixing Public and Dedicated storage under the same Private Virtual Data Center is not supported.

    2. CPU & RAM;

        1. Public. These Cloud Resources are available as Shared Resources as specified in the Order,

        2. Private. These Cloud Resources are available as Dedicated Resources as specified in the Order. The Provider is responsible for architecting and deploying CPU & RAM in a high availability configuration;

    3. Bandwidth (Public or Private). Bandwidth is available as a Shared Resource as specified in the Order. On Orders where network bandwidth is not specified, it is included, abiding by the Excessive Use Section on the Acceptable Use Policy;

    4. Business Models (Public or Private). Cloud Resources are available in either Reserved, Burst, or Reserved plus Burst models as specified in the Order; and

    5. Overhead (Private only). The Customer acknowledges that all applications and hypervisors require some amount of overhead resource capacity in order to run optimally. The Customer agrees that the Dedicated Resources on the Order will be used for the overhead capacity of the Customer's applications/hypervisor and

that it is the sole responsibility of the Customer to ensure sufficient Cloud Resources exist.

2. **Provider's Obligations.** The Provider is responsible for the following in accordance with industry best practices:

    1. Onboarding the Customer into the Provider's Cloud Services by giving access to the service and guiding the Customer through the process of deploying the service;

    2. Provide documentation, project management, and guiding the Customer through an initial set up;

    3. Provide ongoing support and education on the service at the Customer's request;

    4. Creating Virtual Data Center(s) consisting of compute, memory, storage infrastructure, and network bandwidth per specifications detailed in the Order;

    5. Maintaining the underlying cloud infrastructure components such as compute, memory, storage and networking by following the Provider’s guidelines for managing these environments;

    6. Providing the Customer with the URL and authentication credentials to access the Customer’s Cloud Resources;

    7. Assigning external and internal IP addresses for the virtual router per the Customer-provided requirements; and

    8. Providing VM templates with Microsoft Windows Data Center Licensing.

3. **Customer's Obligations.** The Customer is responsible for the following in accordance with industry best practices:

    1. Unless specified on the Order, implementing dedicated physical or virtual network security appliance, managing Firewall(s) including but not limited to the configuration of Network Address Translation (NAT) Access List, Virtual Private Network (VPN), Dynamic Host Configuration Protocol (DHCP), Load Balancing, and static routing;

    2. If the Customer chooses to Seed Data, then the Customer must follow the Provider’s then-current Data Seeding Guidelines;

    3. Maintaining operating systems and applications installed on the Customer's Virtual Machines or in the Customer's Virtual Data Center, including, but not limited to, patching, upgrades, updates and anti-virus software in accordance with industry best practices;

    4. Fixing any problems resulting from upgrades to the Virtual Machines operating system;

    5. Providing Virtual Machine and application log monitoring;

6. Providing support for operating systems and applications installed on the Customer-Managed Virtual Machines; and

7. If the Customer provisions Reserved Resources in excess of the specifications set out on the Order, the Customer hereby acknowledges that the Provider is not responsible for any performance degradation or errors caused by over allocation.

4. **Encryption.**

    1. VM Encryption.

        1. The Provider offers encryption on a per VM or per volume basis, and is available to the Customer if purchased on the Order,

        2. The Customer agrees and understands that when running VM Encryption some features in the 11:11 Cloud Console that require access to the Customer's VMs may not function or provide information, since the Customer's VM will be encrypted, and

        3. VM Encryption encrypts data using AES-128/256 algorithms and allows the Customer to manage the encryption keys. The Customer understands that the Provider has no access to encryption keys.

5. **Security Features.**

    1. The 11:11 Cloud Console performs the following function:

        1. Vulnerability Scanning. Assesses systems, networks and applications for weaknesses and detects known and zero-day attacks. Examines all incoming and outgoing traffic for protocol deviations, policy violations, or content that signals an attack. The weekly predefined scan generates a report which is added to the historical data.

2. **11:11 Secure Cloud.** The terms and conditions of this Section 3.2 are applicable to each Order that includes 11:11 Secure Cloud services.

    1. **Resources.**

        1. Storage;

            1. Public. These Cloud Resources are available as Shared Resources with Accelerated and/or SSD Storage types as specified in the Order; and

            2. Dedicated. These Cloud Resources are available as Dedicated Resources with Accelerated and/or SSD Storage types as specified in the Order with varying parameters:

1. Capacity. Dedicated Storage is sold in preconfigured sizes, each size providing different usable capacity as specified in the Order, which is determined by the maximum recommended usable capacity for the underlying storage component that accounts for the average deduplication and compression ratios.

2. Performance. Performance for each preconfigured size is specified in the Order and it's defined based on the underlying storage component's total IOPS based on 50/50 Read/Write and using 4K random block size.

3. Interoperability. Dedicated Storage resources are only supported under Private Virtual Data Centers, which should only be comprised of resources with similar capacity and performance. Mixing Public and Dedicated storage under the same Private Virtual Data Center is not supported.

2. CPU & RAM;

    1. Public. These Cloud Resources are available as Shared Resources as specified in the Order; and

    2. Private. These Cloud Resources are available as Dedicated Resources as specified in the Order. The Provider is responsible for architecting and deploying CPU & RAM in a high availability configuration;

3. Bandwidth (Public or Private). Bandwidth is available as a Shared Resource as specified in the Order. On Orders where network bandwidth is not specified, it is included, abiding by the Excessive Use Section on the Acceptable Use Policy;

4. Business Models (Public or Private). Cloud Resources are available in either Reserved Resources, Burst, or Reserved Resources plus Burst models as specified in the Order; and

5. Overhead (Private only). The Customer acknowledges that all applications and hypervisors require some amount of overhead resource capacity in order to run optimally. The Customer agrees that the Dedicated Resources on the Order will be used for the overhead capacity of the Customer's applications/hypervisor and that it is the sole responsibility of the Customer to ensure sufficient Cloud Resources exist.

2. **Provider's Obligations.** The Provider is responsible for the following in accordance with industry best practices:

1. Onboarding the Customer into the Provider's Cloud Services by giving access to the service and guiding the Customer through the process of deploying the service;
2. Provide documentation, project management, and guiding the Customer through an initial set up;
3. Provide ongoing support and education on the service at the Customer's request;
4. Creating Virtual Data Center(s) consisting of compute, memory, storage infrastructure, and network bandwidth per specifications detailed in the Order;
5. Maintaining the underlying cloud infrastructure components such as compute, memory, storage and networking by following the Provider's guidelines for managing these environments;
6. Providing the Customer with the URL and authentication credentials to access the Customer's Cloud Resources;
7. Assigning external and internal IP addresses for the virtual router per the Customer-provided requirements; and
8. Providing VM templates with Microsoft Windows Data Center Licensing.

3. **Customer's Obligations.** The Customer is responsible for the following in accordance with industry best practices:
    1. Unless specified on the Order, implementing dedicated physical or virtual network security appliance, managing Firewall(s) including but not limited to the configuration of Network Address Translation (NAT) Access List, Virtual Private Network (VPN), Dynamic Host Configuration Protocol (DHCP), Load Balancing, and static routing;
    2. If the Customer chooses to Seed Data, then the Customer must follow the Provider's then-current Data Seeding Guidelines;
    3. Maintaining operating systems and applications installed on the Customer's Virtual Machines or in the Customer's Virtual Data Center, including, but not limited to, patching, upgrades, updates and anti-virus software in accordance with industry best practices;
    4. Fixing any problems resulting from upgrades to the Virtual Machines operating system;
    5. Providing Virtual Machine and application log monitoring;
    6. Providing support for operating systems and applications installed on the Customer-Managed Virtual Machines; and
    7. If the Customer provisions Reserved Resources in excess of the specifications set out on the Order, the Customer hereby

acknowledges that the Provider is not responsible for any performance degradation or errors caused by over allocation.

4. **Encryption.**

    1. Storage Encryption. Storage is encrypted at rest with AES-256 in XTS cipher mode with FIPS 140-2 approved algorithms;

5. **Security Features.**

    1. The Provider offers internal and external vulnerability scanning and reporting on the Customer's public Internet facing IPv4 address blocks and presents the information in the 11:11 Cloud Console;

    2. The 11:11 Cloud Console performs the following functions, if enabled, and displays them in reports. In order to enable some features, a software agent may be required to be loaded on the Virtual Machine:

        1. Vulnerability Scanning. Assesses systems, networks and applications for weaknesses and detects known and zero-day attacks. Examines all incoming and outgoing traffic for protocol deviations, policy violations, or content that signals an attack. There are 2 types of scanning available:

            1. Weekly predefined scan and report, and

            2. On-demand scan that generates new reports ad-hoc.

        2. Malware Detection. Detects malware, viruses, spyware, trojans, and other malware,

        3. Firewall. Bidirectional host-based stateful firewall that audits all traffic incoming and outgoing from the VM,

        4. Configuration Auditing. Checks that IT assets are compliant with the Provider’s policies and standards,

        5. Compliance Reports. Provides logs and data necessary to fulfill audit requirements,

        6. Web Application Scanning. Discovers web server and services weaknesses and OWASP vulnerabilities, and

        7. Integrity Monitoring. Monitors critical operating system and application files, such as directories, registry keys, and values, to detect and report malicious and unexpected changes in real time; and

    3. The information contained within the reports are intended solely to identify threats, vulnerabilities, and statuses of the Cloud environment components, and is provided “as is” without warranty of any kind, express or implied, including but not limited to

warranties for fitness of purpose. The Provider does not warrant the completeness of accuracy of the report, nor does it make any recommendations based on the findings noted herein.

3. **Standard Backups.** The terms and conditions of this Section 3.3, are applicable to each Order that includes both the Provider's Standard Backups and at least one of the Provider's services that are described in any of the following Sections: Section 3.1 (11:11 Cloud), Section 3.2 (11:11 Secure Cloud), 11:11 Secure Private Cloud, Section 3.6 (11:11 DRaaS for Zerto Cloud-to-Cloud), Section 3.10 (11:11 DRaaS for Zerto), and Section 3.11 (11:11 Secure DRaaS for Zerto) of this Schedule.
    1. **Resources.**
        1. Storage. The amount of storage available for backups as specified by the Order;
        2. Licensing. All required licensing is included in the service on the Target Site;
        3. Business Models. Storage is available in a Reserved plus Burst model;
    2. **Provider's Obligations.** The Provider is responsible for the following in accordance with industry best practices:
        1. Providing the pool of storage as specified by the Order;
        2. Creating initial backup jobs with the number and frequency of the backup restore points on the target location as specified by the Order;
        3. Provide ongoing support and education on the Service at the Customer's request;
        4. Maintaining the underlying cloud infrastructure components such as compute, memory, storage and networking by following Provider's guidelines for managing these environments;
        5. Providing storage pool modification options to the Order as required by the Customer, which is directly linked to the amount of production storage;
        6. In case of Provider-assisted restoration, assisting the Customer with initiating the restore at-time-of-Disaster; and
        7. In the event of Disaster and restoration from the Target Site, the Provider can, if needed, assisting the Customer with restoration from Disasters to the Customer's Source Site for additional i-Tech fees.
    3. **Customer's Obligations.** The Customer is responsible for the following in accordance with industry best practices:

1. Providing the Provider with information reasonably request to fulfill its obligations, including without limitation backup requirement details;

2. At the Customer's discretion, restoring backups either through the self-service 11:11 Cloud Console or by requesting support from the Provider in restoring backups;

3. Performing agent-based application aware backups and restores, as the Provider does not guarantee the recoverability of individual applications running on the Virtual Machines, such as databases or email messaging systems. The Customer is also responsible for performing granular recovery of individual items from agent-based application aware backups;

4. Promptly notifying the Provider if the Cloud Resources are hacked, accessed by a person lacking permission to access the Cloud Resources, or infected with a virus, worm or similar code;

5. If the Customer provisions Reserved Resources in excess of the specifications set out on the Order, the Customer hereby acknowledges that the Provider is not responsible for any performance degradation, loss of backup data, or errors caused by over allocation, this includes the storage necessary for processing the snapshot-based backups, which could result in production storage Burst charges; and

6. In order for the Customer to restore Virtual Machine data, the Customer must have sufficient storage available. If the Customer does not have sufficient storage available, the Customer may have to purchase more storage to make the restore possible.

4. **Risks.**

    1. There may be times where the Provider's service is unable to perform daily backups. Reasons for a backup job failure include, but are not limited to, situations where a job is unable to start during retry windows, services are temporarily unavailable, conflicts occur between resources, etc. Where such failure occurs, the Provider will use reasonable efforts to attempt to remedy any potential backup job failures, and the Customer shall hold the Provider harmless in the event that a backup job did not occur successfully.

4. **Advanced Backups.** The terms and conditions of this Section 3.4, are applicable to each Order that includes both the Provider's Advanced Backups and at least one of the Provider's services that are described in following Sections: Section 3.1 (11:11 Cloud), Section 3.2 (11:11 Secure Cloud), Section 3.6 (11:11 DRaaS for Zerto Cloud-to-Cloud), Section 3.8 (11:11 DRaaS for Veeam), Section 3.9 (11:11 Secure DRaaS for Veeam), Section 3.10 (11:11 DRaaS for Zerto), Section 3.11 (11:11 Secure DRaaS for Zerto), and Section 3.45 (11:11 DRaaS for Cohesity) of this Schedule.

    1. **Resources**

1. Backup Policies. The policies that define the Advanced Backup schedule of how frequently and when to take a backup and also the retention timeframe for that backup. The policies also define how often full backups should be taken and how often to retry in the event of backup failure;
2. Backup Groups. Groups define what Virtual Machines and backup agents are backed up and assigns defined Backup Policy to those virtual machines and backup agents;
3. Licensing. All required licensing is included in the service on the Target Site; and
4. Business Models. Storage is available in a Reserved plus Burst model.

2. **Provider's Obligations.** The Provider is responsible for the following in accordance with industry best practices:
    1. Providing the pool of Storage as specified by the Order;
    2. Providing documentation and guide the Customer through an initial setup;
    3. Providing ongoing support and education on the Service at the Customer's request;
    4. Maintaining the underlying cloud infrastructure components such as compute, memory, storage and networking by following Provider's guidelines for managing these environments;
    5. Providing storage pool modification options to the Order as required by the Customer;
    6. In case of Provider-assisted restoration, assisting the Customer with initiating the restore at-time-of-Disaster; and
    7. In the event of Disaster and restoration from the Target Site, the Provider can, if needed, assist the Customer with restoration from Disasters to the Customer's Source Site for additional i-Tech fees.
3. **Customer's Obligations.** The Customer is responsible for the following in accordance with industry best practices:
    1. Providing the Provider with information reasonably request to fulfill its obligations, including without limitation backup requirement details;
    2. Creating and Maintaining the Backup Policies and Backup Groups through the self-service 11:11 Cloud Console. The Customer is responsible to ensure that their Virtual Machines are in the appropriate Backup Groups and have the appropriate Backup Policies applied to meet the Customer's desired RPO and retention times;

3. Performing agent-based application aware backups and restores, as the Provider does not guarantee the recoverability of individual applications running on the Virtual Machines, such as databases or email messaging systems. The Customer is also responsible for performing granular recovery of individual items from agent-based application aware backups;

4. At the Customer's discretion, restoring backups either through the self-service 11:11 Cloud Console or by requesting support from the Provider in restoring backups;

5. Promptly notifying the Provider if the Cloud Resources are hacked, accessed by a person lacking permission to access the Cloud Resources, or infected with a virus, worm or similar code;

6. If the Customer provisions Reserved Resources in excess of the specifications set out on the Order, the Customer hereby acknowledges that the Provider is not responsible for any performance degradation, loss of backup data, or errors caused by over allocation, this includes the storage necessary for processing the snapshot-based backups, which could result in production storage Burst charges; and

7. In order for the Customer to restore Virtual Machine data, the Customer must have sufficient storage available. If the Customer does not have sufficient storage available, the Customer may have to purchase more storage to make the restore possible.

4. **Risks.**

    1. Customer acknowledges that Provider is not responsible for monitoring backup job performance and status. Customer is fully responsible for the monitoring of job performance, SLAs, Backup Policies and Backup Groups. Customer may engage Provider in assistance in monitoring such items for additional i-Tech fees; and

    2. There may be times where the Providers service is unable to perform daily backups. Reasons for a backup job failure include, but are not limited to, situations where a job is unable to start during retry windows, services are temporarily unavailable, conflicts occur between resources, etc. Where such failure occurs, the Provider will use reasonable efforts to attempt to remedy any potential backup job failures, and Customer shall hold Provider harmless in the event that a backup job did not occur successfully.

5. **11:11 Managed Migration.** The terms and conditions of this Section 3.5 are applicable to each Order that includes the Provider's Managed Migration in combination with either 11:11 Cloud or 11:11 Secure Cloud.

    1. **Assets & Deliverables.**

1. Connectivity Design Documentation. Technical documents and/or diagrams providing engineering level information and configuration details for the purpose of interconnecting the Customer Primary Site(s) to the designated Provider Site(s) delivering the service capabilities to the Customer;

2. On-boarding Project Plan A documented overview of all tasks associated with the Provider's on-boarding process for interconnectivity and delivery of the Managed Migration from the Customer Primary Site(s) Workloads within scope of the mutually agreed upon service contract. The purpose of this document is to track ownership, progress and completion of all applicable on-boarding tasks in collaboration between the Customer and the Provider; and

3. Migration Workbook. A detailed discovery document used to collect all of the Customer specific technical and infrastructure related information for the sole purpose of the Provider providing the Managed Migration as part of the service contract.

2. **Migration Project Management.**

    1. Project managers. Both the Provider and the Customer shall appoint a project manager each who will serve as the primary contact point; and

    2. Migration Project Management Engagement. The Provider's project manager and the Customer's project manager shall meet as required for the duration of the migration process for the purposes of facilitating a successful relationship and overseeing the implementation of all Cloud Resources and Managed Migration outlined in the Order and the Migration Provisioning Form, including but not limited to, (a) tracking the progress of the migration and implementation process and all associated tasks; (b) reviewing other current or future projects or business plans that may impact the Managed Migration, (c) reviewing weekly status reports in order to review the Provider's performance in execution of the project for delivery of all Managed Migration Services, (d) coordinating and planning for any new equipment or software acquisitions specific to supporting the completion of the Managed Migration.

3. **Provider's Obligations.** The Provider is responsible for the following in accordance with industry best-practices:

    1. Providing enhanced onboarding project management deliverables, to include:

        1. Status call between the Provider's migration personnel and the applicable Customer's contacts, and

2. Status report summarizing project tasks progress, project milestones, estimated and actual durations/completion dates and critical path items;

2. Providing and managing supporting service documentation to include:

    1. Inventory and workload specifications (e.g. compute, storage, networking) of all Workloads within scope of the Order, and

    2. L2/L3 network design for compatibility and integration between the Customer's Primary Site(s) and the Provider's networking services and design guidelines;

3. If applicable, providing installation, configuration and management of all services components required for the Managed Migration, to include:

    1. Replication software installation, guiding the Customer through setup and configuration both in the Customer on-premises and the Provider's cloud data center environments (where applicable),

    2. Setup and configuration of VPN connections (where applicable), and

    3. Setup and configuration of all Provider's side networking components support dedicated circuits for WAN connectivity (where applicable);

4. Providing full setup and configuration for replication of the Workloads within scope and applicable to the Order and the Migration Workbook.

4. **Customer's Obligations.** The Customer is responsible for the following in accordance with the Provider's delivery of the 11:11 Managed Migration and industry best-practices:

    1. Ensure all Customer-owned software, applications, devices, systems, processes, and services that maintain the Customer's data to be migrated as part of the Order are covered as specified under Section 2.3.5 of this Service Schedule for the purposes of fulfilling the Order;

    2. Where applicable, the Customer shall maintain all firmware or software updates to all Customer-owned hardware, software, applications, devices, and systems in use with or protected by services provided by the Provider;

    3. Where applicable: contact all software, application, device, system, service, and service providers covered under the Order and add appropriate Provider's personnel as approved contacts for the purposes of fulfilling this Service Schedule;

4. Complete the Migration Provisioning Form provided by the Provider;
5. Provide all current and existing documentation of the Customer's Primary Site(s) to include; environment "as-built" documentation, application contact information, application dependencies, current backup strategy, and disaster recovery plans if applicable;
6. Provide the Provider's personnel with Customer's asset discovery and documentation where applicable;
7. Where applicable; provide all current process documentation in support of the Managed Migration outlined in the Order and provide all assistance necessary to modify existing or implement new processes to streamline the delivery of services;
8. Where applicable, the Customer shall maintain all software and other devices or items provided to the Customer by the Provider located within the Customer's Primary Site(s) in direct support of the delivery of the Managed Migration Service outlined in the Order (the "Equipment') in good working order and in accordance with applicable manufacturers' specifications. The Customer shall notify the Provider immediately upon determination that any Equipment is not in compliance with the foregoing, or is in material breach of the terms and conditions set forth in this Service Schedule; and
9. The Customer shall cooperate with the Provider with regard to the performance of the Provider's obligations hereunder, including (without limitation):
    1. Providing the Provider with the required remote access to Customer's Equipment, as may be reasonable to permit the Provider to perform its obligations hereunder, and
    2. Notifying the Provider of any changes to its configurations that could potentially impact the Managed Migration.

6. **11:11 DRaaS for Zerto Cloud-to-Cloud.** The terms and conditions of this Section 3.6 are applicable to each Order for 11:11 DRaaS for Zerto Cloud-to-Cloud services.
    1. **Resources.** The Cloud Resources used in the Recovery Site mimic the Cloud Resources used in the Primary Site, hence the available features will be the same as the Cloud Resources specified in the Order for the Primary Site.
        1. Storage. The types of storage available are Advanced, Accelerated, and/or SSD Storage purchased by the Customer includes both protected data and Zerto Journal data; Zerto Journal data may not be displayed on the 11:11 Cloud Console, but the Customer is still responsible for paying for this storage and may request a report from the Provider if required. Storage types comprising the environment are specified in the Order;

2. CPU & RAM. These Cloud Resources are available as Shared Resources. CPU & RAM comprising the environment are specified in the Order;

3. Bandwidth. Bandwidth is available as a Shared Resource as specified in the Order. On Orders where network bandwidth is not specified, it is included, abiding by the Excessive Use Section on the Acceptable Use Policy;

4. Replication License. Replication licensing per protected Virtual Machine as specified in the Order; and

5. Business Models. Storage is available in a Reserved plus Burst model. CPU, RAM and Bandwidth are available in a Burst model.

2. **Provider's Obligations.** The Provider is responsible for the following in accordance with industry best practices:

    1. Onboarding the Customer into the Provider's Cloud Services by giving access to the service and guiding the Customer through the process of deploying the service;

    2. Provide documentation, project management, and guiding the Customer through an initial set up;

    3. Provide ongoing support and education on the Service at the Customer's request;

    4. Creating Virtual Data Center(s) consisting of compute, memory, storage infrastructure, and network bandwidth per specifications detailed in the Order;

    5. Maintaining the underlying cloud infrastructure components such as compute, memory, storage and networking by following Provider’s guidelines for managing these environments;

    6. Providing the Customer with the URL and authentication credentials to access the Customer’s Cloud Resources;

    7. Assigning external and internal IP addresses for the Primary Site virtual router per Customer-provided requirements;

    8. Assigning external and internal IP addresses for the Recovery Site virtual router per Customer-provided requirements;

    9. Providing replication licensing and replication management for Virtual Machines as described in the Order as completed by the Customer;

    10. Configuring protection at the Primary Site using the 11:11 Cloud-to-Cloud Recovery replication and retention policy of 24 hours of data retention for replicated servers at Recovery Site with replication frequency occurring once or more per hour between sites;

11. Creating Virtual Protection Groups, per environment, per vApp, and initiate replication on Virtual Machines selected for replication;
12. In case of Provider-assisted Failover, assisting the Customer with initiating Failover at-time-of-Disaster;
13. Maintaining exclusive control of system administration security (e.g. administrator or root) level access for Provider-managed firewall or load balancing infrastructure;
14. In the event of a Disaster and Failover to the Recovery Site, the Provider can, if needed, assist the Customer with Failback from Disasters to the Customer's Primary Site for additional i-Tech fees;
15. Re-advertise the Customer's IP Address Block from in case of Disaster; and
16. If the Customer is running the Standard Backups service defined in Section 3.1, in the event of either a failover or of a VM being active in the Recovery Site's virtual environment, the Provider will automatically begin backing up the Customer's live workloads within 24 hours.

3. **Customer's Obligations.** The Customer is responsible for the following in accordance with industry best practices:
    1. Unless specified on the Order, implementing dedicated physical or virtual network security appliance, managing Firewall(s) including but not limited to the configuration of Network Address Translation (NAT) Access List, Virtual Private Network (VPN), Dynamic Host Configuration Protocol (DHCP), Load Balancing, and static routing;
    2. Providing compute, memory, storage and network requirements for each Virtual Data Center and creating Virtual Data Center network and role-based security policies;
    3. If the Customer chooses to Seed Data, then the Customer must follow the Provider's then-current Data Seeding Guidelines;
    4. Ensuring Virtual Machines match specifications as defined in the Provider's then-current Product Compatibility Matrix;
    5. Maintaining operating systems and applications installed on the Customer's Virtual Machines or in the Customer's Virtual Data Center, including, but not limited to, patching, upgrades, updates and anti-virus software in accordance with industry best practices;
    6. Fixing any problems resulting from upgrades to the Virtual Machines operating system;
    7. Providing Virtual Machine and application log monitoring;
    8. Providing support for operating systems and applications installed on the Customer-Managed Virtual Machines;

9. Informing the Provider at the time any of these changes occur in the Primary Site:
    1. Adding a disk to a Virtual Machine or adding a Virtual Machine to a replicated vApp,
    2. Shutting down Virtual Machine in a protected vApp for an extended period (< 5 minutes),
    3. Deleting a Virtual Machine from a protected vApp, and
    4. Increasing resource capacity in Primary Site in relation to replicated Virtual Machines without increasing Cloud Resources at Recovery site;
10. Initiating failover at-time-of-test and at-time-of-Disaster using the 11:11 Cloud Console;
11. In case of Provider-assisted Failover, declaring a Disaster affecting the Primary Site following the Provider's guidelines; and
12. If the Customer provisions Reserved Resources in excess of the specifications set out on the Order, the Customer hereby acknowledges that the Provider is not responsible for any performance degradation or errors caused by over allocation.

4. **Service Levels.** Recovery Time Objective (RTO) and Recovery Point Objective (RPO) SLAs are accessible at https://www.1111systems.com/legal/sla.

7. **11:11 Cloud Backup for Veeam Cloud Connect.** The terms and conditions of this Section 3.7 are applicable to each Order that includes 11:11 Cloud Backup for Veeam Cloud Connect services.
    1. **Resources.**
        1. Storage and Bandwidth. The Cloud Resources that comprise the 11:11 Cloud Backup for Veeam Cloud Connect service include Archive Storage along with embedded unlimited incoming and outgoing network bandwidth as described in the Order. Unlimited network bandwidth shall be subject to Section 3.7.4 below;
        2. Licensing. Veeam Cloud Connect licensing is included in the service on the Target Site;
        3. Insider Protection. The Provider offers Veeam Insider Protection service to the Customer if purchased on the Order. This service feature is not available for service subscription Item Numbers and/or Data Centers identified in the Order with the reference "PC1"; and
        4. Business Models. Storage is available in a Reserved model only.

2. **Provider's Obligations.** The Provider is responsible for the following in accordance with industry best practices:

    1. Providing pool of Cloud Storage, Veeam Cloud Connect licensing, and network bandwidth at Target Site per specifications detailed in the Order;

    2. Maintaining Target Site Cloud Storage infrastructure including patching, upgrades and updates;

    3. Creating Cloud Resources per specifications detailed in the Order;

    4. Providing Customer the URL and authentication credentials to access the Customer's Cloud Resources;

    5. Providing storage pool modification options to the Order as required by the Customer;

    6. Providing up to two active connections between the backup server at the Source Site and the Cloud Resources at the Target Site per set of credentials. Additional active connections can be requested with the Provider's approval. All other jobs running concurrently will sit idle until the job using the connection completes. The same set of credentials can be used to send to concurrent backups from different locations, or Source Sites to the same Target Site Alternatively, two different sets of credentials can be used to send backups concurrently from the same backup server at the Source Site;

    7. Insider Protection. Providing the Customer with Insider Protection if purchased on the Order with the following parameters:

        1. Retention. Insider Protection retention shall be set at 7 calendar days for the entire cloud repository,

        2. Backup repository. After the Customer deletes a backup on a cloud repository, regardless if this was intentional, accidental or caused by malware, the backup file(s) will be moved from the cloud repository to a "recycle bin" folder on the Provider backup repository that's not accessible by the Customer. While backup metadata files are deleted from disk immediately, the Provider will retain only full and incremental backup files,

        3. Repository quota. Backup files retained by the Provider shall not consume the Customer's cloud repository quota, as they are stored in a different folder only accessible by the Provider, and

        4. Backup recovery. Should the Customer submit a request to the Provider to recover a backup via a support ticket along with the i-Tech fees for the professional services to perform the restoration tasks, the Provider shall locate the backup

file(s) required for data restore in the "recycle bin" and pass it/them to the Customer over the network or on a portable drive on a best-effort basis; Once the support ticket is closed, the Provider shall delete the temporary copies of the backup files;

8. Cloud Backup Restore to 11:11 Cloud Services. Providing the Customer with the option to purchase a best-effort cloud restoration service of VMware backups to 11:11 Cloud Services at an additional cost using the backup file chain stored at the Target Site with the following parameters:

    1. The accuracy and success of the restoration depends on the reliability of the backup file chain backed up by the Customer,

    2. The creation of Virtual Data Center(s) will consist of the specifications detailed in the relevant Order,

    3. The network connectivity to the restored environment will be provided by the Provider,

    4. The restoration shall be limited to repositories smaller than 20,000 GB,

    5. The restoration shall be limited to VMware based environments, and

    6. The Provider will start the restoration process within 24 hours after the Customer has both declared a Disaster by notifying the Provider and approved the new Order that contains the cloud resources required to run the workloads along with the i-Tech fees for the professional services required to perform the restoration tasks; and

9. Backup immutability. Providing the Customer with 30 days of immutability with the following parameters:

    1. Availability. 30 days of built in immutability is only available in Data Centers identified with the reference "PC1",

    2. Retention. 30 days of immutability is applicable to any backup stored in the Veeam Cloud Connect Backup repository. Any backup created with a GFS policy, will remain immutable for the duration of the GFS retention. All backups stored will be held for a minimum of the retention period plus the immutability period of 30 days plus the block generation period of 30 days and cannot be removed or deleted by the Customer or Provider until all three periods have passed, and

    3. Repository quota. Immutability storage overhead shall be accounted for when the solution is sized.

Backup Immutability is only available for service subscription Item Numbers and/or Data Centers identified in the Order with the reference “PC1”.

3. **Customer's Obligations.** The Customer is responsible for the following in accordance with industry best practices:

    1. Providing the Provider with information reasonably required to fulfill its obligations, including without limitation backup requirement details;

    2. Procuring, implementing, and configuring of the correct licensed versions of Veeam Cloud Connect software on the Machines as specified in the Provider's then-current Product Compatibility Matrix;

    3. Configuring and performing of backups, recovery tasks, and Testing within the Veeam software installation;

    4. Managing applicable Customer-controlled firewall(s) including but not limited to the configuration of Network Address Translation (NAT), Access List, Virtual Private Network (VPN), Dynamic Host Configuration Protocol (DHCP), and static routing in relation to the Customer's connectivity to the Target Site;

    5. Fixing any problems resulting from upgrades to the Veeam Cloud Connect software;

    6. Maintaining software (including without limitation the Veeam Cloud Connect software) on the Customer's machines including, but not limited to, patching, upgrades, updates and anti-virus software in accordance with industry best practices;

    7. Ensuring the functioning of services or software running on the Customer’s machines;

    8. Providing support for operating systems and applications installed on the Customer’s machines;

    9. Promptly notifying the Provider if the Cloud Resources are hacked, accessed by a person lacking permission to access the Cloud Resources, or infected with a virus, worm or similar code;

    10. Ensuring that during the term of the Order the Customer maintains enough bandwidth to ensure the continued successful backup of the data. The Customer acknowledges that the Provider is not in breach of the agreement if there is not enough bandwidth available at Source Site;

    11. If the Customer provisions backup jobs in excess of the specifications set out on the Order, the Customer hereby acknowledges that the Provider is not responsible for any performance degradation, loss of backup data, or errors caused by over allocation;

12. Insider Protection. In case of requesting the Provider to recover a deleted backup:
    1. Making the request via a support ticket,
    2. Providing the Provider with the sufficient information about the deleted backup data so the Provider can locate the backup file(s) required for data restore,
    3. Importing the full backup file(s) to the backup server on the Customer side, and
    4. Restoring the data from the backup after successfully importing the backup file(s);
13. Cloud Backup Restore. In case of requiring a cloud backup restore:
    1. Declaring a Disaster by notifying the Provider and approving the Order that contains the cloud resources required to run the workloads along with the i-Tech fees for the professional services required to perform the restoration tasks; and
    2. The Customer understands that restoring the environment from cloud backup files is a best-effort service and acknowledges that the Provider is not responsible for any performance degradation, loss of data, or errors on the VMware-based restored environment as the success of the restoration depends on the reliability of the backup file chain;

This service feature is not available for service subscription Item Numbers and/or Data Centers identified in the Order with the reference “PC1”; and

14. Encryption at Rest. The Customer may optionally configure encryption for backup data using the Veeam software prior to transmitting the data to the Provider. Encryption of backup data shall be automatically enforced for service subscription Item Numbers and/or Data Centers identified in the Order with the reference "PC1".

4. **Data Egress**
    1. Data egress charges are included if usage patterns are deemed reasonable for the service offering. Reasonable data egress shall mean allowed egress of up to 50% of total stored data, measured in GB per month per region, within the Customer account; and
    2. The Provider reserves the right to charge for any data egress exceeding the reasonable data egress standard above.

8. **11:11 DRaaS for Veeam.** The terms and conditions of this Section 3.8 are applicable to each Order that includes 11:11 DRaaS for Veeam services, regardless as to whether the Order for public or private cloud services.

1. **Resources.**

    1. Storage and Bandwidth (Public or Private). The Cloud Resources that comprise the 11:11 DRaaS for Veeam service include Accelerated and/or SSD Storage along with embedded unlimited incoming and outgoing network bandwidth as described in the Order;

    2. CPU & RAM;

        1. Public. These Cloud Resources are available as Shared Resources as specified in the Order; and

        2. Private. These Cloud Resources are available as Dedicated Resources as specified in the Order. The Provider is responsible for architecting and deploying CPU & RAM in a high availability configuration;

    3. Licensing (Public or Private). Veeam Cloud Connect licensing is included in the service on the Recovery Site;

    4. Business Models (Public or Private). Cloud Resources are available in either Reserved, Burst, or Reserved plus Burst models as specified in the Order. The business model available depends on whether the Customer has a vCenter based environment or a vCloud Director based environment;

        1. vCenter based environments (legacy) – Storage is available in a Reserved model only. CPU and RAM are available in Burst model only, and

        2. vCloud Director based environments – shared Cloud Resources (including Storage, CPU, and RAM) are available in either Reserved or Reserved plus Burst models; and

    5. Overhead (Private only). The Customer acknowledges that all applications and hypervisors require some amount of overhead resource capacity in order to run optimally. The Customer agrees that the Dedicated Resources on the Order will be used for the overhead capacity of the Customer's applications/hypervisor and that it is the sole responsibility of the Customer to ensure sufficient resources exist.

2. **Provider's Obligations.** The Provider is responsible for the following in accordance with industry best practices:

    1. Onboarding the Customer into the Provider's Cloud Services by giving access to the service and guiding the Customer through the process of deploying the service;

    2. Provide documentation, project management, and demonstrate the failover steps for a full site failover to the Customer on the Provider's test environment. In the event that a Customer would like the

Provider to assist with design, implementation or testing of a partial site failover, additional i-Tech fees will apply;

3. Provide ongoing support and education on the service at the Customers' request;
4. Creating Virtual Data Center(s) for recovering VMware based workloads, consisting of compute, memory, storage infrastructure, per specifications detailed in the Order;
5. Maintaining the underlying cloud infrastructure components such as compute, memory, storage and networking by following the Provider's guidelines for managing these environments;
6. Assigning external and internal IP addresses for the Recovery Site virtual router per the Customer-provided requirements;
7. Providing the Customer the URL and authentication credentials to access the Customer's Cloud Resources;
8. Providing up to two active connections between the replication server at the Primary Site and the Cloud Resources at the Recovery Site per set of credentials. Additional active connections can be requested with the Provider's approval. All other jobs running concurrently will sit idle until the job using the connection completes;
9. In case of Provider-assisted Failover, assisting the Customer with initiating Failover at-time-of-Disaster; and
10. In the event of a Disaster and Failover to the Recovery Site, the Provider can, if needed, assist the Customer with Failback from Disasters to the Customer's Primary Site for additional i-Tech fees.

3. **Customer's Obligations.** The Customer is responsible for the following in accordance with industry best practices:
    1. Procuring, implementing, and configuring of the correct licensed versions of Veeam Cloud Connect software on the Machines as specified in the Provider's then-current Product Compatibility Matrix to enable the Secure DRaaS for Veeam Service from the Customer's Premises;
    2. Ensuring that only VMware based workloads are replicated to the Provider and that the Virtual Machine environment matches specifications as defined in the Provider's then-current Product Compatibility Matrix;
    3. Configuring compute, memory, storage and network requirements for each Veeam Hardware Plan and/or Veeam Failover Plan(s), and initiating Veeam replication jobs to the Provider;
    4. Unless specified on the Order, implementing dedicated physical or virtual network security appliance, managing Firewall(s) including

but not limited to the configuration of Network Address Translation (NAT) Access List, Virtual Private Network (VPN), Dynamic Host Configuration Protocol (DHCP), Load Balancing, and static routing;

5. Notifying the Provider before making any changes to the Primary site that might affect the DRaaS service, including, but not limited to, any upgrades or patches to Veeam, the underlying virtualization layer, or the network. The Customer notes that any such actions could break the ability of the Service to function;
6. If the Customer chooses to Seed Data from the Primary site, following the Provider's then-current *Data Seeding Guidelines*;
7. Creating and testing Recovery Plan;
8. Initiating Failover at-time-of-test and at-time-of-Disaster;
9. In case of Provider-assisted Failover, declaring a Disaster via a support ticket;
10. Monitoring available storage in Veeam Cloud Connect Repository to ensure the Service will continue to function properly;
11. Maintaining operating systems and applications installed on the Customer's Virtual Machines or in the Customer's Virtual Data Center, including, but not limited to, providing support, patching, upgrades, updates and anti-virus software in accordance with industry best practices;
12. Providing Virtual Machine and application log monitoring;
13. The Customer understands that Testing can be stopped by the Provider in the event that a Testing event has run long enough to impact replication or the underlying infrastructure;
14. In the event of a Disaster and Failover to the Recovery Site, in order for the Customer to Failback to the Primary Site, the Customer needs to recreate the original environment in the Primary Site by providing similar compute, memory, storage and network resources, and Virtual Machines on the Customer's hosts, enable site peering to Recovery Site, set up and configure Recovery Groups before replicating data from Recovery Site. The Customer is responsible for paying the associated i-Tech fees if assistance from the Provider is required;
15. Promptly notifying the Provider if the Cloud Resources are compromised, accessed by a person lacking permission to access the Cloud Resources, or infected with a virus, worm or similar malicious code;
16. Ensuring that there is enough bandwidth at Primary Site to enable initial replication and successive incremental changes of data to Recovery Site;

17. Ensuring that there are enough Cloud Resources at Recovery site in relation to replicated Virtual Machines from Primary Site;

18. If the Customer provisions replication jobs in excess of the specifications set out on the Order, the Customer hereby acknowledges that the Provider is not responsible for any performance degradation or errors caused by over allocation;

19. Defining, configuring and managing the required number of restore points stored as part of each replication job; and

20. If using Veeam Continuous Data Protection (CDP), installing and maintaining Veeam CDP proxy servers and Veeam CDP software installed on the VMware ESXi Servers.

4. **Encryption.** Providing the Customer with Storage Encryption with the following parameters:

    1. Storage Encryption. Storage is encrypted at rest with AES-256 in XTS cipher mode with FIPS 140-2 approved algorithms;

    2. VM Encryption;

        1. The Provider offers encryption on a per VM or per volume basis, and is available to the Customer if purchased on the Order,

        2. The Customer agrees and understands that when running VM Encryption some features in the 11:11 Cloud Console that require access to the Customer's VMs may not function or provide information, since the Customer's VM will be encrypted, and

        3. VM Encryption encrypts data using AES-128/256 algorithms and allows the Customer to manage the encryption keys. The Customer understands that the Provider has no access to encryption keys.

5. **Security Features (applicable to vCloud director-based environments only).** The 11:11 Cloud Console performs the following function:

    1. Vulnerability Scanning. Assesses systems, networks and applications for weaknesses and detects known and zero-day attacks. Examines all incoming and outgoing traffic for protocol deviations, policy violations, or content that signals an attack. The weekly predefined scan generates a report which is added to the historical data; and

6. **Service Levels** Recovery Time Objective (RTO) and Recovery Point Objective (RPO) SLAs are accessible at https://www.1111systems.com/legal/sla.

9. **11:11 Secure DRaaS for Veeam.** The terms and conditions of this Section 3.9 and, to the extent not inconsistent with this Section 3.9, Section 3.8, are applicable to each Order that includes 11:11 Secure DRaaS for Veeam services, regardless as to whether the Order for public or private cloud services.

1. **Security Features (applicable to vCloud director-based environments only).** Providing the Customer with the following Security Features:
    1. The Provider offers internal and external vulnerability scanning and reporting on the Customer's public Internet facing IPv4 address blocks and presents the information in the 11:11 Cloud Console;
    2. The 11:11 Cloud Console performs the following functions, if enabled, and displays them in reports. In order to enable some features, a software agent may be required to be loaded on the Virtual Machine:
        1. Vulnerability Scanning. Assesses systems, networks and applications for weaknesses and detects known and zero-day attacks. Examines all incoming and outgoing traffic for protocol deviations, policy violations, or content that signals an attack. There are 2 types of scanning available:
            1. Weekly predefined scan and report, and
            2. On-demand scan that generates new reports ad-hoc,
        2. Malware Detection. Detects malware, viruses, spyware, trojans, and other malware,
        3. Firewall. Bidirectional host-based stateful firewall that audits all traffic incoming and outgoing from the VM,
        4. Configuration Auditing. Checks that IT assets are compliant with the Provider's policies and standards,
        5. Compliance Reports. Provides logs and data necessary to fulfill audit requirements,
        6. Web Application Scanning. Discovers web server and services weaknesses and OWASP vulnerabilities, and
        7. Integrity Monitoring. Monitors critical operating system and application files, such as directories, registry keys, and values, to detect and report malicious and unexpected changes in real time; and
    3. The information contained within the reports are intended solely to identify threats, vulnerabilities, and statuses of the Cloud environment components, and is provided "as is" without warranty of any kind, express or implied, including but not limited to warranties for fitness of purpose. The Provider does not warrant the completeness of accuracy of the report, nor does it make any recommendations based on the findings noted herein.
10. **11:11 DRaaS for Zerto.** The terms and conditions of this Section 3.10 are applicable to each Order that includes 11:11 DRaaS for Zerto services, regardless as to whether the Order for public or private cloud services.

1. **Resources.**

    1. Storage (Public or Private). The types of storage available are Advanced, and/or SSD Storage purchased by the Customer includes both protected data and Zerto Journal data; Zerto Journal data may not be displayed on the 11:11 Cloud Console, but the Customer is still responsible for paying for this storage and may request a report from the Provider if required. Storage types comprising the environment are specified in the Order;

    2. CPU & RAM.

        1. Public. These Cloud Resources are available as Shared Resources as specified in the Order; and

        2. Private. These Cloud Resources are available as Dedicated Resources as specified in the Order. The Provider is responsible for architecting and deploying CPU & RAM in a high availability configuration;

    3. Bandwidth (Public or Private). Bandwidth is available as a Shared Resource as specified in the Order. On Orders where network bandwidth is not specified, it shall be considered to be embedded in storage;

    4. Replication License (Public or Private). Replication licensing per protected Virtual Machine as specified in the Order. On Orders where replication licensing is not specified, it shall be considered to be embedded in storage;

    5. Business Models (Public or Private). Cloud Resources are available in either Reserved or Reserved plus Burst models as specified in the Order; and

    6. Overhead (Private only). The Customer acknowledges that all applications and hypervisors require some amount of overhead resource capacity in order to run optimally. The Customer agrees that the Dedicated Resources on the Order will be used for the overhead capacity of the Customer's applications/hypervisor and that it is the sole responsibility of the Customer to ensure sufficient resources exist.

2. **Provider's Obligations.** The Provider is responsible for the following in accordance with industry best practices:

    1. Onboarding the Customer into the Provider's Cloud Services by giving access to the service and guiding the Customer through the process of deploying the service;

    2. Provide documentation, project management, and demonstrate the failover steps for a full site failover to the Customer on the Provider's test environment. In the event that a Customer would like the

Provider to assist with design, implementation or testing of a partial site failover, additional i-Tech fees will apply;

3. Provide ongoing support and education on the Service at the Customers' request;
4. Creating Virtual Data Center(s) consisting of compute, memory, storage infrastructure, and network bandwidth per specifications detailed in the Order;
5. Maintaining the underlying cloud infrastructure components such as compute, memory, storage and networking by following the Provider's guidelines for managing these environments;
6. Providing the Customer with the URL and authentication credentials to access the Customer's Cloud Resources;
7. Assigning external and internal IP addresses for the Recovery Site virtual router per the Customer-provided requirements;
8. Providing Zerto Cloud Connector;
9. Providing Zerto replication licensing for Virtual Machines as defined in the Provider's then-current Product Compatibility Matrix;
10. In case of Provider-assisted Failover, assisting Customer with initiating Failover at-time-of-Disaster;
11. In the event of a Disaster and Failover to the Recovery Site, the Provider can, if needed, assist the Customer with Failback from Disasters to Customer Primary Site for additional i-Tech fees; and
12. If the Customer is running the Standard Backups service defined in Section 3.1, in the event of either a failover or of a VM being active in the Recovery Site's virtual environment, the Provider will automatically begin backing up the Customer's live workloads within 24 hours.

3. **Customer's Obligations.** The Customer is responsible for the following in accordance with industry best practices:
    1. Unless specified on the Order, implementing dedicated physical or virtual network security appliance, managing Firewall(s) including but not limited to the configuration of Network Address Translation (NAT) Access List, Virtual Private Network (VPN), Dynamic Host Configuration Protocol (DHCP), Load Balancing, and static routing;
    2. Providing compute, memory, storage and network requirements for each Virtual Data Center and creating Virtual Data Center network and role-based security policies;
    3. Ensuring that only VMware based Workloads are replicated to the Provider and that the Virtual Machine environment matches specifications as defined in the Provider's Product Compatibility

Matrix. By purchasing this product, the Customer specifically acknowledges that Hyper-V Workloads are not supported;

4. Creating Virtual Machines for Zerto Virtual Manager (ZVM), downloading and installing ZVM software and Zerto Virtual Replication Appliance (ZvRA) on Customer hosts;
5. Configuring Zerto Protection at the Primary Site; Creating Recovery Groups and initiating replication on Virtual Machines selected for replication;
6. Notifying the Provider before making any changes to the Primary site that might affect the DRaaS service, including but not limited to, any upgrades or patches to Zerto, the underlying virtualization layer, or the network. The Customer hereby acknowledges that any such actions could break the ability of the Service to function;
7. If the Customer chooses to Seed Data, then the Customer must follow the Provider's then-current Data Seeding Guidelines;
8. Ensuring Virtual Machines match specifications as defined in the Provider's then-current Product Compatibility Matrix;
9. Creating and testing Recovery Plan;
10. Initiating Failover at-time-of-test and at-time-of-Disaster;
11. In case of Provider-assisted Failover, declaring a Disaster following the Provider's guidelines;
12. Ordering additional Zerto licenses when new VMs are added;
13. Maintaining operating systems and applications installed on the Customer's Virtual Machines or in the Customer's Virtual Data Center, including, but not limited to, providing support, patching, upgrades, updates and anti-virus software in accordance with industry best practices. This includes a supported release of Zerto Virtual Manager. Should the Customer be running a version of Zerto Virtual Manager that is End of Support, the Provider reserves the right to disconnect the service until the Customer has upgraded to a supported version;
14. Providing Virtual Machine and application log monitoring;
15. The Customer understands that Testing can be stopped by the Provider in the event that a Testing event has run long enough to impact replication or the underlying infrastructure;
16. In the event of a Disaster and Failover to the Recovery Site, in order for the Customer to Failback to the Primary Site, the Customer needs to recreate the original environment in the Primary Site by providing similar compute, memory, storage and network resources, Virtual Machines, Zerto Virtual Manager (ZVM) and Zerto Replication Appliance (ZvRA) on the Customer's hosts, enable site peering to

Recovery Site, set up and configure Recovery Groups before replicating data from Recovery Site. The Customer is responsible for paying the associated i-Tech fees if assistance from the Provider is required;

17. Promptly notifying the Provider if the Cloud Resources are compromised, accessed by a person lacking permission to access the Cloud Resources, or infected with a virus, worm or similar malicious code;

18. Informing the Provider at the time any of these changes occur in the Primary Site:

    1. Adding a Virtual Machine to a replicated vApp that exceeds the maximum number of Zerto replication licensing specified on the Order;

    2. Increasing resource capacity in Primary Site in relation to replicated Virtual Machines without increasing Cloud Resources at Recovery site; and

    3. Defining, configuring and managing the required journal retention setting within each VPG.

19. Ensuring that there is enough bandwidth at Primary Site to enable initial replication and successive incremental changes of data to Recovery Site;

20. If the Customer provisions Reserved Resources in excess of the specifications set out on the Order, the Customer hereby acknowledges that the Provider is not responsible for any performance degradation or errors caused by over allocation; and

21. Defining, configuring and managing the required journal retention setting within each VPG.

4. **Encryption.**

    1. <u>VM Encryption.</u>

        1. The Provider offers encryption on a per VM or per volume basis, and is available to the Customer if purchased on the Order,

        2. The Customer agrees and understands that when running VM Encryption some features in the 11:11 Cloud Console that require access to the Customer's VMs may not function or provide information, since the Customer's VM will be encrypted, and

        3. VM Encryption encrypts data using AES-128/256 algorithms and allows the Customer to manage the encryption keys. The Customer understands that the Provider has no access to encryption keys.

5. **Security Features.** The 11:11 Cloud Console performs the following function:

    1. Vulnerability Scanning. Assesses systems, networks and applications for weaknesses and detects known and zero-day attacks. Examines all incoming and outgoing traffic for protocol deviations, policy violations, or content that signals an attack. The weekly predefined scan generates a report which is added to the historical data.

6. **Service Levels.** Recovery Time Objective (RTO) and Recovery Point Objective (RPO) SLAs are accessible at https://1111systems.com/legal/sla.

11. **11:11 Secure DRaaS for Zerto.** The terms and conditions of this Section 3.11 and, to the extent not inconsistent with this Section 3.11, Section 3.10, are applicable to each Order that includes 11:11 Secure DRaaS for Zerto services, regardless as to whether the Order for public or private cloud services.

    1. **Resources.**

        1. Storage. The types of storage available are Accelerated, and/or SSD Storage purchased by the Customer includes both protected data and Zerto Journal data; Zerto Journal data may not be displayed on the 11:11 Cloud Console, but the Customer is still responsible for paying for this storage and may request a report from the Provider if required. Storage types comprising the environment are specified in the Order.

    2. **Encryption.**

        1. Storage Encryption. Storage is encrypted at rest with AES-256 in XTS cipher mode with FIPS 140-2 approved algorithms.

    3. **Security Features.**

        1. The Provider offers internal and external vulnerability scanning and reporting on the Customer's public Internet facing IPv4 address blocks and presents the information in the 11:11 Cloud Console;

        2. The 11:11 Cloud Console performs the following functions, if enabled, and displays them in reports. In order to enable some features, a software agent may be required to be loaded on the Virtual Machine:

            1. Vulnerability Scanning. Assesses systems, networks and applications for weaknesses and detects known and zero-day attacks. Examines all incoming and outgoing traffic for protocol deviations, policy violations, or content that signals an attack. There are 2 types of scanning available:

                1. Weekly predefined scan and report, and

                2. On-demand scan that generates new reports ad-hoc,

2. Malware Detection. Detects malware, viruses, spyware, trojans, and other malware,
3. Firewall. Bidirectional host-based stateful firewall that audits all traffic incoming and outgoing from the VM,
4. Configuration Auditing. Checks that IT assets are compliant with the Provider's policies and standards,
5. Compliance Reports. Provides logs and data necessary to fulfill audit requirements,
6. Web Application Scanning. Discovers web server and services weaknesses and OWASP vulnerabilities, and
7. Integrity Monitoring. Monitors critical operating system and application files, such as directories, registry keys, and values, to detect and report malicious and unexpected changes in real time; and

3. The information contained within the reports are intended solely to identify threats, vulnerabilities, and statuses of the Cloud environment components, and is provided "as is" without warranty of any kind, express or implied, including but not limited to warranties for fitness of purpose. The Provider does not warrant the completeness of accuracy of the report, nor does it make any recommendations based on the findings noted herein.

12. **11:11 Secure DRaaS Carbonite Availability (formerly known as DoubleTake).** The terms and conditions of this Section 3.12 are applicable to each Order for 11:11 Secure DRaaS with Carbonite Availability. The Customer acknowledges that this product requires that the services listed in Section 3.1 or 3.2 to be deployed in conjunction with it.
    1. **Resources.**
        1. Replication License. Either Physical or Virtual Edition Replication Licenses as described in the Order;
        2. Business Models. Replication licenses are available in a per job Reserved model with two options as described in the Order:
            1. Constant replication, or
            2. Migration only.
    2. **Provider's Obligations.** The Provider is responsible for the following in accordance with industry best practices:
        1. Onboarding the Customer into the Provider's DRaaS with Carbonite Availability service by guiding the Customer through the process of deploying the service;

2. Building target VMs for each server requiring replication with Carbonite Availability;
3. Deploying the Carbonite Availability agent and Carbonite Availability Metered Usage (DTMU) on each target VM for licensing purposes;
4. Deploying a Carbonite Availability management server in the Provider's hosted infrastructure to act as the management console for the customer;
5. Providing the Customer with a URL to download the Carbonite Availability agent and the corresponding license keys;
6. Assisting the Customer in setting up replication jobs utilizing the Carbonite Availability management server;
7. Providing documentation, project management, and demonstrate the DR failover steps to the Customer and successfully test failover;
8. In case of Provider-assisted Failover, assisting the Customer with initiating Failover at-time-of-Disaster; and
9. In the event of a Disaster and Failover to the Recovery Site, the Provider can, if needed, assist the Customer with Failback from Disasters to the Customer's Primary Site for additional i-Tech fees.

3. **Customer's Obligations.** The Customer is responsible for the following in accordance with industry best practices:
    1. Providing the Provider with information reasonably required to fulfill its obligations, including without limitation backup requirement details;
    2. Ensuring that only VMware based workloads are replicated to the Provider and that the Virtual Machine environment matches specifications as defined in the Provider's then-current Product Compatibility Matrix. By purchasing this product, the Customer specifically acknowledges that Hyper-V workloads are not supported;
    3. Downloading and installing the Carbonite Availability agent on each of the source servers that require replication;
    4. Working with the Provider to set up replication jobs utilizing the Carbonite Availability management server;
    5. Unless specified on the Order, implementing dedicated physical or virtual network security appliance and managing Firewall(s) including, but not limited to, the configuration of Network Address Translation (NAT) Access List, Virtual Private Network (VPN), Dynamic Host Configuration Protocol (DHCP), Load Balancing, and static routing;

6. Notifying the Provider before making any changes to the Primary site that might affect the DRaaS service, including any upgrades or patches to Carbonite Availability, the underlying virtualization layer, the replication jobs, or the network. The Customer hereby acknowledges that any such actions could break the ability of the Service to function;
7. Initiating Failover at-time-of-test and at-time-of-Disaster;
8. In case of Provider-assisted Failover, declaring a Disaster via a support ticket;
9. Monitoring available storage in the hosted environment to ensure the Service will continue to function properly;
10. Maintaining operating systems and applications installed on the Customer's Virtual Machines or in the Customer's Virtual Data Center, including, but not limited to, patching, upgrades, updates and anti-virus software;
11. Promptly notifying the Provider if the Cloud Resources are compromised, accessed by a person lacking permission to access the Cloud Resources, or infected with a virus, worm or similar malicious code;
12. Ensuring that there is enough bandwidth at Primary Site to enable initial replication and successive incremental changes of data to Recovery Site;
13. Ensuring that during the term of the Order the Customer maintains enough bandwidth to ensure the continued successful replication of the data. The Customer acknowledges that the Provider is not in breach of the agreement if there is not enough bandwidth available at Primary Site; and
14. If the Customer provisions replication jobs in excess of the specifications set out on the Order, the Customer hereby acknowledges that the Provider is not responsible for any performance degradation or errors caused by over allocation and the Customer may incur in additional costs to cover the additional licenses.

13. **11:11 Flexible Cloud Environment.** The terms and conditions of this Section 3.13 are applicable to each Order that includes 11:11 Flexible Cloud Environment.
    1. **Resources.**
        1. Bare Metal Resources. CPU, RAM, Local Storage, Networking Backplane and Redundant Power comprise the Bare Metal server in the form of a blade or physical appliance as described in the Order;
        2. Licensing. Microsoft and/or Broadcom VMware licensing as described in the Order following the terms and conditions of Section

3.54 (Microsoft Licensing) and Section 3.55 (VMware Licensing) respectively;

3. Virtualization Layer. VMware vSphere for compute virtualization and VMware NSX for network virtualization;

4. Storage Layer. HPE storage arrays provide datastores to VMware for the provisioning of virtual machines; and

5. Business Models. Bare Metal resources and licensing for Microsoft SPLA are available in Reserved model. Software licensing for Broadcom VMware is available in Reserved plus Burst model.

2. **Provider's Obligations.** The Provider is responsible for the following in accordance with industry best practices:

    1. Providing Bare Metal resources and optional software licensing as specified on the relevant Order;

    2. Providing to the Customer vCenter server access to allow provisioning and workload management tasks to complete;

    3. Providing to the Customer, upon request via support ticket, Graphic Console access;

    4. Using commercially reasonable efforts to power on and ensure connectivity to the Bare Metal resources, and additionally VMware services for managed service Customers, before handoff to the Customer;

    5. Using commercially reasonable efforts to provide first and second tier support to ensure the connectivity of the Bare Metal resources; and

    6. For managed service Customers:

        1. Operating the VMware compute and network virtualization layers, and

        2. Applying security patches, and

        3. Yearly upgrades to decimal or major updates to a VMware vSphere and vCenter versions.

3. **Customer’s Obligations.** The Customer is responsible for the following in accordance with industry best practices:

    1. Unless specified on the Order, implementing dedicated physical or virtual network security appliance, managing Firewall(s) including but not limited to the configuration of Network Address Translation (NAT) Access List, Virtual Private Network (VPN), Dynamic Host Configuration Protocol (DHCP), Load Balancing, and static routing;

2. Selecting and securing the appropriate authentication procedures to allow access to the Bare Metal server OS and applications residing in it;

3. Following the Provider's then-current Data Seeding Guidelines if the Customer chooses to seed data;

4. Maintaining operating systems and applications installed on the Bare Metal server(s), including, but not limited to, patching, upgrades, updates and anti-virus software in accordance with industry best practices;

5. Fixing any problems resulting from upgrades to the Bare Metal server operating system;

6. Providing Bare Metal server and application log monitoring;

7. Providing support for operating systems and applications installed on the Bare Metal server(s);

8. Maintaining all backups for all Customer data residing on the Bare Metal servers;

9. If the Customer provisions Reserved Resources in excess of the specifications set out on the Order, the Customer hereby acknowledges that the Provider is not responsible for any performance degradation or errors caused by over allocation.

10. For Customers opting out of VMware as a Service, maintaining operating systems and applications installed on the Bare Metal server(s), including, but not limited to, patching, upgrades, updates and anti-virus software in accordance with industry best practice; and

11. For managed service Customers:

    1. Providing the use case for vCenter server access to allow the Provider to configure the minimum required permissions for vCenter server access aligning with industry best practices.

4. **Risks**

1. Implementation and integration complexity. VMware's advanced virtualization and cloud technologies (such as vSphere, vCenter and NSX) require precise configuration and seamless integration with existing Customer systems. Errors in setup or compatibility issues could disrupt services or degrade performance;

2. Security and compliance. Virtualized environments are prime targets for cyberattacks. Even applying security best practices, misconfigurations or outdated software could lead to security breaches;

3. Service reliability and performance. Downtime or performance hiccups in the VMware infrastructure could disrupt critical Customer workloads, potentially causing financial or operational harm. Overuse of shared resources in a virtualized setup might create bottlenecks, particularly during high-demand periods;

4. Vendor lock-In. Heavy reliance on VMware's ecosystem could limit future flexibility, making it costly or challenging to switch to other virtualization platforms. Shifts in Broadcom's strategy or product offerings (e.g., following VMware's acquisition by Broadcom) might affect service stability or features;

5. Licensing and pricing changes. Broadcom's move to subscription-based licensing or changes driven by Broadcom could raise costs or alter terms, impacting the service's financial model. Non-compliance with licensing rules might lead to penalties or service interruptions;

6. Customer adoption and usage. Customers unfamiliar with VMware's capabilities might underuse the service, reducing its value. Conversely, overuse or improper setup by Customers (especially in self-service scenarios) could strain resources and affect performance;

5. **Assumptions**

1. Customer Infrastructure and Readiness. Customer possesses the required Bare Metal Resources, including compatible hardware and networks, to support VMware deployment. Customers will provide accurate workload details to ensure the service is properly sized and configured;

2. Stable Vendor Relationship. VMware, under Broadcom, will continue supporting and enhancing its products, ensuring the service's long-term viability. The provider's partnerships with VMware and hardware vendors like HPE will remain robust, providing access to updates and support; and

3. Customer Collaboration. Customers will work closely with the provider during deployment, migration, and ongoing management to align the service with their goals. For managed services, Customers will engage in regular reviews to optimize performance and adapt to changing needs.

14. **11:11 Cross Connects.** The terms and conditions of this Section 3.14 are applicable to each Order that includes 11:11 Cross Connect services.

1. **Resources**

1. Cross Connect Resources. Copper or Fiber Cross Connects as described in the Order;

2. Business Models. Colocation resources are available in Reserved Resources model; and

3. The Provider does not include any rack space as part of the Cross Connect service

2. **Provider's Obligations.** The Provider is responsible for the following in accordance with industry best practices:
    1. Patching in the Provider’s side of the cross connect up to the Demarcation Point:
        1. On Cross Connects which media type is fiber, the Provider will supply a single-mode fiber optic patch cable to connect the cross connect to the Provider's switching infrastructure, unless otherwise specified on the Order, or
        2. On Cross Connects which media type is copper, the Provider will supply a 1000Base-LX patch cable to connect the cross connect to the Provider's switching infrastructure; and
    2. Supporting port configurations of 1 GB or 10 GB.
3. **Customer's and/or Carrier’s Obligations.** The Customer is responsible for the following in accordance with industry best practices:
    1. Ensuring that the Carrier has a presence in the specific Provider’s Data Center where the Cross Connect will be deployed as described in the Order. The Carrier’s presence should be within the acceptable range of the media type relative to the Provider’s presence within the Data Center;
    2. Managing the relationship with the Carrier;
    3. Providing the Provider with a signed Letter of Authorization (LOA), using the Carrier’s letterhead, authorizing the Provider and the Data Center to connect the Carrier's Equipment to the cross connect with the following information:
        1. Data Center address,
        2. Authorization excerpts – referencing the Provider to complete the work,
        3. Demarcation location (ports included),
        4. Media type, and
        5. Connector type;
    4. The Customer and the Customer’s Carrier shall be responsible for all circuit provisioning up to the Carrier Demarcation Point. This includes but is not limited to all the necessary access, timelines for completion, installation, and any other relevant items; and
    5. Contacting their Carrier and request that the cross connect be patched in.

15. **11:11 Shared Colocation.** The terms and conditions of this Section 3.15 are applicable to each Order that includes 11:11 Shared Colocation services.
    1. **Resources.**
        1. Colocation Resources. Cabinet or Rack Units, Power, Bandwidth and Networking components comprise the Colocation service as described in the Order; and
        2. Business Models. Colocation resources are available in Reserved model.
    2. **Grant of License.** The Provider hereby grants to the Customer the right to use the Colocation Rack Space for the placement of Provider-Supplied Equipment and/or Customer-Provided Equipment during the term of the Order on the terms and subject to the conditions set out in this Schedule, provided that the Provider retains the right to access the Colocation Rack Space for any legitimate business purpose at any time.
    3. **Provider's Obligations.** The Provider is responsible for the following in accordance with industry best practices:
        1. Use commercially reasonable efforts to prepare any Colocation Rack Space to the relevant Specifications set in the Statement of Work (SOW) and/or the Order on or before the relevant Commencement Date;
        2. Once the Customer provides the tracking information for the Equipment upon shipment, the Provider will alert the Data Center of the shipment to ensure acceptance;
        3. Install the Equipment after it has arrived at the Data Center according to the cabling diagram provided by the Customer;
        4. Using commercially reasonable efforts to power on and ensure connectivity to the Equipment. On Customer-Provided Equipment, issues on the pre-configuration shall result in project timeline delays and the Customer may incur in additional costs to cover the additional time;
        5. The Provider shall not in any case be liable for any type of downtime, connectivity failure, or service interruption and SLA shall not be applied for any of the following:
            1. Full or partial failure in the Customer-Provided Equipment,
            2. Misconfiguration of the Customer-Provided Equipment, and
            3. Failure in any external Customer-Provided Carrier;

6. To the extent legally practicable, assign to the Customer any warranty received by the Provider from the manufacturer of the Provider-Supplied Equipment to allow the Customer to pursue a remedy from such manufacture in respect of defects in the Provider-Supplied Equipment. Other than as set out in the previous sentence, the Provider-Supplied Equipment shall be provided for Customer's use "as is", with all faults and the Provider hereby disclaims all implied warranties including, without limitation, warranties of merchantability, fitness for a specific purpose, and warranties of satisfactory quality in respect of the Provider-Supplied Equipment; and

7. The Provider shall not grant physical access to the Customer into the Data Center. Shall the Customer require physical access to the Equipment, the Provider will coordinate with the Customer and schedule remote hands services to gain physical access.

4. **Customer's Obligations.** The Customer is responsible for the following in accordance with industry best practices:

    1. Ensure that any Customer-Provided Equipment sent out to the Provider is in good working conditions in accordance with prevailing industry standards throughout the term of the relevant Colocation Order such that the Customer-Provided Equipment does not damage any other property within the Colocation Rack Space, Colocation Area or Data Center. The Provider shall have the right to take such actions, without liability under this Schedule, the Agreement or the Colocation Order, as are reasonably necessary to protect property in the Data Center from harm caused by the Customer-Provided Equipment, including without limitation by disconnecting the Equipment, if the Provider in its reasonable discretion believes that the Equipment poses a threat of damage to property within the Data Center;

    2. Ensure that any Customer-Provided Equipment sent out to the Provider is preconfigured with relevant information in such a way that the Customer can access them remotely as they are racked and cabled;

    3. Ensure that the Customer-Provided Equipment does not rely on Wi-Fi or radio frequency (RF) as it is not permitted;

    4. Ensure that the Customer-Provided Equipment supports dual power connected to redundant A+B power circuits. In the event of a power outage, the Provider shall not be liable for any power failure to the Customer-Provided Equipment if such Customer-Provided Equipment does not support redundant power supply or if the Customer does not provide the necessary cables to connect the redundant power supply;

5. Provide a cabling diagram that includes a physical view of each port of the Equipment that needs to be plugged;
6. Ensure that the Customer-Provided Equipment is properly labeled;
7. Provide all the necessary network patch and power cables;
8. Provide the tracking information for the Customer-Provided Equipment upon shipment;
9. In the event that the Customer-Provided Equipment fails:
    1. The Customer is responsible for troubleshooting the Equipment,
    2. The Customer is responsible for applying any warranty with the manufacturer to pursue a remedy from such manufacture in respect of defects in the Customer-Provided Equipment, and
    3. If a replacement is required, the Customer shall be responsible for, but not limited to, the costs and management of the removal, packaging, and logistics of the Customer-Provided Equipment and the corresponding replacement. The Provider shall not be liable for any loss of data or hardware, or damage incurred by the Customer arising out of the Provider's disconnection, removal, or disposal of the Customer-Provided Equipment if the Customer fails to respond after several communication attempts from the Provider. The obligations of this Section 3.14.4 are applicable to the Customer-Provided Equipment that shall act as a replacement and managed under a new Order.
10. In the event that a Colocation Order is terminated, the Customer shall be financially responsible for the disconnection, removal, packaging, logistics, and/or disposal of Customer-Provided Equipment. If the Customer leaves Customer-Provided Equipment in the Provider's Data Center for thirty (30) days after the termination of a Colocation Order, the Provider reserves the right to dispose of any such hardware and shall not be liable to the Customer for any associated loss of data or hardware.

5. **Risks.**

    1. Power. If the Customer does not purchase redundant power or if any of the Customer-Provided Equipment does not support redundant power, the Customer is at risk if a power failure occurs. Provider's best practice recommendation is to purchase redundant power and to utilize the Customer-Provided Equipment that supports redundant power;

2. Rack Mounting. The Equipment cannot be racked back-to-back, such that the rear of two devices is facing each other in the middle of a rack. Only one device shall be used per shelf or unit (U). If the Provider finds that the Customer did not supply the rack-mounting materials, or the Customer-Provided Equipment is not rack-mountable and an additional shelf or tray is needed to securely mount the Equipment to the rack, the Customer shall incur an additional cost to correctly rack the Equipment, and the project timeline may be delayed while additional colocation space is allocated;

3. Shelves. If the Customer uses a shelf and the combined height of the Customer-Provided Equipment and shelf use more than the allotted space, the Customer shall incur an additional cost for additional U(s). The project timeline shall also be delayed while additional colocation space is allocated;

4. Shipping. All Customer-Provided Equipment that is shipped must follow the Provider's Shipping Process and must be handled through the Provider's project manager. This ensures the Provider's ability to effectively track the Equipment to ensure it does not get lost. If the Equipment is shipped without following the Provider's shipping requirements or without the Provider's project managers involvement, the likelihood the Equipment is lost is increased;

5. Reject Equipment. Provider reserves the right to reject any Customer-Provided Equipment that appears unsafe. In this event, the Customer-Provided Equipment will be shipped back to Customer and the project timeline shall be delayed while new hardware is shipped or a new solution is devised;

6. Equipment Size. If the Customer-Provided Equipment is larger than the space allocated, Provider shall increase the monthly cost, and the project timeline may be delayed while additional colocation space is allocated;

7. Required Cables. It is the Customer's responsibility to ship the Customer-Provided Equipment with all required cables and to test the cables prior to shipping, ensuring they work as intended. If the Equipment is shipped with missing or defective cables, Customer shall be charged for the required cables and the corresponding Provider's i-Tech fee for any additional time required to install the cables, and the project timeline shall be delayed; and

8. Shipping Materials. All shipping and packaging materials are destroyed once equipment arrives at the Data Center. The Provider will not return any boxes, manuals, packing materials, or any other items that are shipped.

6. **Storage of Equipment.** Following the request of the Customer, the Provider may, at its option, store Customer-Provided Equipment that the Customer

intends to collocate in the Colocation Rack for not more than five days prior to the Commencement Date as a courtesy incidental to the license granted to the Customer by the Provider under this Schedule. The Provider will not charge the Customer a fee for such storage. Absent the Provider's gross negligence or intentional misconduct, the Provider shall have no liability to the Customer or any third-party arising from such storage services. If the Customer stores Customer-Provided Equipment for longer than ten days, the Provider may, but shall not be obligated to, return the Customer's equipment to the Customer without liability, at the Customer's sole cost and expense.

7. **Changes.** The Provider reserves the right to change from time to time, and at the Provider's cost, the location or configuration of the Colocation Rack Space in which the Customer-Provided Equipment and/or the Provider-Supplied Equipment is located, provided that the Provider shall not arbitrarily require such changes. The Provider and the Customer shall work in good faith to minimize any disruption in the Customer's services that may be caused by such changes in location or configuration of the Colocation Rack Space.

16. **11:11 Dedicated Colocation.** The terms and conditions of this Section 3.16 are applicable to each Order that includes 11:11 Dedicated Colocation services and are accessible at https://1111systems.com/legal/1111-colocation-service-terms/

17. **Multi-Cloud Connect (formerly known as Zipline)**. The terms and conditions of this Section 3.17 are applicable to each Order that includes 11:11 Multi-Cloud Connect services.

    1. **Resources.**

        1. Multi-Cloud Connect Resources. Bandwidth, access to the elastic interconnection fabric based on a Software Defined Network, and a shared physical Cross Connect in the Provider's Data Center comprise the Multi-Cloud Connect connection as described in the Order; and

        2. Business Models. Multi-Cloud Connect resources are available in a Reserved model.

    2. **Provider's Obligations.**

        1. Patching in the Provider’s side of the Cross Connect up to the Demarcation Point;

        2. Creating and maintaining a subscription to the elastic interconnection fabric based on a Software Defined Network service;

3. Creating and maintaining the required number of virtual Cross Connects to support Multi-Cloud Connect connectivity as defined in the Order;

4. Using commercially reasonable efforts to provide first and second tier support to ensure the performance and connectivity of the Multi-Cloud Connect resources; and

5. Escalating support request(s) on the Customer's behalf for tier 3 support, if performance or connectivity issues are determined to be on the Provider's side.

18. **11:11 Secure Cloud Backup for Microsoft 365.** The terms and conditions of this Section 3.18 are applicable to each Order that includes 11:11 Secure Cloud Backup for Microsoft 365 services. The terms Office 365 and Microsoft 365 can be used interchangeably as they refer to the same service.

    1. **Resources.**

        1. Storage and Bandwidth. The Cloud Resources that comprise the Secure Cloud Backup for Microsoft 365 service include unlimited shared storage per user account along with embedded unlimited incoming and outgoing network bandwidth used for backup purposes;

        2. Licensing. Veeam Backup for Microsoft Office 365 licensing is included in the service on the Provider's site, unless explicitly specified in the Order;

        3. Business Models. All subscription licenses are sold per user account in a Reserved plus Burst model as described in the Order according to the minimum license commitment and incremental guidelines specified by the Provider; and

        4. Secondary Copies. In addition to the standard subscription licenses, Customers could opt in for secondary copies of the data as described in the Order. Where applicable, location pairings between primary and secondary copies can be found in the Success Center article available at https://success.1111systems.com/article/xUJlTC. This service feature is only available for service subscription Item Numbers and/or Data Centers identified in the Order with the reference “PC1”.

    2. **Provider's Obligations.** The Provider is responsible for the following in accordance with industry best practices:

        1. Providing a user-based cloud backup service comprised of cloud storage, Veeam Backup for Microsoft Office 365 licensing, unless explicitly specified in the Order and network bandwidth at the Provider's Site to store Microsoft 365 data per user account as specified in the Order;

2. Maintaining the Provider's Cloud Storage infrastructure including patching, upgrades and updates;
3. Providing the Customer the URL and authentication credentials to access the Microsoft 365 user's data via the Veeam Explorer applications through Veeam Cloud Connect;
4. During initial setup, assisting the Customer in creating an inclusion and exclusion groups that can be used in the backup jobs to manage user license counts;
5. Backing up Exchange Online mailbox items (email, calendar and contacts), as well as OneDrive for Business, SharePoint Online files and folders, and Teams data on the Microsoft 365 organization that hosts the licensed Microsoft 365 user accounts for, as specified by the Customer, either (a) the entire Microsoft 365 organization, or (b) a subset of Microsoft 365 users via an Active Directory security group. Each Microsoft 365 user account consist of the following objects:
    1. A personal mailbox,
    2. An online Archive mailbox,
    3. OneDrive documents,
    4. Personal SharePoint sites, and
    5. Teams data;
6. Backing up Microsoft 365 items for shared and group mailboxes, group SharePoint sites, as well as user objects that do not have a Microsoft 365 license applied, without requiring an 11:11 Secure Cloud Backup for Microsoft 365 license, as specified by the Customer;
7. The Provider considers licensed users based on the requirements by object type as described in the Success Center article accessible at https://success.1111systems.com/article/YPXbCN. The Customer can designate specific user accounts for deletion from backups from the Provider’s infrastructure; once all backups have been deleted for an account designated for deletion, the licenses associated with such deleted accounts can be reassigned by the Customer.
8. During initial setup, configuring and performing backups, that shall occur at least once a day;
9. Retaining backups while a Veeam Backup for Microsoft Office 365 license is assigned to a Microsoft 365 user according to the Customer's required retention policy during onboarding, for the primary and secondary copies, if applicable, and such retention policy will not affect the price specified in the Order. Shall the Customer require immutability for the secondary copy, its retention

shall be linked directly to the retention policy since they are the same; and

10. Providing the following recovery options to the Customer:
    1. Restoring Organization Mailbox, OneDrive, SharePoint, or Teams data,
    2. Exporting Exchange mailbox objects to a PST file,
    3. Saving Exchange email items as a Microsoft Exchange Mail Document (.msg) file,
    4. Saving items as HyperText Markup Language (.html) files,
    5. Sending items as attachments to specified recipients, and
    6. Saving OneDrive, SharePoint, or Teams files and folders as a ZIP file.

3. **Customer's Obligations.** The Customer is responsible for the following in accordance with industry best practices:
    1. Providing a list of either (a) the entire Microsoft 365 organization's users, or (b) a subset of Microsoft 365 users via an Active Directory security group in addition to a list of Group SharePoint sites, and/or a list of Teams' teams that are to be protected by the Provider with 11:11 Secure Cloud Backup for Microsoft 365 licenses. If the Customer provides a subset of Microsoft 365 users in accordance with part (b) of the preceding sentence, the Customer shall be responsible for any charges associated to the mailboxes, documents, sites, and/or items selected explicitly or implicitly under the security group;
    2. Providing the Provider with information reasonably required to fulfill its obligations, including, but not limited to, the Microsoft 365 organization name that contains the user accounts to back up, and a Microsoft 365 account with the following criteria and rights:
        1. An account that belongs to the Microsoft 365 organization that shall be backed up. Having a mailbox in that organization is optional,
        2. Role Management role. To grant ApplicationImpersonation role,
        3. ApplicationImpersonation role. To allow this role assignment, the account must be granted the Organization Management permission,
        4. Organizations Configuration role. To manage role assignments,

5. View-Only Configuration role. To obtain the necessary organization configuration parameters,
6. View-Only Recipients role. To view mailbox recipients (required for job creation),
7. MailboxSearch or MailRecipients. To backup groups,
8. Global Administrator role, or the SharePoint Administrator role. To connect to the Microsoft SharePoint organization,
9. This account may optionally use modern authentication including app ID, client secret and app password, and
10. Or this account may optionally use modern application authentication which will automatically configure the proper roles needed to connect to the service;

3. Procuring, implementing, and configuring of the correct licensed versions of Microsoft 365;
4. Procuring, implementing, and configuring an appropriate method of payment against the customer's Azure subscription to support any additional costs incurred by accessing data through Microsoft Graph API calls. Microsoft Teams channel chat data will include an additional charge imposed and collected by Microsoft. For more information, please review our Success Center article available at https://success.1111systems.com/article/KcGTRO;
5. Ensuring the functionality of Microsoft 365 services and contacting Microsoft, or the Microsoft 365 reseller, for any type of support related to the Microsoft 365 service as the Provider is not responsible for this service including, but not limited to, performance, malfunction, or downtime;
6. During initial setup, informing the Provider if Teams channel chats are required to be backed up, as those are not backed up by default;
7. During initial setup, informing the Provider about the retention policy, and, when applicable, immutability;
8. Utilizing its own Microsoft 365 credentials, with the appropriate administration and impersonation permissions, to access the organization's data backups via the Veeam Explorer applications through Veeam Cloud Connect. This account shall use modern application authentication;
9. Configuring and performing self-service recovery tasks based on the recovery options listed by the Provider;
10. Promptly notifying the Provider if the Microsoft 365 service has been hacked, accessed by a person lacking permission to access the Microsoft 365 and/or the Microsoft 365 cloud backups stored at the Provider's site, or infected with a virus, worm or similar code;

11. Informing the Provider when a retention policy change needs to be made, except when immutability is present, since retention period and immutability period are the same, and cannot be changed once set;

12. Unless immutability is present, removing specific user accounts from backups and purging the user accounts from the Provider's infrastructure, so that the licenses associated with such deleted accounts can be revoked and potentially reassigned in order for the Customer to avoid incurring Burst charges for the then-current month. The Customer shall reduce license count prior to the end of the month or the Customer will be responsible for any applicable Burst Resource charges incurred for the then-current month;

13. Sorting specific user accounts into inclusion or exclusion groups as appropriate to manage licenses and prevent exceeding the contracted license count;

14. Monitoring daily service summary e-mails which may include information about backup job failures;

15. Rectifying any job failures related to something outside of the Providers control, which shall include, but not be limited to, credentials issues for accessing Microsoft 365. The Customer may contact the Provider for assistance in rectifying backup job failures; and

16. Updating existing backup job(s) or creating new ones subsequent to the initial setup.

4. **Risks.**

    1. Redundant Backups. If the Customer is running multiple backups of their Microsoft 365 environment, either on-prem or with another cloud provider, the Customer acknowledges that there could be performance and/or data loss situations. These situations arise due to connectivity restrictions and rate limiting throttling that is set outside of the Provider's control.

5. **Immutability.**

    1. This service feature is only available for service subscription Item Numbers and/or Data Centers identified in the Order with the reference "PC1";

    2. By configuring immutability on backup jobs, data stored by such jobs won't be susceptible to alteration or deletion by neither the Customer nor the Provider during its retention period. The exception would be applicable only when the Customer wishes to stop consuming the services under this Section 3.18, by cancelling the corresponding Order, resulting in the removal of the entire Customer data associated to these services;

3. Immutability is optional and shall be configured during the initial setup as requested by the Customer. Immutability shall only be applicable to secondary copies;

4. The immutability period is determined by the retention period, which is linked to the retention period. Once it is set, it cannot be changed, or removed;

5. Unlimited retention for data that has been configured to be immutable is not supported; and

6. The ability to delete and purge users or data when immutability is present is not supported as it defeats the purpose.

19. **11:11 Cloud Object Storage.** The terms and conditions of this Section 3.19 are applicable to each Order that includes 11:11 Cloud Object Storage services.

    1. **Resources.**

        1. Storage, bandwidth, operations, and fees on objects. The Cloud Resources that comprise the Cloud Object Storage service include shared storage along with embedded unlimited incoming and outgoing network bandwidth and unlimited operations on objects as described in the Order but shall be subject to Sections 3.19.5 and 3.19.6 below. Storage is represented in gibibytes (GiB), defined by the International Electrotechnical Commission (IEC) where 1 GiB is 2^30 bytes. Other representations may be found in different systems but shall refer to the same base2 unit, for example binary gigabytes (GB). Similarly, 1 TiB is 2^40 bytes, i.e. 1024 GiB; and

        2. Business Model. Object Storage is available in a Reserved model, except for service subscription Item Numbers and/or Data Centers identified in the Order with the reference “PC1” where the model is Reserved plus Burst for the Standard Infrequent Access class plus a burst component on all non-contracted usage for operation costs and non-reserved storage classes.

    2. **Provider’s Obligations.**

        1. Providing Cloud Storage and network bandwidth at Target Site as per specifications detailed in the Order;

        2. Maintaining Target Site Cloud Storage infrastructure including patching, upgrades and updates;

        3. Creating Cloud Resources as per specifications detailed in the Order;

        4. Providing Customer the initial URL and Object Storage Access Credentials to access the Customer’s Cloud Resources upon completion of the Order;

        5. Providing storage modification options to the Order as required by the Customer;

6. Providing an industry-standard method of protecting, either through replication or erasure coding, of Customer data uploaded to the Provider's Cloud Object Storage at the Data Center described by the Order. For service subscription Item Numbers and/or Data Centers identified in the Order with the reference “PC1”, data stored in any S3 storage class, except for the S3 One Zone Infrequent Access class, is always stored across a minimum of three Availability Zones; and

7. Non-Contracted burst charges. For service subscription item Numbers and/or Data Centers identified in the Order with the reference “PC1”, Non-Contracted burst charges are based on AWS’ then current rates and are subject to change. Rate changes take effect on the 1st day of the calendar month in which the change was made. These charges will be reflected on your invoice as BLEND and/or DT (Data Transfer) burst costs.

3. **Customer’s Obligations.** The Customer is responsible for the following in accordance with industry best practices:

    1. Management and creation of all data stored and consumed on the Provider’s Cloud Object Storage;

    2. Consuming only the resources reserved as described in the Order;

    3. Verifying and adhering to all S3-compatibility requirements for all third-party applications or client software used to connect, store and consume the Customer's data on the Provider’s Cloud Object Storage;

    4. Installation, version control, patching and updates on all third-party applications or client software used to connect, store and consume the Customer's data on the Provider’s Cloud Object Storage;

    5. Creating and managing of all subsequent security rights, access controls, S3-credentials and retention policies for the Customer's data stored and consumed on the Provider’s Cloud Object Storage once the Customer has been provided initial URL and Object Storage Access Credentials from the Provider. For service subscription Item Numbers and/or Data Centers identified in the Order with the reference “PC1”, the Customer can request additional credentials to be generated by the Provider's Support team;

    6. Performance response of any and all third-party applications used to connect, store and consume the Customer's data on the Provider's Cloud Object Storage;

    7. Tracking and maintaining all Object Storage Access Credentials used to store and consume the Customer's data on the Provider’s Cloud Object Storage;

    8. Encrypt and maintain encryption keys for any data uploaded to the Provider’s Cloud Object Storage; and

9. If available, understanding the implications that enabling immutability and data versioning might impact the total consumed storage.

4. **Service Support.**

    1. Storage Encryption. All Cloud Object Storage support for clients is provided as "best effort" as there are many clients that all implement Object Storage functionality in different ways. The Provider can demonstrate functionality with known clients, but individual implementations may vary.

5. **Data Egress.**

    1. Data egress, from an acceptable use policy perspective, is comprised of two components: Data Retrieval API calls and Data Transfer out to the Internet;

    2. For service subscription Item Numbers and/or Data Centers identified in the Order with the reference "PC1" and S3 Standard Infrequent Access class, data egress charges are included if usage patterns are deemed reasonable for the service offering. Reasonable data egress shall mean allowed egress of up to 50% of the highest of contracted or total stored data, measured in GB per month per region, within the Customer account;

    3. If the Provider determines (in its sole discretion) that the Customer has exceeded the reasonable usage of data egress, the Provider will (1) notify the Customer of such usage and (2) advise the Customer to upgrade its Order to reflect the additional usage. If the Provider advises the Customer to upgrade its Order in the preceding sentence and the Customer does not upgrade its Order within 30 days after receiving that notice, the Provider reserves the right to charge for any data egress exceeding the reasonable data egress standard above. The Customer agrees to pay any invoices or charges for any additional data egress allowed under this Section; and

    4. For all other S3 storage classes, data egress usage shall be charged at the current rate found in the Provider's Account Management Application.

6. **API Requests.**

    1. For service subscription Item Numbers and/or Data Centers identified in the Order with the reference "PC1", some API requests charges are included in the 11:11 Object Storage service if usage patterns are deemed reasonable for the service offering. These thresholds would use the highest of contracted or total S3 Standard Infrequent Access class storage usage as the determining factor;

    2. Exclusively for S3 Standard Infrequent Access class, reasonable API requests shall mean the following:

1. PUT/COPY/POST/LIST requests <= 1,100 per GB per month per region, and
2. GET/SELECT requests <= 300 per GB per month per region;

3. Exclusively for S3 Standard class, reasonable API requests shall mean the following:
    1. PUT/COPY/POST/LIST requests <= 2,200 per GB per month per region;
4. If the Provider determines (in its sole discretion) that the Customer has exceeded the reasonable usage of API requests, the Provider will (1) notify the Customer of such usage and (2) advise the Customer to upgrade its Order in to reflect the additional usage. If the Provider advises the Customer to upgrade its Order in the preceding sentence and the Customer does not upgrade its Order within 30 days after receiving that notice, the Provider reserves the right to charge for any API requests usage exceeding the predefined limits defined above. The Customer agrees to pay any invoices or charges for any additional API requests allowed under this Section; and
5. For all other request types and/or S3 storage classes, API requests usage shall be charged at the current rate found in the Provider's Account Management Application.

7. **Minimum Object Size.**
    1. For service subscription Item Numbers and/or Data Centers identified in the Order with the reference "PC1", S3 Standard Infrequent Access, S3 One Zone Infrequent Access, and Glacier Instant Retrieval classes have a minimum billable object size of 128 KB. Smaller objects may be stored but will be considered as 128 KB of storage at the appropriate small object storage class rate. Small objects under the S3 Standard Infrequent Access class, will be tracked as part of the contracted quota, although they won't contribute to the API Requests or Data Egress thresholds defined above.
8. **Data Retention.**
    1. For service subscription Item Numbers and/or Data Centers identified in the Order with the reference "PC1", S3 Standard Infrequent Access and S3 One Zone Infrequent Access classes shall be charged for a minimum storage duration of 30 days. Objects that are deleted, overwritten, or transitioned to a different storage class before 30 days will incur the normal storage usage charge plus a pro-rated charge for the remainder of the 30-day minimum, and they will be tracked as part of the contracted quota, although they won't contribute to the API Requests or Data Egress thresholds defined above.

9. **Service operations.**

    1. For service subscription Item Numbers and/or Data Centers identified in the Order with the reference “PC1”, permissions to modify resources shall be limited to s3:*, except for s3:CreateBucket, which is restricted to the region where the service subscription has been procured. All other AWS operations are restricted.

20. **Veeam Licensing.** The terms and conditions of this Section 3.20 are applicable to each Order that includes Veeam Licensing.

    1. **Resources.**

        1. License Key. A digital key that defines the scope of the license, terms and options for Agent, Backup & Replication Edition, Veeam Backup for Microsoft 365, Veeam Recovery Orchestrator, or Veeam ONE rental licenses as described in the Order. The license unit options are:

            1. VM. A protected Virtual Machine that is backed up, replicated, copied or otherwise consumed by the software,

            2. Server. A physical or virtual host, that contains an application or applications that serves one or more client workstations, where the software is installed. Each node of a clustered setup needs to be licensed separately,

            3. Workstation. A physical or virtual host, typically used as a personal computer, where the software is installed. Each node of the clustered setup needs to be licensed separately,

            4. Unstructured data. Unstructured data backup, typically NAS, File to Tape or Object Storage data is licensed in increments of 500GB. Each 500GB of data protected requires one Unstructured Data license,

            5. Plug-ins for Enterprise Applications. An enterprise application as defined by and supported by Veeam Plug-ins. Typically additional integration with enterprise applications like database applications. Each Application Server must be licensed separately,

            6. Public Cloud Workloads. Backup for supported public cloud Virtual Machine, Database and File Server workloads. Each workload must be licensed separately,

            7. Veeam ONE. Monitored workloads including Veeam Backup and Replication and VMware vSphere virtual infrastructure. Each monitored workload must be licensed separately,

            8. Veeam Backup for Microsoft 365. A protected Microsoft 365 user that has one or more of its Exchange Online, OneDrive, SharePoint or Teams resources backed up, or

9. Veeam Recovery Orchestrator. A Virtual Machine that is protected by and forms part of a Veeam Recovery Orchestrator recovery plan.

2. **Provider's Obligations.** The Provider is responsible for the following in accordance with industry best practices:

    1. Creating and deleting the corresponding Veeam Cloud Connect Tenant(s) that links the license key(s) to specific Customer(s);

    2. Provide the security credentials to the Customer for pairing with the Provider's cloud infrastructure for delivery of the license key(s);

    3. Procuring the license key(s) associated to the Veeam products as described in the Order;

    4. Maintaining the cloud infrastructure needed to deliver the Veeam licenses to the Customer; and

    5. Troubleshooting and Supporting issues related to both the procured Veeam license and the corresponding Veeam software using it. Provider shall not troubleshoot or support issues related to other licenses not procured by the Provider, including, but not limited to, Evaluation, "Not for Resale", Free, and Community Licenses.

3. **Customer's Obligations.** The Customer is responsible for the following in accordance with industry best practices:

    1. Verifying the system requirements for both hardware and software compatible with Veeam's compatibility matrix available at www.veeam.com;

    2. Installing and updating the Veeam software on the corresponding workstations, servers, or Virtual Machines;

    3. Pairing the Veeam Agent(s), Backup & Replication server(s), Veeam ONE, Veeam Backup for Microsoft 365, and/or Veeam Recovery orchestrator Servers to the Provider in order to receive and maintain the license key(s);

    4. Managing and monitoring any alarms, reports, audits, and logs generated by the Veeam software and its configuration;

    5. Providing the information to the Provider necessary for troubleshooting the Veeam license and the corresponding Veeam software using it; and

    6. Except for Evaluation, "Not for Resale", Free, and Community Licenses, adhering to Veeam's End User License Agreement (EULA) found at https://www.veeam.com/eula.html

21. **11:11 Autopilot Managed Recovery for DRaaS.** The terms and conditions of this Section 3.21 are applicable to each Order that includes 11:11 Autopilot Managed Recovery for DRaaS in combination with 11:11 Secure DRaaS.

1. **Assets & Deliverables.**

    1. Connectivity Design Documentation. Technical documents and/or diagrams providing engineering level information and configuration details for the purpose of interconnecting the Customer's Primary Site(s) to the designated Provider's Recovery Site(s) delivering the DRaaS service capabilities;

    2. On-boarding Project Plan A documented detailed overview of all tasks associated with the Provider on-boarding process for interconnectivity and delivery of the services protecting Workloads replicated from the Customer's Primary Site(s) Workloads within scope of the mutually agreed upon service contract. The purpose of this document is to track ownership, progress and completion of all applicable on-boarding tasks in collaboration between the Customer and the Provider;

    3. On-boarding Provisioning Form. A detailed discovery document used for information gathering and collection of all Customer specific technical and infrastructure related information for the sole purpose of the Provider providing the onboarding service, integration, and management services to the Customer as part of the Secure DRaaS service contract;

    4. Recovery Action Plan. A disaster recovery process document providing enhanced details for all steps and tasks required for proper failover or failback of the Customer's replicated Workloads to the designated Provider's Recovery Site(s). Additional details include task ownership, estimated/actual task duration times, and Customer's specific and managed application acceptance criteria testing processes. This document is developed and managed in collaboration between the Customer and the Provider; and

    5. Recovery Service Guide. A process document providing a business level view of the DRaaS solution. Key content includes general service description, service capabilities, the Customer's Primary Site(s) and the designated Provider's Recovery Site(s) location information, recoverable application service catalog, protected workload inventories, and failover process overview with key metrics (RTO / RPO).

2. **On-boarding Project Management.**

    1. Project managers. Both the Provider and the Customer shall appoint a project manager each who will serve as the primary contact point; and

    2. On-boarding Project Management Engagement. The Provider's project manager and the Customer's project manager shall meet as required for the duration of the on-boarding process for the purpose of facilitating a successful relationship and overseeing the

implementation of all Cloud Resources and services outlined in the Order and the On-boarding Provisioning Form, including but not limited to, (a) tracking the progress of the on-boarding and implementation process and all associated tasks; (b) reviewing other current or future projects or business plans that may impact the onboarding of the Cloud Resources and services, (c) Weekly status reports to review the Provider's performance in execution of the on-boarding project for delivery of all Cloud Resources and services, (d) coordinating and planning for any new equipment or software acquisitions specific to supporting the completion of on-boarding all Cloud Resources and services.

3. **On-Boarding Acceptance Test.**

    1. The On-Boarding Acceptance Test consists of non-service impacting Failover Test operation performed by Provider, as well as Application Testing and Verification performed by Customer. Fully committed Failover and Failback are not supported. The Test does not include modification of Primary Site resources including Virtual Machines and networking;

    2. The On-Boarding Acceptance Test is performed during the Provider's normal business hours of Monday-Friday 8:00 am – 5:00 pm with the time zone being based on data center location where services are located;

    3. Onboarding Acceptance Test Scheduling. Upon completion of the on-boarding project tasks required for implementing the Cloud Resources within the scope identified in the Onboarding Provisioning Form, the Customer will be notified and will have fourteen (14) days from the day of notice in which to schedule a final On-Boarding Acceptance Test;

    4. On-Boarding Acceptance Test Success Criteria. Successful completion of the On-boarding Acceptance Test shall be determined by validation of the Provider's ability to meet the RTO agreed during the planning phase of the onboarding project. The Target Objectives will be documented in the Recovery Action Plan and Recovery Service Guide. In the event that the On-Boarding Acceptance Test exceeds the RTO agreed in the planning phase, the Customer agrees to provide the Provider with any data or information reasonably requested by the Provider in order to enable the Provider to diagnose and resolve any problems associated with any failure to meet that RTO in the On-Boarding Acceptance Testing. The Provider project manager will notify the Customer via email or phone upon resolution of any such issues. After the Provider has notified the Customer that the problem has been resolved, the Customer and the Provider will promptly conduct a follow-up On-Boarding Acceptance Test to validate that the RTO with such follow-up test no longer exceeds the RTO provided in the original the On-Boarding

Acceptance Test. This process will continue, if necessary, until the On-Boarding Acceptance Test Criteria meets the required success criteria. Notwithstanding anything to the contrary in this Service Schedule, if the Customer fails to respond to the On-Boarding Acceptance Test reschedule notice within fourteen (14) days of the date of notification, then the Provider shall consider the on-boarding completed and will have no further obligations to the Customer in regard to the On-Boarding Acceptance Test. Under these circumstances in which the Provider deems on-boarding completion due to failure of response by the Customer, the Customer shall reserve the right to exercise unlimited self-service testing or the allocated (2) Recovery Test per 12-months as outlined in Section 1.5 of the Autopilot Managed Recovery for DRaaS SLA for completion of the On-Boarding Acceptance Testing; and

5. On-boarding Acceptance Test Failure. Failure of the Onboarding Acceptance Testing shall be defined as the inability for the Provider to meet the RTO SLA target objectives as outlined in Section 1.2.1 of the Autopilot Managed Recovery for DRaaS SLA. The Customer agrees to provide the Provider with any data or information reasonably requested by the Provider in order to enable the Provider to diagnose and resolve any problems associated with a failure in the On-boarding Acceptance Testing. The Provider project manager will notify the Customer via email or phone upon resolution of any such issues. After the Provider has notified the Customer that the problem has been resolved, the Customer and the Provider will promptly conduct a follow-up On-boarding Acceptance Test to validate that all test criteria associated with the On-boarding Acceptance Test have now been met. This process will continue, if necessary, until the On-boarding Acceptance Test Criteria meets the required success criteria. Notwithstanding anything to the contrary in this Service Schedule, if the Customer fails to respond to the On-boarding Acceptance Test reschedule notice within fourteen (14) days of the date of notification, then the Provider shall consider the on-boarding completed and will have no further obligations to the Customer in regard to the On-boarding Acceptance Test. Under these circumstances in which the Provider deems on-boarding completion due to failure of response by the Customer, the Customer shall reserve the right to exercise unlimited self-service testing, where self service is available, or the allocated (2) Recovery Test per 12-months as outlined in Section 1.5 of the Autopilot Managed Recovery for DRaaS SLA for completion of the Onboarding Acceptance Testing.

4. **Service Delivery Management.**

    1. Service Delivery Management Contacts. The Customer shall appoint an individual who will serve as the primary contact point for the Provider in connection with ongoing lifecycle management and

delivery of the services (the “Customer Primary Contact”), and the Provider shall appoint a project manager (the “Enterprise Solutions Manager”); and

2. Service Delivery Management Engagement. The Provider and the appointed Customer's project contact shall meet as required during the term of each service for the purpose of facilitating a successful relationship and overseeing the delivery and performance of each service, including but not limited to, (a) tracking the progress of the on-boarding and implementation process and all associated tasks, (b) reviewing other current or future projects or business plans that may impact all services and/or delivery of all services, (c) reviewing the Provider’s performance in the delivery of the service levels set forth in the Service Level Agreement, (d) coordinating and planning for any new equipment or software acquisitions or needs, (e) reviewing strategic and tactical decisions for the Customer in respect of the establishment, budgeting and implementation of the Customer’s priorities and plans for information technology that may impact services and/or delivery of all services, (f) monitoring and resolving concerns that may arise regarding the provision of all services, this SLA and/or the Service Schedule;

5. **Provider’s Obligations.** The Provider is responsible for the following in accordance with industry best-practices:

    1. Providing enhanced onboarding project management deliverables, to include:

        1. Weekly status call between the Provider on-boarding personnel and applicable Customer's contacts, and

        2. Weekly status report summarizing project tasks progress, project milestones, estimated and actual durations/completion dates and critical path items;

    2. Providing and managing all supporting Service documentation to include:

        1. Documented inventory and workload specifications (e.g. compute, storage, networking) of all Workloads within scope of the Order,

        2. Documented L2/L3 network design for compatibility and integration between the Customer Primary Site(s) and 11:11 Secure DRaaS networking services and design guidelines, and

        3. Documented Customer network security configurations, including firewall security policies, NAT policies and network security segmentation design;

3. Providing full installation, configuration and ongoing management of all services components required for delivery of 11:11 Secure DRaaS, to include;
    1. Replication software installation, setup and configuration both in the Customer's premises and the Provider’s cloud data center environments (where applicable),
    2. Setup and configuration of VPN connections (where applicable),
    3. Setup and configuration of all the Provider's side networking components support dedicated circuits for WAN connectivity (where applicable), and
    4. Setup & configuration of any cross-connects to support networking connectivity in accordance with Section 3.14 of this Service Schedule;
4. Providing full setup and configuration for replication of the Recovery Groups for all Workloads within scope and applicable to the Order and the Onboarding Provisioning Form;
5. Providing full assistance with development and creation of the Customer’s Disaster Recovery Runbook(s) within the 11:11 Cloud Console (where applicable);
6. Providing full assistance with development and creation of the Customer’s Recovery Activation Plan;
7. Providing managed failover testing and live failover/fallback declaration events. Managed failback operations are only provided for live declaration events when required;
8. Providing a completed Recovery Service Guide at the completion of the on-boarding process and manage all ongoing updates;
9. Fulfilling Customer requests for new Recovery Groups, increased capacity, VPN connections, and other change requests; and
10. Providing ongoing updates, patching and maintenance for all the Provider provided service components required for delivery of the 11:11 Secure DRaaS, to include:
    1. Replication software, and
    2. Network virtual appliances sold and provided on the Order.

6. **Customer’s Obligations.** The Customer is responsible for the following in accordance with Provider’s delivery of the Autopilot Managed Recovery for DRaaS and industry best-practices:
    1. Ensure all Customer-owned software, applications, devices, systems, processes, and services that maintain Customer Data to be

protected by the services delivered as part of this Agreement are covered as specified under Section 2.3.5 of this Service Schedule for the purposes of fulfilling this Agreement;

2. Where applicable, the Customer shall maintain all firmware or software updates to all Customer-owned hardware, software, applications, devices, and systems in use with or protected by Cloud Resources provided by the Provider;

3. Where applicable, contact all software, application, device, system, service, and service providers covered under this Agreement and add the appropriate Provider's personnel as approved contacts for the purposes of fulfilling this Service Schedule;

4. Complete the On-boarding Provisioning Form provided by the Provider;

5. Provide all current and existing documentation of the Customer Primary Site(s) to include; environment "as-built" documentation, application contact information, application dependencies, current backup strategy, and disaster recovery plans if applicable;

6. Provide the Provider's personnel with the Customer's asset discovery and documentation where applicable;

7. Where applicable; provide all current process documentation in support of the services outlined in this Agreement and provide all assistance necessary to modify existing or implement new processes to streamline the delivery of services;

8. Where applicable, the Customer shall maintain all software and other devices or items provided to the Customer by the Provider located within the Customer's Primary Site(s) in direct support of the delivery of Cloud Resources outlined in the Order (the "Equipment') in good working order and in accordance with applicable manufacturers' specifications. The Customer shall notify the Provider immediately upon determination that any Equipment is not in compliance with the foregoing, or is in material breach of the terms and conditions set forth in this Service Schedule; and

9. The Customer shall cooperate with the Provider with regard to the performance of the Provider's obligations hereunder, including (without limitation):

    1. Providing the Provider with the required remote access to the Customer's Equipment, as may be reasonable to permit Provider to perform its obligations hereunder, and

    2. Notifying the Provider of any changes to its configurations that could potentially impact the services.

7. **Service Levels.** All applicable SLAs are defined in the Autopilot Managed Recovery for DRaaS Service Level Agreement.

22. **11:11 Network Support.** The terms and conditions of this Section 3.22 are applicable to each Order that includes both the Provider's Network Support and at least one of the Providers services that are identified in Section 3.1, Section 3.2, Section 3.8, Section 3.9, Section 3.10, and Section 3.11 of this Schedule, regardless as to whether the Order is for public or private cloud services.

    1. **Assets & Deliverables.**

        1. On-boarding Provisioning Form. A documented overview of the network details associated with the Provider's network on-boarding process for delivery of the Network Support within scope of the mutually agreed upon SOW. The purpose of this document is to document applicable on-boarding network details in collaboration between the Customer and the Provider; and

        2. Network Diagram. Technical diagrams providing engineering level information and configuration details for the purpose of detailing network connectivity within the Provider Site(s) delivering the service capabilities to the Customer within scope of the mutually agreed upon SOW.

    2. **Provider's Obligations.** The Provider is responsible for the following in accordance with industry best-practices:

        1. Providing and managing all supporting service documentation to include:

            1. Documented L2/L3 network details within the Provider's networking services and design guidelines;

        2. Providing full installation and configuration of virtual network components, as described in the Network Support components on the Order, to include:

            1. Setup, licensing and configuration of virtual network device(s), and

            2. Setup, licensing and configuration is limited to no more than 5 hours in aggregate to plan, implement and test; and

        3. Ongoing support of virtual network components, as described in the Order, to include technical support as initiated by the Customer for routine configuration changes and basic troubleshooting activities; and

        4. Individual support activities which take the Provider more than two hours to plan and execute are out of scope for this service and are considered projects. Project work will require a separate SOW and may result in additional fees.

    3. **Customer's Obligations.** The Customer is responsible for the following in accordance with Provider's delivery of the 11:11 Network Support and industry best-practices:

1. The Customer shall complete the On-boarding Provisioning Form provided by the Provider;

2. The Customer shall cooperate with the Provider with regard to the performance of the Provider's obligations hereunder, including (without limitation):

    1. Providing the Provider with the required remote access to the Customer's Equipment and/or Workloads, as may be reasonable to permit the Provider to perform its obligations hereunder, and

    2. Notifying the Provider of any changes to its configurations that could potentially impact the 11:11 Network Support; and

3. The Customer shall sign a confirmation that it accepts the potential risks for any Customer requests that fall outside of industry and security best-practices.

4. **Service Levels.**

    1. The Provider shall use commercially reasonable efforts to make sure that the Technical Ticket Response Management process adheres to the Targets set out in the current Service Level Agreement accessible at https://www.1111systems.com/legal/sla.

23. **11:11 Backup Deployment.** The terms and conditions of this Section 3.23 are applicable to each Order that includes the Provider's Backup Deployment Service in combination with 11:11 Cloud Backup for Veeam Cloud Connect.

    1. **Assets & Deliverables.**

        1. Statement of Work. Overall project document defining the terms of the engagement, steps and expected outcomes with sign-off by the Customer;

        2. Kick-off Call. Initial project call for introductions, defining timeframes and ensuring project alignment from Provider and Customer;

        3. Onboarding Provisioning Form. Documentation of existing environment including list of servers, VMs and backup jobs;

        4. Backup Deployment Service Guide. As-built documentation provided at the end of the engagement describing the architecture and environment that has been designed and deployed on the Customer site by the Provider; and

        5. Sign-off document validating knowledge transfer. Sign-off documentation validating that the Customer has received adequate instruction and education on the Provider-built environment.

    2. **Backup Deployment Project Management.**

1. Project managers. Both the Provider and the Customer shall appoint a project manager each who will serve as the primary contact point; and

2. Backup Deployment Project Management Engagement. The Provider's project manager and the Customer's project manager shall meet as required for the duration of the migration process for the purposes of facilitating a successful relationship and overseeing the implementation of all tasks outlined in the Statement of Work, including but not limited to, (a) tracking the progress of the implementation process and all associated tasks; (b) reviewing other current or future projects or business plans that may impact the Backup Deployment Service, (c) reviewing weekly status reports in order to review the Provider's performance in execution of the project for delivery of all Backup Deployment Service, (d) coordinating and planning for any new equipment or software acquisitions specific to supporting the completion of the Backup Deployment Service.

3. **Provider's Obligations.** The Provider is responsible for the following in accordance with industry best-practices:

    1. Providing enhanced onboarding project management deliverables, to include:

        1. Statement of Work documentation at the beginning of the project,

        2. Kick-off call between the Provider's deployment personnel and the applicable Customer's contacts, and

        3. Backup Deployment Service guide at the end of the engagement to the applicable Customer's contacts;

    2. Providing and managing supporting service documentation to include the Onboarding Provisioning Form detailing inventory and job specifications of all Workloads to be protected within scope of the Order;

    3. Providing installation, configuration and management of all services components required for the Backup Deployment Service, to include:

        1. Backup software installation, guiding the Customer through setup and configuration both in the Customer on-premises and to the Provider's cloud data center environments,

        2. Setup and configuration of backup jobs and schedules, and

        3. Setup and configuration of all Provider's side software components to support Customer's backup jobs.

4. **Customer's Obligations**. The Customer is responsible for the following in accordance with this Section 3.23 and industry best-practices:

    1. Ensuring that all required assets and services are obtained, and, where applicable, installed on the Customer's environment that are needed as part of the Order to include software, licenses, operating systems, bandwidth, hardware, storage, etc.;

    2. Ensuring that all required assets and services are deployed and configured in accordance with the applicable manufacturers' specifications and supportability requirements;

    3. Providing and managing supporting service documentation to include the Onboarding Provisioning Form detailing inventory and job specifications of all Workloads to be protected within scope of the Order;

    4. Ensuring all Customer-owned software, applications, devices, systems, processes, and services that maintain the Customer's data to be protected as part of the Order are documented as part of the Onboarding Provisioning Form;

    5. Providing all current and existing documentation of the Customer's Site(s) to include; environment "as-built" documentation, application contact information, application dependencies, current backup strategy, and disaster recovery plans if applicable;

    6. Providing the Provider's personnel with Customer's asset discovery and documentation where applicable;

    7. Where applicable, maintaining all software and other devices or items provided to the Customer by the Provider located within the Customer's Site(s) in direct support of the delivery of the Backup Deployment Service outlined in the Order (the "Equipment') in good working order and in accordance with applicable manufacturers' specifications. The Customer shall notify the Provider immediately upon determination that any Equipment is not in compliance with the foregoing, or is in material breach of the terms and conditions set forth in this Service Schedule; and

    8. Cooperating with the Provider with regard to the performance of the Provider's obligations hereunder, including (without limitation):

        1. Providing the Provider with the required remote access to Customer's Equipment, as may be reasonable to permit the Provider to perform its obligations hereunder, and

        2. Notifying the Provider of any changes to its configurations that could potentially impact the Backup Deployment Service.

24. **11:11 DRaaS Deployment.** The terms and conditions of this Section 3.24 are applicable to each Order that includes 11:11 DRaaS Deployment in combination with 11:11 Secure DRaaS.

    1. **Assets & Deliverables.**

        1. Connectivity Design Documentation. Technical documents and/or diagrams providing engineering level information and configuration details for the purpose of interconnecting the Customer's Primary Site(s) to the designated Provider's Recovery Site(s) delivering the DRaaS service capabilities;

        2. On-boarding Project Plan. A documented detailed overview of all tasks associated with the Provider on-boarding process for interconnectivity and delivery of the services protecting Workloads replicated from the Customer's Primary Site(s) Workloads within scope of the mutually agreed upon service contract. The purpose of this document is to track ownership, progress and completion of all applicable on-boarding tasks in collaboration between the Customer and the Provider;

        3. On-boarding Provisioning Form. A detail discovery document used for information gathering and collection of all Customer specific technical and infrastructure related information for the sole purpose of the Provider providing the onboarding service, integration, and management services to the Customer as part of the Secure DRaaS service contract;

        4. Recovery Action Plan. The initial disaster recovery process document developed between the Customer and the Provider which provides enhanced details for all steps and tasks required for proper failover or failback of the Customer's replicated Workloads to the designated Provider's Recovery Site(s). The Customer will own any changes after the initial development of the document; and

        5. Recovery Service Guide. A process document providing a business level view of the DRaaS solution. Key content includes general service description, service capabilities, the Customer's Primary Site(s) and the designated Provider's Recovery Site(s) location information, recoverable application service catalog, protected workload inventories, and failover process overview with key metrics (RTO / RPO).

    2. **On-boarding Project Management.**

        1. Project managers. Both the Provider and the Customer shall appoint a project manager each who will serve as the primary contact point; and

        2. On-boarding Project Management Engagement. The Provider's project manager and the Customer's project manager shall meet as required for the duration of the on-boarding process for the purpose

of facilitating a successful relationship and overseeing the implementation of all Cloud Resources and services outlined in the Order and the On-boarding Provisioning Form, including but not limited to, (a) tracking the progress of the on-boarding and implementation process and all associated tasks; (b) reviewing other current or future projects or business plans that may impact the onboarding of the Cloud Resources and services, (c) Weekly status reports to review the Provider's performance in execution of the on-boarding project for delivery of all Cloud Resources and services, (d) coordinating and planning for any new equipment or software acquisitions specific to supporting the completion of on-boarding all Cloud Resources and services.

3. **On-boarding Acceptance Test.**

    1. The On-Boarding Acceptance Test consists of non-service impacting Failover Test operation performed by Provider, as well as Application Testing and Verification performed by Customer. Fully committed Failover and Failback are not supported. The Test does not include modification of Primary Site resources including Virtual Machines and networking;

    2. The On-Boarding Acceptance Test is performed during the Provider's normal business hours of Monday-Friday 8:00 am – 5:00 pm with the time zone being based on data center location where services are located;

    3. <u>On-Boarding Acceptance Test Scheduling.</u> Upon completion of the on-boarding project tasks required for implementing the Cloud Resources within the scope identified in the Onboarding Provisioning Form, the Customer will be notified and will have fourteen (14) days from the day of notice in which to schedule a final On-Boarding Acceptance Test;

    4. <u>On-Boarding Acceptance Test Success Criteria.</u> Successful completion of the On-boarding Acceptance Test shall be determined by validation of the Provider's ability to meet the RTO agreed during the planning phase of the onboarding project. The Target Objectives will be documented in Recovery Action Plan and Recovery Service Guide; and

    5. In the event that the On-Boarding Acceptance Test does not meet the RTO agreed in the planning phase, the Customer agrees to provide the Provider with any data or information reasonably requested by the Provider in order to enable the Provider to diagnose and resolve any problems associated with any failure to meet that RTO in the On-Boarding Acceptance Testing. The Provider project manager will notify the Customer via email or phone upon resolution of any such issues. After the Provider has notified the Customer that the problem has been resolved, the Customer and

the Provider will promptly conduct a follow-up On-Boarding Acceptance Test to validate that the RTO associated with the On-Boarding Acceptance Test have now been met. This process will continue, if necessary, until the On-Boarding Acceptance Test Criteria meets the required success criteria. Notwithstanding anything to the contrary in this Service Schedule, if the Customer fails to respond to the On-Boarding Acceptance Test reschedule notice within fourteen (14) days of the date of notification, then the Provider shall consider the on-boarding completed and will have no further obligations to the Customer in regard to the On-Boarding Acceptance Test.

4. **Provider's Obligations.** The Provider is responsible for the following in accordance with industry best-practices:

    1. Providing enhanced onboarding project management deliverables, to include:

        1. Weekly status call between the Provider on-boarding personnel and applicable Customer's contacts, and

        2. Weekly status report summarizing project tasks progress, project milestones, estimated and actual durations/completion dates and critical path items;

    2. Providing all supporting Service documentation to include:

        1. Documented inventory and workload specifications (e.g. compute, storage, networking) of all Workloads within scope of the Order,

        2. Documented L2/L3 network design for compatibility and integration between the Customer Primary Site(s) and 11:11 Secure DRaaS networking services and design guidelines, and

        3. Documented Customer network security configurations, including firewall security policies, NAT policies and network security segmentation design;

    3. Providing full installation and configuration of all services components required for delivery of 11:11 Secure DRaaS, to include:

        1. Replication software installation, setup and configuration both in the Customer's premises and the Provider's cloud data center environments,

        2. Setup and configuration of VPN connections (where applicable),

        3. Setup and configuration of all the Provider's side networking components support dedicated circuits for WAN connectivity (where applicable), and

4. Setup & configuration of any cross-connects to support networking connectivity in accordance with Section 3.14 of this Service Schedule;

4. Providing full setup and configuration for replication of the Recovery Groups for all Workloads within scope and applicable to the Order and the Onboarding Provisioning Form;

5. Providing full assistance with development and creation of the Customer's Disaster Recovery Runbook(s) within the 11:11 Cloud Console;

6. Providing full assistance with development and creation of the Customer's Recovery Activation Plan;

7. Providing the initial managed failover test; and

8. Providing a completed Recovery Service Guide at the completion of the on-boarding process.

5. **Customer Obligations.** The Customer is responsible for the following in accordance with Provider's delivery of the 11:11 DRaaS Deployment and industry best-practices:

    1. Ensure all Customer-owned software, applications, devices, systems, processes, and services that maintain Customer Data to be protected by the services delivered as part of this Agreement are covered as specified under Section 2.3.5 of this Service Schedule for the purposes of fulfilling this Agreement;

    2. Where applicable, the Customer shall maintain all firmware or software updates to all Customer-owned hardware, software, applications, devices, and systems in use with or protected by Cloud Resources provided by the Provider;

    3. Where applicable, contact all software, application, device, system, service, and service providers covered under this Agreement and add the appropriate Provider's personnel as approved contacts for the purposes of fulfilling this Service Schedule;

    4. Complete the On-boarding Provisioning Form provided by the Provider;

    5. Provide all current and existing documentation of the Customer Primary Site(s) to include; environment "as-built" documentation, application contact information, application dependencies, current backup strategy, and disaster recovery plans if applicable;

    6. Provide the Provider's personnel with the Customer's asset discovery and documentation where applicable;

    7. Where applicable; provide all current process documentation in support of the services outlined in this Agreement and provide all

assistance necessary to modify existing or implement new processes to streamline the delivery of services;

8. Where applicable, the Customer shall maintain all software and other devices or items provided to the Customer by the Provider located within the Customer's Primary Site(s) in direct support of the delivery of Cloud Resources outlined in the Order (the "Equipment') in good working order and in accordance with applicable manufacturers' specifications. The Customer shall notify the Provider immediately upon determination that any Equipment is not in compliance with the foregoing, or is in material breach of the terms and conditions set forth in this Service Schedule;

9. The Customer shall cooperate with the Provider with regard to the performance of the Provider's obligations hereunder, including (without limitation):

    1. Providing the Provider with the required remote access to the Customer's Equipment, as may be reasonable to permit Provider to perform its obligations hereunder, and

    2. Notifying the Provider of any changes to its configurations that could potentially impact the services;

10. Manages and updates to any documentation after the initial handoff of the documentation to the Customer; and

11. All other obligations as outlined in Section 3.10.3

25. **Managed Appliance.** The terms and conditions of this Section 3.25 are applicable to each Order that includes the Provider's Managed Appliance Services as described in the Order.

    1. **Service options (applicable only to Managed Firewalls).** Either Managed Firewall service offering can be delivered to physical or virtual firewalls running on premises or cloud infrastructure. Firewall management service options encompass net new firewall deployments for greenfield environments, firewall replacement for existing brownfield environments, and management takeover of existing brownfield environments. Major re-architectures and redesigns, as identified at Provider's discretion, are out of scope for Basic and Advanced management service options and would require a separate Professional Services engagement with Provider.

        1. Basic. Basic Firewall Management provides basic management of the firewall appliance with basic NOC monitoring and reporting as defined at https://success.1111systems.com/article/0rdysi;

        2. Advanced. Advanced Firewall Management includes management of the full Unified Threat Protection (UTP) capabilities of the firewall appliance and includes custom advanced monitoring by the NOC; and

3. SD-WAN. SD-WAN expands the traditional basic management of the firewall appliance to include configuration and implementation assistance, and device administration when such device(s) is/are part of an SD-WAN architecture. The SD-WAN service definition is further explained in Section 3.36.

2. **Provider's Obligations.** The Provider is responsible for the following in accordance with industry best practices:

    1. Procuring any appliance hardware, licensing, and/or support identified in the Order as Provider-Supplied Equipment;

    2. Onboarding Managed Device(s) into the Provider's infrastructure;

    3. Providing recommended firmware upgrades based on critical Common Vulnerabilities and Exposures (CVEs) ratings, which may not always align with the most recent firmware from the vendor;

    4. Completing firmware upgrades as deemed appropriate and necessary by the Provider;

    5. Use best efforts to coordinate all firmware upgrades with the Customer prior to completion of the upgrade;

    6. Providing commercially reasonable Change Management support such as;

        1. The Provider will make reasonable attempts to discuss and notify the Customer of any changes prior to making changes to the configuration of the appliance, and

        2. In the case of an Emergency, where the Provider determines (in its sole discretion) that the security, confidentiality, integrity, or availability of the switch is at risk, changes may be made without prior notification to the Customer in order to attempt to mitigate the risk;

    7. Maintaining backup configurations after changes are made to the supported appliance to ensure rollback and recovery capability; and

    8. Supporting Next Business Day (NBD) or Premium 4-hour replacement for the Provider-Supplied Equipment, as specified in the Order. RMA delivery may be impacted by customer location. Provider is not liable for RMA gear delivered late due to delays caused by location constraints and/or shipping and receiving issues;

    9. For Managed Firewalls.

        1. As supported by hardware, software, and licensing specified in Order, configuration of zones, rules, objects, NATs, site-to-site VPNs, user access VPNs, routing, and UTM configuration in accordance with Customer's completed Customer Design Requirements (CDR) form,

2. Basic configuration review of NGFWs for high level best practices around zones and rules. This does not include automated rule analysis via tools, or manual line by line review of the entire ruleset, which remains Customer's obligation in absence of a separated professional services agreement between Customer and Provider,

3. Configuring remote access VPN to provide Customer's end-user access to the internal network requested by Customer in accordance with CDR form. This includes local user setup or Lightweight Directory Access Protocol (LDAP). The Provider will make commercial best efforts to configure VPN client connectivity, however VPN connectivity is subject to a variety of factors, including, but not limited to, local ISP issues, local or home office network issues, and public WiFi port blocking,

4. Providing seven (7) days of active log retention from each supported NGFW.

    1. When the specified seven (7) day log limit is exceeded, the oldest logs shall be overwritten to make room for new logs.

    2. Destruction of logs upon termination in accordance with the terms of the Agreement; and

5. Exclusively for the Advanced Managed Firewall:

    1. Providing UTM feature configuration and optimization as per the Provider's then current Product Compatibility Matrix, including but not limited to:

1. IDS/IPS. Configuring Intrusion Detection and Prevention Services (IDS/IPS) to detect and block traffic patterns that contain malicious threats on Equipment.

2. Application Control. Configuring application control to provide detailed visibility into user traffic.

3. Web Filtering. Configuring web content filtering to monitor and block websites based on category.

    2. Performing UTM security updates.

    3. Providing performance & utilization monitoring.

    4. Providing a monthly activity report.

    5. Supporting High Availability (HA) deployments.

    6. Providing a ninety (90) day active log retention.

    7. Specific to Fortinet firewalls, providing a one (1) year long archive.

10. For Managed Routers. As supported by hardware, software and licensing specified in Order, configuration support for interfaces, routing, route maps, ACLs, Zone Based Firewall (ZBFW), Dynamic Multipoint VPN (DMVPN), and IPSec VPNs; and

11. For Managed Switches. As supported by hardware, software and licensing specified in Order, configuration support for VLANs, access ports, trunks, LACP, vPC, HSRP/VRRP, layer 3 SVIs, VRFs, static routes and dynamic routing.

3. **Customer's Obligations.** The Customer is responsible for the following in accordance with Provider's delivery of the Managed Appliance services and industry best practices:

    1. Promptly providing all information requested by Provider's technical team related to existing network policies and configurations associated with the old equipment, if applicable, to ensure a seamless migration process and to minimize any potential conflicts or challenges that may arise during the transition. In the event Customer requires additional assistance or expertise for the actual transfer of rules from the old equipment to the new SD-WAN infrastructure, then Provider is prepared to offer such services as part of a separate paid professional services engagement the terms of which will be mutually agreed to in writing signed by the Parties;

    2. Providing architectural design for network and applications;

    3. Installing and cabling the Provider's Equipment at the Customer's location(s). Upon request, the Provider offers installation services as an add-on, based on availability at the respective location(s);

    4. For Customer-provided appliances, either physical or virtual, ensuring that the hardware is supported by the Provider's then-current Product Compatibility Matrix.

        1. For Customer-provided Managed Firewalls, either physical or virtual, ensuring that the NGFW(s) is exclusively powered by Fortinet FortiGate or Cisco Firepower and supported by the Provider's then-current Product Compatibility Matrix;

    5. For Customer-provided appliances, either physical or virtual, ensuring that up-to-date vendor support is attached to all applicable hardware, software and licensing;

    6. Providing an approved network diagram;

    7. Providing access to existing appliance configuration;

    8. Providing applicable specifications to the Provider to allow for configuration of network interfaces, VLANs, access ports, trunks, LACP, vPC, HSRP/VRRP, layer 3 SVIs, VRFs, static routes and dynamic routing;

9. Providing access to the customer's internal network to allow provider to configure remote access VPN;
10. Providing a technical resource for the duration of the implementation project;
11. Providing coordination for scheduling necessary maintenance windows to complete the implementation;
12. Providing a technical resource to assist in troubleshooting issues for hardware at customer premises as Provider does not provide on-site support for physical appliance;
13. Notifying the Provider with Change Management requests;
14. For Managed Appliance services in a DR environment where the Provider does not manage the production environment:
    1. Adopting strict change management control processes to capture all changes made to production devices,
    2. Analyzing all changes in production for applicability in the DR environment,
    3. Translating any changes in production to equivalent changes required on the DR Managed Appliance, including but not limited to, re-mapping of ACLs, NATs, VLANs, etc. as needed if the DR environment employs different public or private IP addressing schemes or VLANs,
    4. Notifying the Provider with Change Management requests as applicable for the DR environment, and
    5. Regularly auditing and maintaining ownership of configuration sync between production and DR;
15. Notifying the Provider in the event of any major changes that may potentially impact the Managed appliance service, including, but not limited to:
    1. Changing Internet service at the location where the appliance resides,
    2. Changing internal networking scheme,
    3. Moving the appliance to a different location,
    4. For Managed Firewalls, significantly increasing the users of SSL VPN (as determined by the Provider at the Provider's sole discretion),
    5. For physical appliances only:
        1. Ensuring proper power is available at the location where the appliance resides.

2. Ensuring that the necessary rack space has been allocated.

3. Ensuring that proper environmental requirements are met for any new Equipment installations.

4. Providing the physical address of the appliance to the Provider.

6. For virtual appliances only:

1. Providing all vCPU, RAM, and storage resources to host the virtual appliance.

2. If deployed on a Customer-managed cluster or cloud environment, Customer is responsible for virtual appliance deployment and providing console access to Provider

16. For Managed Firewalls.

1. Filling out the Customer Design Requirements (CDR) form in its entirety to capture all firewall configuration requirements, including but not limited to: zones, rules, objects, NATs, site to site VPNs, user access VPNs, routing, and UTM configuration,

2. If migrating from a different vendor platform, Customer is responsible for translating existing configuration to populate in the Customer Design Requirements (CDR) form,

3. Providing applicable specifications to the Provider to allow for configuring Network Address Translation (NAT) and inbound and outbound stateful firewall rules, and

4. Customer is responsible for defining all inbound and outbound rules and VPN configuration and is responsible for following best practices around network segmentation and least-privileged access. Customer is responsible for any security incidents or a breach resulting from unsecured ACLs, public NATs, VPN or any other customer defined configuration; and

17. For Managed Routers and Switches. Providing applicable specifications to the Provider to allow for configuration of network interfaces, VLANs, access ports, trunks, LACP, vPC, HSRP/VRRP, layer 3 SVIs, VRFs, static routes and dynamic routing.

26. **Managed SIEM (Security Information and Event Management).** The terms and conditions of this Section 3.26 are applicable to each Order that includes Managed SIEM services.

1. **Provider's Obligations.** The Provider is responsible for the following in accordance with industry best practices:

1. Assisting the Customer in deploying the collector and/or agent on the agreed Customer locations;
2. Ensuring that all event sources are properly sending logs to the SIEM;
3. Optimizing the data collection and tuning of alerts;
4. Creating custom alerting and notifications;
5. Log Ingestion:
    1. Log files will be subjected to automated analysis procedures designed to identify attacks, operational problems, or compromises,
    2. Anomalies discovered by this process shall be communicated to the Customer, and
    3. A ticket with a monthly report shall be provided to the Customer summarizing the results of the analysis and any applicable network traffic trends;
6. Log File Analysis:
    1. Log files will be subjected to automated analysis procedures designed to identify attacks, operational problems, or compromises,
    2. Anomalies discovered by this process shall be communicated to the Customer, and
    3. A ticket with a monthly report shall be provided to the Customer summarizing the results of the analysis and any applicable network traffic trends; and
7. Log Retention:
    1. Providing a ninety (90) day active log retention. When the specified ninety (90) day limit is exceeded, the oldest logs will be overwritten to make room for new logs,
    2. Providing a one (1) year archive of log files, and
    3. Destruction of logs upon termination in accordance with the terms of the Agreement.

2. **Customer's Obligations.** The Customer is responsible for the following in accordance with Provider’s delivery of the Managed SIEM services and industry best practices:
    1. Populating Provider provided security questionnaire;
    2. Providing an approved network diagram and any other information relevant to the security of the environment that will aid the Provider in security monitoring;

3. Providing a technical resource for the duration of the implementation project, including, but not limited to, installing and uninstalling the collectors and/or agents, and configuring log sources;

4. Providing hardware to collect event logs. In the event that the collector is part of the Customer's virtual Data Center, providing virtual resources to deploy the collector;

5. As needed for certain deployments, providing the Provider with an admin account to pull information from the environment;

6. Providing a list of log sources on the Customer's network;

7. Configuring the event sources for log data ingestion based on the Provider's instructions;

8. Notifying the Provider in the event of any changes to the list of log sources or if the network environment changes, including, but not limited to, adding or removing devices; and

9. Responding in a timely manner to Provider's incident escalations and any other issues that arise related to the health of the system or the health of any data sources.

27. **Managed CRS (Continuous Risk Scanning).** The terms and conditions of this Section 3.27 are applicable to each Order that includes Managed CRS services.

    1. **Provider's Obligations.** The Provider is responsible for the following in accordance with industry best practices:

        1. Providing network discovery and asset prioritization;

        2. Identifying critical vulnerabilities;

        3. Providing a remediation workflow engine;

        4. Performing distributed scanning;

        5. Providing visibility to reporting and scorecards;

        6. Creating tenant in the Managed Security Portal;

        7. Setting up Customer's user(s) in the Managed Security Portal;

        8. Creating an agent installer and supporting the Customer in the deployment of the scanning agent. Agent support shall be limited to Windows OS;

        9. If necessary, assisting the Customer in the deployment of the virtual scanning appliance; and

        10. Setting up the external cloud scanner for external asset scanning.

2. **Customer's Obligations.** The Customer is responsible for the following in accordance with Provider's delivery of the Managed CRS services and industry best practices:
    1. Providing all documented IP space (including subnets);
    2. Providing any changes to the network;
    3. Providing an Access Control List (ACL) to allow the Provider's scanner to reach all devices;
    4. Maintaining proper access to the network and assets being scanned by the Provider;
    5. Assisting the Provider in the deployment of the agenda and/or virtual scanner;
    6. Assisting the Provider in the grouping of assets into business contexts;
    7. Remediating threats and vulnerabilities; and
    8. Notifying the Provider in the event of any major changes that could potentially impact the service, including, but not limited to:
        1. Changing Internet service at the Customer location,
        2. Changing internal networking scheme,
        3. Moving to a different location,
        4. Removing agents,
        5. Adding new endpoints, and
        6. Replacing endpoints.

28. **Managed EDR (Endpoint Detection and Response).** The terms and conditions of this Section 3.28 are applicable to each Order that includes Managed EDR services.
    1. **Provider's Obligations.** The Provider is responsible for the following in accordance with industry best practices:
        1. Guiding the Customer in the deployment of the agent(s), which shall be limited to Fortinet FortiEDR or Trend Micro Vision One XDR agents;
        2. Creating and optimizing the policies and tuning alerts;
        3. Creating and optimizing the Playbook according to threat data and Customer's business requirements;
        4. Analyzing logs and notifying the Customer of suspicious activity or identified threats;
        5. Creating custom alerting and notifications;
        6. For Fortinet FortiEDR only, providing a six (6) month log retention;

1. When the specified six (6) month log limit is exceeded, the oldest logs shall be overwritten to make room for new logs, and

2. Destruction of logs upon termination in accordance with the terms of the Agreement;

7. Optionally, for Fortinet FortiEDR only, configuring the following external integrations:

    1. Custom SIEM target(s), upon Customer's reasonable request, that are publicly accessible.

2. **Customer's Obligations.** The Customer is responsible for the following in accordance with Provider's delivery of the Managed EDR services and industry best practices:

    1. Providing an approved network diagram;

    2. Providing a technical resource for the duration of the implementation project;

    3. Assisting the Provider in deployment of agents on endpoints;

    4. Ensuring that the endpoints, on which the Fortinet FortiEDR or Trend Micro Vision One XDR agents are deployed, match the specifications as defined in the Provider's then-current Product Compatibility Matrix;

    5. Assisting the Provider in the customization of Playbooks and policies during the tuning period and ongoing;

    6. Providing incident response and remediating threats; and

    7. Notifying the Provider in the event of any major changes that could potentially impact the service, including, but not limited to:

        1. Changing Internet service at the Customer location,

        2. Changing internal networking scheme,

        3. Moving to a different location,

        4. Removing agents,

        5. Adding new endpoints, and

        6. Replacing endpoints.

29. **Professional Security Services.** The terms and conditions of this Section 3.29 are applicable to each Order that includes Professional Security services.

    1. **Service options.**

        1. Network Architecture Review and Design. This service includes professional services by the Provider's security professionals to

review the Customer's existing architecture, and design a network solution driven by both security and business objectives;

2. Appliance Configuration and Implementation. This service includes professional services by the Provider's security professionals to configure and optimize the Customer's Fortinet FortiGate appliance(s), and test the Customer's Equipment for readiness and quality before deployment. This service is limited to Fortinet products only; and

3. Health Check. This service includes professional services by the Provider's security professionals to perform a detailed review of the Customer's security solution and identify potential areas of improvement within the scope of the mutually agreed upon SOW.

2. **Provider's Obligations.** The Provider is responsible for the following in accordance with commercially reasonable efforts:

    1. Developing a Statement of Work based on Customer's provided business objectives and/or goals; and

    2. Performing duties necessary to deliver the service as defined in the Statement of Work.

3. **Customer's Obligations.** The Customer is responsible for the following in accordance with Provider's delivery of the Professional Security services and industry best practices:

    1. Providing a technical resource for the duration of the engagement;

    2. Providing an approved network diagram;

    3. Providing business objectives and/or goals for the engagement;

    4. Acknowledging that the Provider does not guarantee prevention of security breaches;

    5. Exclusively for the Appliance Configuration and Implementation service, accurately identifying the Equipment that needs to be replaced and provide the Provider with the current configuration for the Equipment; and

    6. Exclusively for the Health Check service, providing the Provider with all relevant and necessary details for the Customer's current security posture and existing system controls.

30. **Managed Backup for Cohesity.** The terms and conditions of this Section 3.30 are applicable to each Order that includes the Provider's Managed Backup for Cohesity service.

    1. **Resources.**

1. Storage. The resources that comprise the Managed Backup for Cohesity service include dedicated Equipment that provide storage capacity in pre-determined cluster sizes as specified in the Order;

2. Licensing. All required licensing is included in the Managed Backup for Cohesity service as specified in the Order; and

3. Business Models. Capacity is available in a reserved business model as specified in the Order.

2. **Assets & Deliverables.** The Provider is responsible for the following in accordance with commercially reasonable efforts:

    1. On-Boarding Project Plan. A documented detailed overview of all tasks associated with the Provider on-boarding process defined within scope of the mutually agreed upon Statement of Work. The purpose of this document is to track ownership, progress and completion of all applicable on-boarding tasks in collaboration between the Customer and the Provider;

    2. On-Boarding Provisioning Form. A detailed discovery document used for information gathering and collection of all Customer-specific technical and infrastructure-related information for the sole purpose of the Provider providing the onboarding service, integration, and management services to the Customer;

    3. Backup Policies. The policies define the managed backup schedule of how often and when to take a backup and the retention timeframe for that backup. The policies also define how often full backups should be taken and how often to retry in the event of backup failure; and

    4. Backup Groups. Groups define what resources are backed up and assigns the applicable Backup Policy to those resources.

3. **On-Boarding Project Management.**

    1. Project managers. Both the Provider and the Customer shall appoint a project manager to serve as the primary contact point; and

    2. On-Boarding Project Management Engagement. The Provider's project manager and the Customer's project manager shall meet as required for the duration of the on-boarding process for the purpose of facilitating a successful relationship and overseeing the implementation of all backup resources and services outlined in the Order and the On-boarding Provisioning Form, including but not limited to: (a) tracking the progress of the on-boarding and implementation process and all associated tasks; (b) reviewing other current or future projects or business plans that may impact the onboarding of the Equipment and services; (c) weekly status reports to review the Provider’s performance in execution of the on-boarding project for delivery of all Equipment and services; and (d)

coordinating and planning for any new Equipment or software acquisitions specific to supporting the completion of on-boarding the Managed Backup for Cohesity service.

4. **On-Boarding Acceptance Test.**

    1. The On-Boarding Acceptance Test consists of non-service impacting backup recovery test operation performed by the Provider in conjunction with the Customer, as well as data recovery verification performed by the Customer, in each case as defined in the On-Boarding Project Plan;

    2. The On-Boarding Acceptance Test is performed during the Provider's normal business hours of Monday-Friday 8:00 am – 5:00 pm with the time zone being based on the location where services are located, excluding any federal or other holidays observed by the Provider in such location;

    3. On-Boarding Acceptance Test Success Criteria. Successful completion of the On-boarding Acceptance Test shall be determined by validation to recover data either to the original location or an alternative location. Any other target objectives will be documented in the On-Boarding Project Plan. If the On-Boarding Acceptance Test cannot be completed for technical reasons, the Customer will provide the Provider with any data or information reasonably requested by the Provider in order to enable the Provider to diagnose and resolve any problems associated with any failure to recover data during the On-Boarding Acceptance Testing. The Provider project manager will notify the Customer via email or phone upon resolution of any such issues. After the Provider has notified the Customer that the problem has been resolved, the Customer and the Provider will promptly conduct a follow-up On-Boarding Acceptance Test to verify data recovery. This process will continue, if necessary, until the On-Boarding Acceptance Test Criteria meets the required success criteria; and

    4. Notwithstanding anything to the contrary in this Service Schedule, if the Customer fails to timely participate in the On-Boarding Acceptance Test process as identified in the On-Boarding Project Plan, all of the Provider's on-boarding obligations will be considered completed and Provider will have no further obligations to the Customer regarding the On-Boarding Acceptance Test. In such event, the Customer may continue to exercise unlimited self-service testing.

5. **Service Delivery Management.**

    1. Service Delivery Management Contacts. The Customer shall appoint an individual who will serve as the primary contact point for the Provider in connection with ongoing lifecycle management and delivery of the services, and the Provider shall appoint a point of contact; and

2. Service Delivery Management Engagement. The Provider and the appointed Customer's project contact shall meet as required during the term of each service for the purpose of facilitating a successful relationship and overseeing the delivery and performance of each service, including but not limited to, (a) tracking the progress of the onboarding and implementation process and all associated tasks, (b) reviewing other current or future projects or business plans that may impact all services and/or delivery of all services, (c) coordinating and planning for any new equipment or software acquisitions or needs, (d) reviewing strategic and tactical decisions for the Customer in respect of the establishment, budgeting and implementation of the Customer's priorities and plans for information technology that may impact services and/or delivery of all services, and (e) monitoring and resolving concerns that may arise regarding the provision of the Service Schedule.

6. **Provider's Obligations.** The Provider is responsible for the following in accordance with industry best practices:

    1. Providing the Equipment as specified by the Order;

    2. Providing documentation and guiding the Customer through the On-Boarding Acceptance Test and related process;

    3. Providing ongoing support and education about Customer's self-service data recovery features of the Managed Backup for Cohesity service at the Customer's request;

    4. Maintaining the underlying cloud infrastructure components to support the Managed Backup for Cohesity service such as compute, memory, storage and networking by following Provider's guidelines for managing these environments;

    5. Providing backup Equipment capacity increase options via Order as recommended by the Provider or as otherwise requested by the Customer;

    6. In case of Provider-assisted restoration, assisting the Customer with initiating the restore from the Provider-Supplied Equipment at-time-of-Disaster;

    7. Monitoring performance and status of the Managed Backup for Cohesity service in compliance with the Backup Policies for each of the Backup Groups;

    8. Providing enhanced onboarding project management deliverables, to include:

        1. Weekly status call between the Provider on-boarding personnel and applicable Customer's contacts, and

2. Weekly status report summarizing project tasks progress, project milestones, estimated and actual durations/completion dates and critical path items;

9. Providing the Provider's published Managed Backup for Cohesity service documentation and managing supporting documentation, including:

    1. Documented inventory and workload specifications (e.g. compute, storage, networking) of all Workloads within the scope of the Order, and

    2. Documented Customer network security configurations, including firewall security policies, NAT policies and network security segmentation design.

10. Providing full installation, configuration and ongoing management of all services components required for delivery of Managed Backup for Cohesity service, to include (as applicable):

    1. Backup hardware & software installation, setup and configuration in the Customer's on-premises environments used for provision of such services;

11. Providing full setup and configuration for backup of the Backup Policies for all Workloads within the scope and applicable to the Order and the On-Boarding Provisioning Form;

12. Providing full assistance with the development and creation of the Customer's Backup Policy definitions;

13. Providing managed data recovery testing from backup and live data recovery from backup declaration events;

14. Fulfilling Customer requests for new Backup Policies, increased capacity, and other change requests; and

15. Providing ongoing updates, patching and maintenance for all the Provider-supplied service components required for delivery of the Managed Backup for Cohesity service, to include:

    1. Customer's on-premises Equipment, and

    2. Software components used by the Managed Backup for Cohesity service; and

16. Provided the Customer has returned the Equipment to the Provider in accordance with the requirements of this Service Schedule, the Provider will permanently destroy the Equipment and provide the Customer with a Certification of Destruction within a reasonable period following such destruction.

7. **Customer's Obligations.** The Customer is responsible for the following in accordance with industry best practices (as applicable):

1. Providing the Provider with full and timely cooperation in the Provider's provision of the Managed Backup for Cohesity service, including without limitation by: (a) providing the Provider with all information reasonably requested by the Provider, such as backup requirement details and site access details and (b) making available Customer's designated contact reasonably accessible to the Provider;

2. Restoring backups from the Provider-Supplied Equipment provided with the Managed Backup for Cohesity service. While the Provider will provide Customer with reasonable support with restoring its backups upon request, Customer remains responsible for performing granular recovery of individual items from agent-based application aware backups. Customer further acknowledges that the Provider does not guarantee the recoverability of individual applications running on the Virtual Machines, such as databases or email messaging systems;

3. Promptly notifying the Provider if the protected Resources are compromised, modified or infected by an unauthorized user, malware, virus, worm, or similar code or otherwise Hacked or accessed by a person lacking permission to access the protected Resources;

4. If the Customer provisions Reserved Resources in excess of the specifications set out on the Order, including the storage necessary for processing the snapshot-based backups, the Provider is not responsible for any performance degradation, loss of backup data, or errors caused by over allocation;

5. Ensuring all Customer-owned software, applications, devices, systems, processes, and services that maintain Customer data to be protected by the services delivered as part of this Agreement are covered as specified under Section 2.3.5 of this Service Schedule for the purposes of fulfilling the Agreement;

6. Maintaining all firmware or software updates to all Customer-owned hardware, software, applications, devices, and systems in use with or protected by the Managed Backup for Cohesity service provided by the Provider;

7. Contacting all software, application, device, system, service, and service providers covered under this Agreement and add the appropriate Provider's personnel as approved contacts for the purposes of fulfilling this Service Schedule;

8. Assisting with the completion of the On-boarding Provisioning Form provided by the Provider;

9. Providing all current and existing documentation of the Customer Primary Site(s) including without limitation, environment "as-built"

documentation, application contact information, application dependencies, current backup strategy, disaster recovery plans and any other documentation reasonably requested by the Provider;

10. Providing the Provider's personnel with the Customer's asset discovery and documentation;

11. Providing all current process documentation in support of the Managed Backup for Cohesity service and provide all assistance to the Provider as necessary to modify existing or implement new processes to streamline the delivery of the Managed Backup for Cohesity service;

12. Maintaining all software and Provider-Supplied Equipment or items provided to the Customer by the Provider located within the Customer's Primary Site(s) in direct support of the delivery of Managed Backup for Cohesity service outlined in the Order in good working order and in accordance with applicable manufacturers' specifications. The Customer shall notify the Provider immediately upon determination that any Provider-Supplied Equipment is not in compliance with the foregoing or is otherwise not working;

13. The Customer shall cooperate with the Provider with regard to the performance of the Provider's obligations hereunder, including (without limitation):

    1. Providing the Provider with the required remote access to the Customer's Equipment, as may be reasonable to permit Provider to perform its obligations hereunder, and

    2. Notifying the Provider of any changes to its configurations that could potentially impact the services. For example, any data protection gaps such as a new virtual machine or physical server not being protected because the Customer did not inform the Provider.

14. Prior to the expiration or termination of any Order for the Managed Backup for Cohesity service, migrating and permanently deleting all of its Customer data residing on any Equipment prior to returning the Equipment to the Provider. Such data migration and deletion obligations are at the Customer's expense, unless otherwise agreed between the Customer and the Provider in a SOW for data migration services; and

15. Within thirty (30) days after the expiration or termination of any Order for the Managed Backup for Cohesity service where such Order covers Equipment, Customer will return the Equipment to the Provider by shipping the Equipment to Provider's designated address at Customer's expense. Risk of loss to the Equipment will remain with Customer until Equipment is delivered to the Provider. Customer acknowledges and agrees if Customer does not ship the

Equipment to Provider within such thirty (30) day period, Customer will pay the applicable Provider the cost of the Equipment.

31. **Managed Off-Site Backup for Cohesity.** The terms and conditions of this Section 3.31 are applicable to each Order that includes the Provider's Managed Off-Site Backup for Cohesity service.

    1. **Resources.**

        1. Storage. The resources that comprise the Managed Off-Site Backup for Cohesity service could include one of the following as specified in the Order:

            1. Dedicated Equipment that provides storage capacity in pre-determined cluster sizes, or

            2. Shared Equipment that provide storage capacity in a multi-tenant environment;

        2. Licensing. All required licensing is included in the Managed Off-Site Backup for Cohesity service unless explicitly specified in the Order for Bring-Your-Own-Device (BYOD) environments; and

        3. Business Models. Capacity is available in a reserved business model for Dedicated Equipment and reserved plus burst business model for Shared Equipment as specified in the Order.

    2. **Assets & Deliverables.**

        1. On-Boarding Project Plan. A documented detailed overview of all tasks associated with the Provider on-boarding process defined within scope of the mutually agreed upon Statement of Work. The purpose of this document is to track ownership, progress, and completion of all applicable on-boarding tasks in collaboration between the Customer and the Provider; and

        2. On-Boarding Provisioning Form. A detailed discovery document used for information gathering and collection of all Customer specific technical and infrastructure-related information for the sole purpose of the Provider providing the on-boarding service, integration, and management services to the Customer.

    3. **On-Boarding Project Management.**

        1. Project managers. Both the Provider and the Customer shall appoint a project manager to serve as the primary contact point; and

        2. On-Boarding Project Management Engagement. The Provider's project manager and the Customer's project manager shall meet as required for the duration of the on-boarding process for the purpose of facilitating a successful relationship and overseeing the implementation of all backup resources and services outlined in the Order and the On-boarding Provisioning Form, including but not limited to: (a) tracking the progress of the on-boarding and

implementation process and all associated tasks; (b) when applicable, reviewing other current or future projects or business plans that may impact the onboarding of the Equipment and services; and (c) when applicable, weekly status reports to review the Provider's performance in execution of the on-boarding project for delivery of services.

4. **Service Delivery Management.**

    1. Service Delivery Management Contacts. The Customer shall appoint an individual who will serve as the primary contact point for the Provider in connection with ongoing lifecycle management and delivery of the services, and the Provider shall appoint a point of contact; and

    2. Service Delivery Management Engagement. The Provider and the appointed Customer's project contact shall meet as required during the term of each service for the purpose of facilitating a successful relationship and overseeing the delivery and performance of each service, including but not limited to, (a) tracking the progress of the onboarding and implementation process and all associated tasks, (b) reviewing other current or future projects or business plans that may impact all services and/or delivery of all services, (c) coordinating and planning for any new equipment or software acquisitions or needs, and (d) monitoring and resolving concerns that may arise regarding the provision of the Service Schedule.

5. **Provider's Obligations.** The Provider is responsible for the following in accordance with industry best practices:

    1. Providing the storage infrastructure and licensing as specified by the Order;

    2. Providing documentation and guiding the Customer through the On-Boarding process;

    3. Maintaining the underlying cloud infrastructure components to support the Managed Off-Site Backup for Cohesity service such as compute, memory, storage and networking by following Provider's guidelines for managing these environments;

    4. Providing Off-Site Backup capacity increase options via Order as recommended by the Provider or as otherwise requested by the Customer;

    5. Providing the Customer with the option to purchase a best-effort cloud restoration service to 11:11 Cloud Services at an additional cost using the backups stored at the Target Site with the following parameters:

        1. The creation of Virtual Data Center(s) will consist of the specifications detailed in the relevant Order,

2. The network connectivity to the restored environment will be provided by the Provider,
3. The restoration shall be limited to VMware based environments, and
4. The Provider will start the restoration process within 24 hours after the Customer has both declared a Disaster by notifying the Provider and approved the new Order that contains the cloud resources required to run the workloads along with the i-Tech fees for the professional services required to perform the restoration tasks;

6. Providing enhanced onboarding project management deliverables, to include:
    1. Weekly status call between the Provider on-boarding personnel and applicable Customer's contacts, and
    2. Weekly status report summarizing project tasks progress, project milestones, estimated and actual durations/completion dates and critical path items;
7. Providing the Provider's published Managed Off-Site Backup for Cohesity service documentation and managing supporting documentation;
8. Providing full installation, configuration and ongoing management of all services components required for delivery of Managed Off-Site Backup for Cohesity service, to include (as applicable):
    1. Backup hardware & software installation, setup and configuration;
9. Fulfilling Customer requests for increased capacity and other change requests; and
10. Providing ongoing updates, patching and maintenance for all the Provider-supplied service components required for delivery of the Managed Off-Site Backup for Cohesity service, to include:
    1. Infrastructure hosting the off-site backups, and
    2. Software components used by the Managed Off-Site Backup for Cohesity service.

6. **Customer's Obligations.** The Customer is responsible for the following in accordance with industry best practices (as applicable):
    1. Providing the Provider with full and timely cooperation in the Provider's provision of the Managed Off-Site Backup for Cohesity service, including without limitation by: (a) providing the Provider with all information reasonably requested by the Provider, such as

backup requirement details and (b) making available Customer's designated contact reasonably accessible to the Provider;

2. Promptly notifying the Provider if the protected Resources are compromised, modified or infected by an unauthorized user, malware, virus, worm, or similar code or otherwise hacked or accessed by a person lacking permission to access the protected Resources;

3. If the Customer provisions Reserved Resources in excess of the specifications set out on the Order, including the storage necessary for processing the snapshot-based backups, the Provider is not responsible for any performance degradation, loss of backup data, or errors caused by over allocation;

4. Maintaining compatible firmware or software updates to all Customer-owned Cohesity hardware, and software used in production that replicates to the Provider's target;

5. Assisting with the completion of the On-boarding Provisioning Form provided by the Provider;

6. Providing the Provider's personnel with the Customer's asset discovery and documentation;

7. Providing all current process documentation in support of the Managed Off-Site Backup for Cohesity service and provide all assistance to the Provider as necessary to modify existing or implement new processes to streamline the delivery of the Managed Off-Site Backup for Cohesity service;

8. The Customer shall cooperate with the Provider regarding the performance of the Provider's obligations hereunder, including (without limitation):

    1. Notifying the Provider of any changes to its configurations that could potentially impact the services. For example, any data protection gaps such as a new virtual machine or physical server not being replicated because the Customer did not include the server in the Backup Policy; and

9. Prior to the expiration or termination of any Order for the Managed Off-Site Backup for Cohesity service, migrating and permanently deleting all of its Customer data residing on the Provider's target environment. Such data migration and deletion obligations are at the Customer's expense, unless otherwise agreed between the Customer and the Provider in a SOW for data migration services.

32. **Managed SteelDome InfiniVault.** The terms and conditions of this Section 3.32 are applicable to each Order that includes the Provider's Managed SteelDome InfiniVault.

    1. **Resources.**

1. Licensing. All required licensing is included in the Managed SteelDome InfiniVault service; and

2. Business Models. Storage capacity is available in a reserved business model as specified in the Order.

2. **Assets & Deliverables.**

    1. On-Boarding Project Plan. A documented detailed overview of all tasks associated with the Provider on-boarding process defined within scope of the mutually agreed upon Statement of Work. The purpose of this document is to track the ownership, progress, and completion of all applicable on-boarding tasks in collaboration between the Customer and the Provider;

    2. On-Boarding Provisioning Form. A detailed discovery document used for information gathering and collection of all Customer specific technical and infrastructure-related information for the sole purpose of the Provider providing the on-boarding service, integration, and management services to the Customer; and

    3. Protection Policies. The policies define the Managed SteelDome InfiniVault schedule of how often and when to take a snapshot of the data and the retention timeframe for that snapshot.

3. **On-Boarding Project Management.**

    1. Project managers. Both the Provider and the Customer shall appoint a project manager to serve as the primary contact point; and

    2. On-Boarding Project Management Engagement. The Provider's project manager and the Customer's project manager shall meet as required for the duration of the on-boarding process for the purpose of facilitating a successful relationship and overseeing the implementation of all resources and services defined in the Order and the On-boarding Provisioning Form, including but not limited to: (a) tracking the progress of the on-boarding and implementation process and all associated tasks; (b) reviewing other current or future projects or business plans that may impact the on-boarding of the backup resources and services; (c) weekly status reports to review the Provider’s performance in execution of the on-boarding project for delivery of all Cloud Resources and services; and (d) coordinating and planning for any new Equipment or software acquisitions specific to supporting the completion of on-boarding all Cloud Resources and services.

4. **On-Boarding Acceptance Test.**

    1. The On-Boarding Acceptance Test consists of non-service impacting data recovery test operations performed by the Provider in conjunction with the Customer, as well as data recovery verification

performed by the Customer, in each case as defined in the On-Boarding Project Plan;

2. The On-Boarding Acceptance Test is performed during the Provider's normal business hours of Monday to Friday, between 8:00 a.m. and 5:00 p.m., with the time zone being based on the data center location where services are located, excluding any federal or other holidays observed by the Provider in such location;

3. On-Boarding Acceptance Test Success Criteria. Successful completion of the On-boarding Acceptance Test shall be determined by validation of data recovery either to the original location or an alternative location. Any other target objectives will be documented in the On-Boarding Project Plan. If the On-Boarding Acceptance Test cannot be completed for technical reasons, the Customer will provide the Provider with any data or information reasonably requested by the Provider in order to enable the Provider to diagnose and resolve any problems associated with any failure to recover data during the On-Boarding Acceptance Testing. The Provider's project manager will notify the Customer via email or phone upon resolution of any such issues. After the Provider has notified the Customer that the problem has been resolved, the Customer and the Provider will promptly conduct a follow-up On-Boarding Acceptance Test to verify data recovery. This process will continue, if necessary, until the On-Boarding Acceptance Test Criteria meets the required success criteria; and

4. Notwithstanding anything to the contrary in this Service Schedule, if the Customer fails to timely participate in the On-Boarding Acceptance Test process as identified in the On-Boarding Project Plan, all of the Provider's on-boarding obligations will be considered completed and Provider will have no further obligations to the Customer regarding the On-Boarding Acceptance Test. In such event, the Customer may continue to exercise unlimited self-service testing.

5. **Service Delivery Management.**

    1. Service Delivery Management Contacts. The Customer shall appoint an individual who will serve as the primary point of contact for the Provider in connection with ongoing lifecycle management and delivery of the services, and the Provider shall appoint a point of contact; and

    2. Service Delivery Management Engagement. The Provider's and the appointed Customer's points of contact shall meet as required during the term of each service for the purpose of facilitating a successful relationship and overseeing the delivery and performance of each service, including but not limited to: (a) tracking the progress of the on-boarding and implementation process and all associated tasks; (b) reviewing other current or future projects or business

plans that may impact all services and/or delivery of all services; (c) coordinating and planning for any new equipment or software acquisitions or needs; (d) reviewing strategic and tactical decisions for the Customer in respect of the establishment, budgeting and implementation of the Customer's priorities and plans for information technology that may impact services and/or delivery of all services; and (e) monitoring and resolving concerns that may arise regarding the provision of all services, this SLA and/or the Service Schedule.

6. **Provider's Obligations.** The Provider is responsible for the following in accordance with industry best practices:
    1. Providing the software solution as specified by the Order;
    2. Providing documentation and guiding the Customer through the On-Boarding Acceptance Test and related processes;
    3. Providing ongoing support and education about the Customer's Managed SteelDome InfiniVault service at the Customer's request;
    4. Maintaining the underlying cloud infrastructure components to support the Managed SteelDome InfiniVault services such as compute, memory, storage and networking by following the Provider's guidelines for managing these environments;
    5. Providing Managed SteelDome InfiniVault capacity increase options via Order as recommended by the Provider or as otherwise requested by the Customer;
    6. In case of Provider-assisted restoration, assisting the Customer with initiating restoration from the Customer Managed SteelDome InfiniVault at the time of Disaster;
    7. Monitoring performance and status of the Managed SteelDome InfiniVault service in compliance with virtual appliance operating at expected CPU, memory and storage requirements;
    8. Providing enhanced on-boarding project management deliverables, to include:
        1. Weekly status call between the Provider on-boarding personnel and applicable Customer's contacts, and
        2. Weekly status report summarizing project tasks progress, project milestones, estimated and actual durations/completion dates and critical path items;
    9. Providing the Provider's published Managed SteelDome InfiniVault service documentation and managing supporting documentation, including:

1. Documented inventory and workload specifications (e.g., compute, storage, networking) of all Workloads within the scope of the Order, and

2. Documented Customer network security configurations, including firewall security policies, NAT policies and network security segmentation design;

10. Providing full installation, configuration and ongoing management of all services components required for delivery of Managed SteelDome InfiniVault service, to include (as applicable): software installation, setup and configuration both in the Customer's premises and the Provider's cloud data center environments used for provision of such services;

11. Providing full setup and configuration for backup of the protection policies for all Workloads within the scope and applicable to the Order and the On-Boarding Provisioning Form;

12. Providing full assistance with the development and creation of the Customer's protection policy definitions;

13. Providing live data recovery from Disaster declaration events;

14. Fulfilling Customer requests for increased capacity and other change requests; and

15. Providing ongoing updates, patching and maintenance for all the Provider-supplied service components required for delivery of the Managed SteelDome InfiniVault service, to include: software components used by the Managed SteelDome InfiniVault service.

7. **Customer's Obligations.** The Customer is responsible for the following in accordance with industry best practices (as applicable):

    1. Providing the Provider with full and timely cooperation in the Provider's provision of the Managed SteelDome InfiniVault services, including without limitation by: (a) providing the Provider with all information reasonably requested by the Provider, such as snapshot frequency and retention requirement details and (b) making available Customer's designated contact reasonably accessible to the Provider;

    2. At the Customer's discretion, restoring data by requesting support from the Provider in restoring data from the Managed SteelDome InfiniVault service;

    3. Promptly notifying the Provider if the Reserved Resources are compromised, modified or infected by an unauthorized user, malware, virus, worm, or similar code or otherwise accessed by a person lacking permission to access the protected Reserved Resources;

4. If the Customer provisions Reserved Resources in excess of the specifications set out on the Order, including the storage necessary for processing the snapshot-based recovery points, the Provider is not responsible for any performance degradation, loss of data, or errors caused by over allocation;

5. Ensuring all Customer-owned software, applications, devices, systems, processes, and services that maintain Customer data to be protected by the services delivered as part of this Agreement are covered as specified under Section 2.3.5 of this Service Schedule for the purposes of fulfilling the Agreement;

6. Maintaining all firmware or software updates to all Customer owned hardware, software, applications, devices, and systems in use with or protected by the Managed SteelDome InfiniVault services provided by the Provider;

7. Contacting all software, application, device, system, service, and service providers covered under this Agreement and adding the appropriate Provider's personnel as approved contacts for the purposes of fulfilling this Service Schedule;

8. Assisting with the completion of the On-boarding Provisioning Form provided by the Provider;

9. Providing all current and existing documentation of the Customer Primary Site(s) including without limitation, environment "as-built" documentation, application contact information, application dependencies, current backup strategy, disaster recovery plans, and any other documentation reasonably requested by the Provider;

10. Providing the Provider's personnel with the Customer's asset discovery and documentation;

11. Providing all current process documentation in support of the Managed SteelDome InfiniVault services and provide all assistance to the Provider as necessary to modify existing or implement new processes to streamline the delivery of the Managed SteelDome InfiniVault services;

12. The Customer shall cooperate with the Provider with regard to the performance of the Provider's obligations hereunder, including (without limitation):

    1. Providing the Provider with the required remote access to the Customer Equipment, as may be reasonable to permit the Provider to perform its obligations hereunder, and

    2. Notifying the Provider of any changes to its configurations that could potentially impact the services. For example, new data being added to the Managed SteelDome InfiniVault services because the Customer did not inform the Provider;

13. Prior to the expiration or termination of any Order for the Managed SteelDome InfiniVault service, migrating and permanently deleting all of its Customer data residing on any Equipment. Such data migration and deletion obligations are at the Customer's expense, unless otherwise agreed between the Customer and the Provider in a SOW for data migration services.

8. **Risks**

    1. There may be times when the Managed SteelDome InfiniVault service is unable to perform scheduled snapshots. Reasons for a snapshot failure include, but are not limited to, situations where a snapshot is unable to start during retry windows, services are temporarily unavailable, conflicts occur between resources, etc. In such events, the Provider will use reasonable efforts to attempt to remedy any potential snapshot failures, and Customer shall hold Provider harmless if a snapshot did not occur successfully.

33. **Connectivity Services General Terms:** The terms and conditions of Section 3.33 are applicable to each Order that includes the Provider's Connectivity Services described in Sections 3.34 - 3.36 and Section 3.43. below.

    1. **Order Effective Date.** Notwithstanding anything to the contrary in the Agreement, all Orders for Connectivity Services will be effective and binding as of the date of execution by the last Party to execute.

    2. **Service Jurisdiction.** Customer acknowledges and agrees that no intrastate circuit provided hereunder may:

        1. be extended by Customer from any Customer Location to an out of state location;

        2. be used for switched termination of interstate calls; or

        3. be used to transmit or otherwise carry more than 10% Interstate Traffic even if the physical end points of the circuit are both within the same state.
        "Interstate Traffic" includes Internet, interstate switched access, and/or any data or switched voice traffic that originates and terminates in different states. If Customer wishes to use or extend any intrastate circuit for the foregoing purposes, Customer must provide Provider with a written request ten (10) business days prior to any such use or extension.

    3. **Service Delivery and Requirements.**

        1. Customer must procure, at its sole cost and expense, all necessary connections within each Customer Location to access and interconnect with the Connectivity Services. Customer is solely responsible for all cross-connection charges necessary to connect to the Connectivity Services. Customer is not permitted to access the Provider Network except at Customer's side of the Service Demarc;

2. Customer must procure and maintain, at its sole cost and expense, Customer Equipment which is technically compatible with the Connectivity Services and the Provider Network; and

3. Unless otherwise noted in the Order, Customer is responsible for obtaining and maintaining, for the duration of the related Order Term, any necessary third-party licenses, approvals or permissions ("Location License(s)") for Provider to connect the Connectivity Services from the public rights-of-way to the Customer Equipment and Customer Location and/or to the Customer Location and install and/or utilize the necessary inside plant facilities and equipment, including power, riser conduit and fiber optics. Such Location License(s) must extend to the installation, maintenance, and retrieval of any Provider equipment.

4. **Compensation.**

    1. Without limiting Section 5.6.1 of the Agreement (Consequences of Termination), if the Customer cancels an Order prior to commencement of the Connectivity Services, Customer will be responsible for any and all third-party costs incurred by Provider, including the costs of carrier circuits, equipment costs, construction costs and building access costs. Notwithstanding Section 4.2 of the Agreement **(Payment)**, Provider will invoice those costs to Customer and the invoice will be due immediately upon receipt; and

    2. Customer is responsible for and will pay any and all fees (i) associated with obtaining and maintaining the Location Licenses, and (ii) assessed by any building owner, landlord or other third-party for the necessary license, approval and/or permission to install and maintain the Connectivity Service to a Customer Location.

5. **Customer's Obligations.** The Customer is responsible for the following in accordance with industry best practices:

    1. Supplying the Provider with information reasonably required to fulfill its obligations;

    2. Promptly notifying the Provider if the CPE is compromised, accessed by an unauthorized person, or infected with a virus, worm or similar malicious code; and

    3. When applicable, configuring the appropriate organization access permissions including the creation, modification, and deletion of end-user 11:11 Cloud Console account(s).

6. **Service Level Agreement.** The Service Level Agreement would be accessible at https://1111systems.com/legal/sla.

34. **11:11 Lit Services.** The terms and conditions of this Section 3.34 are applicable to each Order that includes 11:11 Lit Services.

    1. **Service Delivery and Requirements**

1. Subject to the terms and conditions contained herein, the Order and the Agreement, Provider will provide the Lit Services set forth in the Order. Provider shall use reasonable commercial efforts to cause the Service Commencement Date to occur by the Requested Install Date but Provider does not guarantee that installation will be completed by such Requested Install Date. After completing installation and testing, Provider will notify Customer that the Lit Services are ready. Customer is not entitled to any credits, SLA or otherwise, for claims related to the circuits arising more than (3) days after the installation or where Customer delays in testing the circuits;

2. If installation is delayed as a result of Customer's failure to fulfill its obligations under the Agreement (including, failure to obtain any necessary Location License(s)) (defined below), Provider will give Customer written notice to cure such failure within thirty (30) days. If Customer fails to cure within such period, the Service will be deemed to be delivered and the Service Commencement Date will be deemed to have occurred on the last day of such 30-day period;

3. If an Order requires a site survey or special construction in order to be completed (each, a "**Site Survey**"), then Customer may incur additional Monthly Recurring Charges or Non-Recurring Charges. Customer may cancel an Order with no early termination fees if additional fees of any kind arise after the Site Survey is conducted for the Services covered by the Order; and

4. Cross Connects are not included. Customer is responsible for all cross connects unless otherwise provided in the Order.

2. **Provider Network; Equipment**

    1. The Provider Network remains the sole and exclusive property of Provider or its supplier and nothing contained herein shall give or convey to Customer any right, title, or interest whatsoever in or to the Provider Network, which may never be deemed a fixture to real property. Customer may not adjust, encumber, repair, or attempt to repair the Provider Network, and may not remove or relocate any portion of the Provider Network without the prior written consent of Provider. Customer shall not pledge, lease, sell, transfer, mortgage, otherwise encumber, give away, remove, relocate, alter, or tamper with any portion of the Provider Network (or any notice of ownership thereon) or attach any electrical or other devices to the Provider Network. Provider reserves the right to make such filings or take such other actions as Provider, in its sole discretion, deems necessary or appropriate to evidence its ownership rights in the equipment. Customer agrees to execute all documents required to make such filings or accomplish such actions. If Customer causes any liens to be placed on the Provider Network, it must cause any such liens to be removed within thirty (30) days of Customer's knowledge thereof. Customer is liable to Provider for any loss or damage to the

Provider Network other than loss or damage resulting from an act or omission of Provider, its employees, contractors, or agents;

2. Provider reserves the right to, at any time, alter the Provider Network and any equipment therein or therewith and the features and functionality of the Provider Network or equipment. Provider will use reasonable efforts to schedule maintenance and replacement of equipment to minimize interference with, or interruption of, Services, but shall have no liability for interruptions in Services arising out of, or related to, maintenance or replacements. Provider may charge Customer for any repairs or replacement required due to damage or misuse of the Provider Network or equipment (normal wear and tear excepted). If any of Provider's equipment or any portion of the Provider Network is defective, damaged, destroyed, tampered with, stolen or otherwise removed, Customer must notify Provider immediately and may be held liable for repair or replacement if such notification is not immediately provided;

3. The Customer is responsible for installing and cabling the Provider's Network Equipment at the Customer's location(s). Upon request, the Provider offers installation services as an add-on, based on availability at the respective location(s);

4. Upon termination of Services, the Customer will contact Provider to schedule return of Provider-Supplied Equipment and any portion of the Provider Network and will be responsible for the costs of shipping the equipment to Provider. All equipment and the Provider Network must be returned within thirty (30) business days of circuit termination, in undamaged and full working order (normal wear and tear excepted). If the provided equipment or any portion of the Provider Network is not returned by Customer or is not returned in such condition as originally provided, Customer shall pay Provider the cost of repair or replacement, at fair market value, as reasonably determined by Provider;

5. If an Order specifies that the Customer is required to obtain space and power to support Provider equipment or any portion of the Provider Network for the Services, Customer must provide, at its sole cost and expense, the Site Environmental Specifications;

6. If applicable, the Customer agrees to provide all reasonable assistance to Provider in procuring and installing or activating necessary telecommunication circuits and facilities as necessary to provide telemetry from the Customer Locations to Provider's monitoring center(s) to enable out of band management. Customer shall provide adequate space and power to support the related telemetry equipment; and

7. If Provider deems it necessary, the Customer may be required to renumber the IP addresses assigned to Customer by Provider. Upon expiration, cancellation, or termination of a Service for any reason, Customer agrees to return to Provider any IP addresses or address blocks assigned to the Customer.

3. **Monitoring and Maintenance**

    1. Provider will perform all maintenance and repairs to the Provider Network as it deems necessary to ensure proper functioning of the Service. Provider will maintain the Provider Network at no additional charge to the Customer, except as provided in Section 3.34.3(b). Should any condition exist in any portion of the Provider Network that may impair the integrity of the Service or if Provider determines that it is necessary to conduct tests and adjustments to maintain the efficient working order of the Service, Provider will initiate and coordinate planned maintenance (or will cause such action to occur) which may include the deactivation of a network segment or other facility that supports the Service; and

    2. If all or part of the Provider Network requires restoration, replacement or repair by reason of an act or omission of Customer, or its employees, agents or contractors, such repair, replacement and/or restoration may be made by Provider, at Customer's sole expense, in accordance with Provider's then current time and materials rates plus applicable Taxes. If Provider dispatches personnel for a Provider Network failure caused by Customer equipment or personnel or due to an issue caused by Customer's equipment or other service providers, Provider will invoice, and Customer agrees to pay Provider's actual costs for time and travel associated with the dispatch.

4. **Burst Usage Payment Terms (Applies only if any Order provides for a Service with Burstable Usage)**

    1. Provider will measure Customer's bandwidth usage in five-minute intervals, for each point of connection between Customer and Provider (or its up-stream provider) in two categories: incoming and outgoing. At the end of each billing cycle, all data samples in each category will be sorted from highest to lowest and the top five percent (5%) of measurements will be discarded. The highest remaining data sample in the higher of the two categories will then constitute the bandwidth usage level for that particular billing cycle. "**Burst Usage**" means the amount of bandwidth usage for the particular billing cycle exceeding Customer's Minimum Committed Data Amount (as specified on the applicable Order.).

5. **Internet Over Wireless Service.**

    1. Internet of Wireless ("IOW") Services use cellular radio technologies to transmit data. IOW services have the following limitations:

1. IOW Services may be subject to transmission and service area limitations, interruptions caused by atmospheric, topographical or environmental conditions (including location topology or equipment positioning), or other conditions or activities affecting wireless transmission,
2. An external antenna may be required in some cases (for an additional charge) to boost signal strength, and
3. IOW Services may not be available at all locations;

2. Antenna or Dish Installation
    1. Customer is responsible for installation of any required satellite dish or cellular antenna (antenna) and associated equipment unless Customer purchases Provider's optional managed installation service,
    2. If Customer purchases the managed installation service, Provider will coordinate deployment of the dish or antenna, including site survey and installation support, subject to feasibility and clear line-of-sight requirements, and
    3. In all cases, Customer is responsible for ensuring that the dish or antenna installation locations are accessible and that any necessary permissions (e.g., roof rights, landlord consent) have been obtained;
3. Acceptable Use
    1. Customer must obtain Provider's prior written approval and execute a written agreement before it may install, deploy or use any of its own regeneration equipment or similar mechanism (for example, a repeater) to originate, amplify, enhance, retransmit or regenerate IOW Service, and
    2. USE OF IOW SERVICES FOR REMOTE MEDICAL MONITORING IS EXPRESSLY PROHIBITED;
4. Wireless Data Usage: Wireless data usage is the sum of all data transferred, typically measured in megabytes (MB) or gigabytes (GB), across the subscribed IOW Services during the usage period. Customer is responsible for all wireless data usage, including any usage and the associated charges that exceed the Customer's data plan, regardless of the cause for that usage;
5. Usage-based Data Plans:
    1. Usage-based data plans are based on the maximum amount of data usage available to the Customer before overage charges apply,
    2. Provider's usage-based IOW Services are meant to be used as a back-up to primary office Internet service, as a

temporary primary Internet service, machine to machine communication, or as an Access Transport for the Internet of Things ("IOT"),

3. Customers may not use IOW Services as a permanent primary Internet service without the express permission of Provider,

4. Nevertheless, regardless of Customer's intended use, Customer is responsible for choosing an adequate data plan,

5. Provider is not responsible for providing Customer with high data usage alerts. Customer has the option to purchase an edge device configured with software license to monitor its data usage for an additional fee, and

6. Customer understands that certain applications drive high data usage. Highest among these is video, including security cameras, YouTube videos, live video streams, video conferences, etc. If Customer expects to use IOW Services for such applications, a minimum data plan of 50 GB or 100 GB is recommended, which still may not be adequate. Provider recommends that Customers who choose low data plans block such applications from using its IOW Services;

6. Data Usage with Managed Services (including SD-WAN and Firewalls)

    1. Customer understands that some SD-WAN applications and failover firewall configurations allow for active-active configurations in which a Virtual Private Network ("VPN") tunnel is kept active across the IOW Services with some data traffic routed through that tunnel in order to optimize quality of service. Customer must specify to Provider if it intends to use the IOW Services in active-active mode prior to implementation as certain underlying providers expressly prohibit this configuration,

    2. Customer also understands that active-active configuration often results in high data usage and that if Customer intends to maintain IOW Services in an active-active configuration, a minimum data plan of 5 GB per location is advised, which still may not be adequate depending on the amount of traffic traversing the tunnel,

    3. Customers who choose low data plans will ensure all device configurations are in an active-passive configuration and not active-active mode, and

    4. In addition, certain managed service applications such as SD-WAN and Firewall may require configurations to "poll" for software updates frequently which can drive up data usage. It is the responsibility of the Customer to optimally configure

all managed service equipment in order to minimize IOW Services usage or, if Customer works with a managed services provider (be it Provider or a third-party), ensure said provider optimally configures all equipment in order to minimize IOW Services usage;

7. Speed-based Data Plans

    1. Speed-based data plans are based on maximum service speeds measured in Megabits per second (Mbps); however, the maximum speeds are not guaranteed and are subject to network availability,

    2. Speed-based data plans are intended for official business use only for business-critical data applications. Authorized business applications do not include streaming video, streaming audio, web hosting, public Wi-Fi or guest Wi-Fi. Customer warrants that it will only use a speed-based data plan and the Services arising therefrom or related thereto for business-critical data applications and such usage does not include any unauthorized applications,

    3. Provider may slow speeds on plans after the committed data usage is reached; the Customer has the option to buy additional data usage to restore speeds, and

    4. For speed-based data plan users, Provider will identify users with excessive usage and review if the usage is in line with official business use for business-critical applications and business critical data. If excessive usage does not comply with these terms, Customer must immediately bring the service usage within the terms. Notwithstanding anything to the contrary in the Agreement, if usage is not brought within compliance, Provider may discontinue service or move the user to a traditional usage-based data plan with overage charges. If excessive usage is within business use, Provider will work with Customer to identify and implement an alternative solution, included alternative Internet over Anything (IOA) Services, discussing opportunities for Wi-Fi offload, application settings, and other network efficiency adjustments such as using a managed services to restrict usage.

35. **11:11 Dark Fiber.** The terms and conditions of this Section 3.35 are applicable to each Order that includes 11:11 Dark Fiber services.

    1. **Service Delivery and Requirements**

        1. Subject to the terms and conditions contained herein, the Order and the Agreement, Provider will lease to Customer the Dark Fiber which will constitute the Service set forth in the Order. After completing

installation and testing the Dark Fiber to determine that it meets the Dark Fiber Specifications, Provider will deliver the Dark Fiber by notifying Customer and providing testing results demonstrating compliance with the Dark Fiber Specifications. Provider shall use reasonable commercial efforts to cause the Service Commencement Date to occur by the requested Install Date set forth in the Order but Provider does not guarantee that installation will be completed by such Requested Install Date; and

2. If delivery is delayed as a result of Customer's failure to fulfill its obligations under the Agreement (including failure to obtain any necessary Location License(s)), Provider will give Customer written notice to cure such failure within thirty (30) calendar days. If Customer fails to cure within such period, the Service will be deemed to be delivered and the Service Commencement Date will be deemed to have occurred on the last day of such 30-day period.

2. **Network Relocation and Underlying Rights**

    1. Provider may relocate all or any portion of the Provider Network segments or any of the facilities required to provide Customer with the Dark Fiber: (i) if a third-party with legal authority orders or threatens to order such relocation (e.g. through eminent domain, nationalization, or expropriation), (ii) in order to comply with applicable laws, or (iii) for bona fide operational reasons;

    2. Provider agrees to provide Customer fourteen (14) calendar days prior notice of a relocation, if reasonably feasible;

    3. Provider has the right to direct such relocation, including the right to determine the extent of, the timing of, and methods to be used for such relocation, provided that any relocation:

        1. is constructed and tested in accordance with the Dark Fiber Specifications,

        2. does not result in a materially adverse change to the operations, performance, or connection points with the Provider Network of Customer, and

        3. does not unreasonably interrupt service on the Dark Fiber;

    4. Notwithstanding anything to the contrary contained herein, all Dark Fiber Services to be delivered under an Order are subject and subordinate to the Underlying Rights. "Underlying Rights" means the right of way, franchise, access rights and other agreements obtained by Provider for the construction, operation, and maintenance of its network. All Dark Fiber Services provided to Customer are expressly made subject and subordinate to each and every limitation, restriction or reservation affecting the Underlying Rights. Upon the expiration or other termination of an Underlying Right that is necessary in order to grant, continue or maintain any Dark Fiber

Services, Provider shall use commercially reasonable efforts to renew such Underlying Right or to obtain an alternate right of way. If Provider is required to relocate any part of its network facilities used or required in providing Dark Fiber Services to Customer as the result of a lack of an Underlying Rights, Provider shall determine the extent of, the timing of, and methods to be used for such relocation. Should Provider determine that the cost of relocation or obtaining the necessary Underlying Rights are not commercially reasonable, Provider in its sole discretion may terminate the Agreement or the applicable Order upon thirty (30) days' notice to Customer.

3. **Use of Dark Fiber**

    1. Customer may use the Dark Fiber for any lawful purpose, including for the provision of telecommunications services, information services and capacity to its customers;

    2. Customer may not, without the express written consent of Provider, perform, or contract with any third-party to perform, any repairs or maintenance to any Dark Fiber. Customer will not install any equipment to be used with the Dark Fiber that does or could damage or interfere with the Provider Network; and

    3. Customer shall not, directly or indirectly, create or be permitted to impose any lien on the Dark Fiber or on the rights or title relating thereto, or any interest therein, or in the Agreement. Customer shall promptly, at its own expense, take such action as may be necessary to duly discharge any lien created by it or permitted by it to be imposed on the Dark Fiber.

4. **Maintenance**

    1. Provider will perform all maintenance and repairs to the Provider Network as it deems necessary to ensure proper functioning of the Service. Provider will maintain the Provider Network at no additional charge to Customer, except as provided in Section 3.35.4.b. Should any condition exist in any portion of the Provider Network that may impair the integrity of the Service or if Provider determines that it is necessary to conduct tests and adjustments to maintain the efficient working order of the Service, Provider will initiate and coordinate planned maintenance (or will cause such action to occur) which may include the deactivation of a network segment or other facility that supports the Service;

    2. If all or part of the Provider Network requires restoration, replacement, or repair by reason of an act or omission of Customer, or its employees, agents or contractors, such repair, replacement and/or restoration may be made by Provider, at Customer's sole expense, in accordance with Provider's then current time and materials rates plus applicable Taxes. In the event that Provider dispatches personnel for a reported Provider Network failure caused

by Customer equipment or personnel or due to an issue caused by Customer's equipment or other service providers, Provider will invoice, and Customer agrees to pay Provider's actual costs for time and travel associated with the dispatch; and

3. Customer is responsible, at its sole cost and expense, for acquiring, installing, operating, or otherwise making provision for and maintaining all electronic and optronic equipment necessary for Customer to light the Dark Fiber and/or for Customer's transmissions over the Dark Fiber.

5. **Dark Fiber Specifications and Fiber Optic Cable Splicing, Testing and Acceptance Standards**

Specification
Attenuation at 1310 nm
Non-Dispersion Shifted Fiber (NDSF)
Attenuation at 1550 nm
Non-Dispersion Shifted Fiber (NDSF)
Fiber Cable Construction
Strength Member
Cable Jacket Covering

1. The maximum loss value measured between Customer Locations with an industry-accepted laser source and power meter, or an OTDR, shall have an attenuation of less than or equal to the following:

   1. At 1310 nm: (0.4 dB/km x km of fiber) + (number of connectors x 0.50 dB) + (0.15 dB x number of splices) + 1.0 dB
   2. At 1550 nm: (0.3 dB/km x km of fiber) + (number of connectors x 0.50 dB) + (0.15 dB x number of splices) + 1.0 dB

36. **11:11 SD-WAN and Managed Connectivity.** The terms and conditions of this Section 3.36 are applicable to each Order that includes the SD-WAN and Managed Connectivity services.

    1. **Service.**

        1. SD-WAN and Managed Connectivity services expand the traditional network services (as described in the Lit Services and Dark Fiber

Service Supplements) to include Customer Premises Equipment (CPE) and its support. Standard service deployment includes Provider-Supplied CPE, device configuration, installation, device maintenance, warranty support, device administration, proactive monitoring, and proactive support. Devices vary based on the Customer's requirements and include. Still, they are not limited to SD-WAN-enabled managed Firewalls (as described in section 3.1), Network Switches, Network Routers, Broadband/Cable Modem, Wireless Router/Modems, and Network Interface Devices (NID). Standard service delivery for SD-WAN deployment includes engineering effort of 10 hours per each SD-WAN site managed by Provider. At the end of service delivery, Provider may charge Customer for engineering efforts exceeding a collective 10 hours per site, based on current market rates.

2. **Service Demarcation.**

    1. CPE provided and managed by the Provider as Provider-Supplied Equipment, shall be placed on the Customer premises between the Wide Area Network (WAN) (lit or dark fiber services) and the Customer Local Area Network (LAN) environment. The point of service demarcation shall be extended for managed services to the LAN side of the router, firewall or other managed CPE device. For unmanaged telecommunications service, the demarcation shall be the output jack (typically an RJ45 or fiber optic ports) of the network equipment. Systems maintenance, testing, and support shall be extended to the demarcation on the LAN side of the CPE. It shall not extend into the Customer LAN. While the Provider's technicians may assist the Customer with trouble isolation into the LAN, the Customer remains solely responsible for maintenance and repair of the LAN environment. The Provider accepts no responsibility for the accuracy of any tests, suggested outage causes, or repair costs for any part of the Customer LAN after the point of demarcation on the managed device.

3. **Provider's Obligations.** The Provider is responsible for the following in accordance with industry best practices:

    1. Configuring the managed devices per an agreed configuration plan based on the Customer's requirements, infrastructure, and availability;

    2. Designing the Customer network based on the Customer's requirements and configure the managed devices to support that design once the Customer approves;

    3. Providing replacement hardware in the event of a failure; and

    4. In some cases, the Provider may agree to provide monitoring services for CPE not supplied by Provider. In such cases, the Provider will provide services, as authorized by and agreed with the

Customer, that may include some or all of the following: device configuration, backup configuration support, device administration and change management, proactive monitoring, VPN administration, network management portal access for real-time performance monitoring, graphs and reports.

4. **Customer's Obligations.** The Customer is responsible for the following in accordance with industry best practices:

    1. Promptly providing all information requested by Provider's technical team related to existing network policies and configurations associated with the old equipment, if applicable, to ensure a seamless migration process and to minimize any potential conflicts or challenges that may arise during the transition. In the event Customer requires additional assistance or expertise for the actual transfer of rules from the old equipment to the new SD-WAN infrastructure, then Provider is prepared to offer such services as part of a separate paid professional services engagement the terms of which will be mutually agreed to in writing signed by the Parties;
    2. Providing environmentally controlled rack space and power for the managed devices;
    3. Providing the Provider with out-of-band access;
    4. Installing and cabling the Provider-Supplied Equipment at the Customer's location(s);
    5. Providing unobstructed access to the equipment for maintenance, troubleshooting, and replacement;
    6. Informing the Provider of its existing network design, the applicable IP addresses, the need for high availability, SD-WAN policies, the desired network operation with the managed CPE, and the VPN layout if included;
    7. Confirming the configuration plan prior to installation and that the managed devices are configured per the Customer's preferences after service activation;
    8. Confirming the network design for implementation and its correct operation upon installation;
    9. Upon service connection, providing a test plan to confirm that the network's performance and failover are functioning per the plan. The Customer will allow the Provider ample time to resolve the issue identified during the testing period;
    10. Procuring and maintaining the hardware and software components required for the Local Monitoring Probe. Customer will ensure the proper installation of the Local Monitoring Probe within the premises and shall be responsible for securing and configuring it to align with its corporate policies and specific network requirements.

Customer is responsible for ongoing management tasks, including, but not limited to, patching, upgrades, and updates in accordance with industry best practices; and

11. Should the Provider provide the Customer monitoring services for CPE not supplied by Provider, the Customer will be required to:

    1. Authorizing Provider access the Customer's equipment and making changes to settings and configurations,

    2. Providing the Provider with the necessary login credentials, including login names, passwords, and IP addresses, to access their equipment for management and administration purposes,

    3. Acknowledging that such services may not be as extensive for CPE not supplied by Provider as for Provider-Supplied Equipment due to differences in manufacture and technology from the standard equipment deployed by the Provider and using the Provider's network management platform and expertise, and

    4. Agreeing and acknowledging that, except in cases of gross negligence or willful misconduct, to hold the Provider harmless for any damage to CPE, associated devices, associated services, or data resulting from actions taken by the Provider in the process of monitoring, administering, and managing the CPE.

37. **11:11 DRaaS for Azure.** The terms and conditions of this Section 3.37 are applicable to each Order that includes 11:11 DRaaS for Azure and are accessible at https://1111systems.com/legal/1111-draas-azure-service-terms/

38. **11:11 Shared Workplace.** The terms and conditions of this Section 3.38 are applicable to each Order that includes 11:11 Shared Workplace Recovery services and are accessible at https://1111systems.com/legal/1111-workplace-recovery-shared-service-terms-na/

39. **11:11 Dedicated Workplace.** The terms and conditions of this Section 3.39 are applicable to each Order that includes 11:11 Dedicated Workplace Recovery services and are accessible at https://1111systems.com/legal/1111-workplace-recovery-dedicated-service-terms-na/

40. **Cloudflare.** The terms and conditions of this Section 3.40 are applicable to each Order that includes the Provider's Cloudflare services.

    1. **Resources.**

        1. Application Services. For each quantity of "Cloudflare Application Business Plan+ (Per Zone)" specified in Order:

            1. Customer shall be entitled to a bundle of WAF, DDOS, DNS, and CDN features enabled for a single apex domain,

2. Customer shall be entitled to 1TB monthly throughput usage capacity specific to each Zone,
3. Unused throughput capacity for any given Zone cannot carry over month to month or contribute to other Zones, and
4. Throughput capacity usage exceeding the monthly 1TB allowance will be billed monthly in arrears per TB;

2. Zero Trust Services. Customer shall be entitled to one (1) unique seat for each quantity of the following services specified in the Order:
    1. Cloudflare Access,
    2. Cloudflare Gateway,
    3. Cloudflare Advanced Browser Isolation,
    4. Cloudflare Area 1 Enterprise,
    5. Cloudflare Zero Trust Essentials.
        1. Cloudflare Zero Trust Essentials bundle includes Cloudflare's: Access, Gateway, Tunnel, mTLS, and WARP.
        2. Cloudflare Zero Trust Essentials Plus bundle includes Cloudflare's: Access, Gateway, Tunnel, mTLS, WARP, and Area 1 Email Security.
    6. Cloudflare Zero Trust Advanced.
        1. Cloudflare Zero Trust Advanced bundle includes Cloudflare's: Access, Gateway, Tunnel, mTLS, WARP, RBI, and CASB.
        2. Cloudflare Zero Trust Advanced Plus bundle includes Access, Gateway, Tunnel, mTLS, WARP, RBI, CASB, and Area 1 Email Security.
    7. Cloudflare Zero Trust Premier.
        1. Cloudflare Zero Trust Premier bundle includes Access, Gateway, Tunnel, mTLS, WARP, RBI, CASB and DLP.
        2. Cloudflare Zero Trust Premier Plus bundle includes Access, Gateway, Tunnel, mTLS, WARP, RBI, CASB, DLP, and Area 1 Email Security.

2. **Provider's Obligations.** The Provider is responsible for the following in accordance with industry best practices:
    1. Provisioning Customer account within the Cloudflare portal;
    2. Enabling feature/license entitlements as defined in Order;

3. Providing quick-start guides referencing Cloudflare developer documentation for customer self-deployment and self-management of the service;
4. Billing in the arrears for consumption / usage-based overages; and
5. If Premium Management is specified in Order, Provider is responsible for:
    1. Providing project management services to deploy Cloudflare services in Order,
    2. Providing guided onboarding configuration in Cloudflare portal,
    3. Providing ongoing change configuration in Cloudflare portal at Customer request,
    4. Providing troubleshooting in Cloudflare portal at Customer request, and
    5. Providing initial tuning of WAF and CDN policies with ongoing tuning at Customer request.

3. **Customer's Obligations.** The Customer is responsible for the following in accordance with industry best practices (as applicable):
    1. Adherence to Cloudflare's Enterprise Subscription Agreement set out at https://www.cloudflare.com/enterpriseterms/ which may be modified from time to time;
    2. To the extent not inconsistent with Provider's terms and conditions, adherence to Cloudflare's Service-Specific Terms set out at https://www.cloudflare.com/service-specific-terms-application-services/, which may be modified from time to time;
    3. Payment for any usage-based overages billed in the arrears;
    4. Assisting with the completion of the On-boarding Provisioning Form provided by Provider;
    5. Installation, configuration, ongoing administration and troubleshooting of WARP client software, cloudflared service, and any other software or service component on end user client and server machines to facilitate Cloudflare connectivity; and
    6. Maintaining up to date versions of Cloudflare WARP, cloudflared, and all other Cloudflare software and service components to facilitate Cloudflare connectivity.
4. **Modifications and Usage Based Components:** Customer is responsible for the following in accordance with industry best practices (as applicable):
    1. Cloudflare may change product bundles, features, services, and pricing at any time. Provider reserves the right to modify Customer

order, service terms, and pricing at any time as necessary to align with Cloudflare provided offerings; and

2. Certain Cloudflare products or services may have usage-based components which bill in the arrears. All capacity usage that is over the monthly allowance will be billed in arrears on a monthly basis.

41. **Managed AWS Direct Connect On-ramp.** The terms and conditions of this Section 3.41 are applicable to each Order that includes 11:11 Managed AWS Direct Connect On-ramp services.

    1. **Provider's Obligations.** The Provider is responsible for the following in accordance with industry best practices (as applicable):

        1. For each quantity of 11:11 Managed AWS Direct Connect Hosted On-ramp connection specified in Offer, provision an AWS Direct Connect Hosted connection with the corresponding bandwidth; and

        2. For each quantity of 11:11 Managed AWS Direct Connect Dedicated On-ramp connection specified in Offer, provision an AWS Direct Connect Dedicated connection via a physical cross connect to the AWS on-ramp router.

    2. **Customer's Obligations.** The Customer is responsible for the following in accordance with industry best practices (as applicable):

        1. AWS Direct Connect (DX) port hour charges and data transfer charges as outlined at https://aws.amazon.com/directconnect/pricing/;

        2. Public IP addresses to support public Virtual Interface (VIF) peering;

        3. Providing AWS Account ID, VLAN IDs, and other details as necessary for Provider to provision the service;

        4. Ordering the Dedicated DX port from AWS and providing LOA to Provider for physical extension for each 11:11 Managed AWS Direct Connect On-ramp (Dedicated DX) service specified in the Order;

        5. Hosted Connection Cancellation. If Customer chooses to cancel an 11:11 Managed AWS Direct Connect Hosted On-ramp connection, the following obligations and responsibilities apply:

            1. Decommissioning of AWS side connection. Prior to submitting a request for disconnection to the Provider, Customer agrees to undertake the decommissioning of the AWS side of the Direct Connect connection. Decommissioning entails the removal of all network configurations, resources, and associated infrastructure pertaining to the AWS Direct Connect service. This includes, but is not limited to, the termination of Virtual Private Gateways (VGWs), Virtual Interfaces (VIFs), Direct Connect

Gateway (DXGW), and associated networking components within the AWS environment,

2. Confirmation of decommissioning. Customer shall provide evidence of the decommissioning of the AWS side of the Direct Connect connection to Provider. This evidence may include screenshots, network diagrams, or other documentation demonstrating the removal and cessation of relevant AWS resources and configurations,

3. Compliance with Provider Procedures: Customer acknowledges and agrees to comply with any additional procedures or requirements stipulated by Provider regarding the cancellation and decommissioning process for AWS Direct Connect services, and

4. Non-Compliance: Failure to adhere to the decommissioning requirements outlined herein may result in additional charges, penalties, or liabilities imposed by Provider.

42. **Managed Circuit.** The terms and conditions of this Section 3.42 are applicable to each Order that includes 11:11 Managed Circuit services.

    1. **Provider's Obligations.** The Provider is responsible for the following in accordance with industry best practices (as applicable):

        1. Providing contact information for Customer to report Customer-Owned telecommunications degradation or service disruptions;

        2. Investigating reported issues and work with the telecommunications vendors to identify root causes;

        3. Managing the lifecycle of reported incidents from initial identification through resolution and closure;

        4. Escalating complex or severe issues to higher-tier Support teams within the telecommunications provider for further investigation and resolution;

        5. Keeping Customer informed periodically of progress updates, expected resolution timelines, and any Customer action items; and

        6. If necessary, assisting the Customer in obtaining an LOA to allow the Provider’s Support team to raise issues on its behalf.

    2. **Customer's Obligations.** The Customer is responsible for the following in accordance with industry best practices (as applicable):

        1. Reporting Customer-Owned telecommunications incidents, circuit degradation or service disruptions to the Provider’s Support team;

        2. Notifying the Provider of any changes in circuit type, ranging from upgrades or downgrades to cancellations with third-party vendors;

3. Cooperating with Provider's Support technicians and telecommunication service providers, providing information, and following provided guidance and instructions for troubleshooting technical difficulties and/or incident management;

4. Allowing for escalation of issues by the Provider's Support team when necessary; and

5. Providing the necessary LOA to the Provider authorizing its Support team to raise issues on its behalf.

43. **11:11 Managed Operating System.** The terms and conditions of this Section 3.43 are applicable to each Order that includes 11:11 Managed Operating System services and at least one of the Provider's services that are described in Section 3.1 (11:11 Cloud) and/or Section 3.2 (11:11 Secure Cloud) of this Schedule.

    1. **Resources.**

        1. Operating System (OS). Customer licensed Operating Systems contracted to receive Managed Operating System services.

            1. OS updates are contracted on a per VM basis,

            2. OS updates with OS management services are contracted on a per VM basis, and

            3. OS updates and OS updates with OS management services are mutually exclusive and may not be associated with the same VM.

    2. **Service Delivery Management.** The Customer shall appoint an individual who will serve as the primary contact point for the Provider in connection with ongoing lifecycle management and delivery of the services, and the Provider shall appoint a point of contact.

    3. **Provider's Obligations.** The Provider is responsible for the following in accordance with industry best practices:

        1. Maintaining the underlying OS monitoring and software update tools and processes to facilitate delivery of Managed Operating System services;

        2. Maintaining a secure process for managing administrative rights and password security for each Managed OS;

        3. Providing Customer with one or more methods of access to Provider resources, supporting communications related to both scheduled and reactive OS management tasks and functions;

        4. Providing initial configuration of Managed Operating System services, including automated OS update scheduling for OS updates;

5. Identifying specific change control processes as applicable;
6. Establishing monitoring thresholds and notification preferences for OS Updates with OS Management services;
7. In case of Provider-assisted OS restoration, initiating the OS restore process from the most recent available backup or as directed by Customer; and
8. In-place OS version upgrades (e.g. 1.x to 2.x) are not included with either OS updates or OS updates with OS management services and are not generally recommended, however, in-place OSS version upgrade services are available under certain conditions and may be contracted for an additional per incident per OS fee if Customer accepts the associated risks.

4. **Customer's Obligations.** The Customer is responsible for the following in accordance with industry best practices:
    1. Providing and maintaining vendor supported versions of OS software either directly or through Provider's Services via a separate licensing Order;
        1. For Customer provided OS licenses, providing verification of licenses and necessary license keys applicable to Customer-provided software prior to service provision by Provider
    2. Providing system administration security-level (e.g. admin or root-level) access for each managed OS and, if Customer retains system administration security-level access, permit such access to be traced by Provider;
    3. Providing information reasonably requested to fulfill its obligations, including, without limitation, OS configuration and support parameters and access to backup data specific to any supported OS;
    4. At the Customer's discretion, restoring an OS either through the self-service 11:11 Cloud Console or by requesting support from the Provider; and
    5. Having sufficient storage available to support each Managed OS per OS vendor recommendations.
5. **Risks.**
    1. Should an applied OS patch, OS update or OS upgrade result in a failure of the OS to restart or if any other functional problems are introduced via the referenced OS changes, the sole remediation action available from Provider is the restoration of the effected VM(s) from an available backup as directed by Customer;

44. **11:11 Managed Database.** The terms and conditions of this Section 3.44 are applicable to each Order that includes 11:11 Managed Database services (Managed

DB services) and at least one of the Provider's services that are described in Section 3.1 (11:11 Cloud) and/or Section 3.2 (11:11 Secure Cloud) of this Schedule.

1. **Resources.** Managed Database(DB). Customer licensed database contracted to receive Managed DB services:
    1. Initial database installation and configuration on pre-provisioned 11:11 infrastructure, which must include 11:11 OS updates with 11:11 Managed Operating System services and backup services that are compatible with the contracted database.
2. **Service Delivery Management - Points of Contact.** The Customer and Provider shall each appoint an individual who will serve as the primary points of contact points for ongoing lifecycle management and delivery of the services.
3. **Provider's Obligations.** The Provider is responsible for the following in accordance with industry best practices:
    1. Maintaining the underlying database monitoring and software update tools and processes to facilitate delivery of Managed Database services;
    2. Establishing monitoring thresholds and notification preferences for database software updates;
    3. 24x7x365 database incident management;
    4. Database Change and problem management;
    5. Database configuration changes, subject to Customer's approval;
    6. Escalation and coordination of issues and recommendations with database vendors as and when required, subject to Customer approval;
    7. Database cloning from production data;
    8. Database restores from exports, database dumps or backups;
    9. Maintaining a secure process for managing administrative rights and password security for each managed database;
    10. Outside of available Per Incident Database Upgrade services, database software updates are limited to minor/point releases, which are subject to testing in a Customer's environment (unless under emergency maintenance conditions) and Customer approval;
    11. Providing Customer with one or more methods of access to Provider resources, supporting communications related to both scheduled and reactive database management tasks and functions; and
    12. In case of Provider-assisted database restoration, Provider will initiate the database restore process from the most recent available backup or as directed by Customer.

4. **Customer's Obligations.** The Customer is responsible for the following in accordance with industry best practices:
    1. Providing and maintaining vendor supported versions of database software either directly or through Provider's Services via a separate licensing Order;
    2. Providing verification of Customer provided database licenses and necessary license keys applicable to Customer-provided software prior to service provision by Provider;
    3. Providing system administration security-level (e.g. admin level) access for each managed database and, if Customer retains system administration security-level access, permit such access to be traced by Provider;
    4. Providing information reasonably requested to fulfil its obligations, including, without limitation, database configuration and support parameters and access to backup data specific to any supported database;
    5. Having sufficient storage available to support each managed database per database vendor recommendations; and
    6. Providing a means of testing applied database patches, database updates or database upgrades to facilitate Customer validation of database performance and functionality.
5. **Risks.**
    1. Should an applied database patch, database update or database upgrade result in a failure of the database to restart or if any other functional problems are introduced via the referenced database changes, the sole remediation action available to Customer by Provider is the restoration of the impacted database from an available backup as directed by Customer.
    2. Managed Database Services do not include:
        1. Support for any database configurations that are not supported or recommended by the database vendors,
        2. Application security policy definition, creation or enforcement,
        3. Application, modification or deletion of database objects, schemas, views, procedures, functions and jobs via database management tools,
        4. Resolution of issues caused by software or applications not managed by Provider, and
        5. Major database version upgrades, which are subject to additional fees and an Order.

45. **11:11 DRaaS for Cohesity.** The terms and conditions of this Section 3.45 are applicable to each Order that includes the Provider's 11:11 DRaaS for Cohesity service.

    1. **Resources.**

        1. Replication Storage. The resources that comprise the 11:11 DRaaS for Cohesity service are provided by Shared Equipment that provides storage capacity in a multi-tenant environment;

        2. IaaS Storage. The types of storage available are Accelerated, and/or SSD. Storage types comprising the environment are specified in the Order;

        3. CPU & RAM. These Cloud Resources are available as Shared Resources. CPU & RAM comprising the environment are specified in the Order;

        4. Bandwidth. Bandwidth is included, subject to abiding by the Excessive Use Section on the Acceptable Use Policy;

        5. Licensing. All required licensing is included in the 11:11 DRaaS for Cohesity service; and

        6. Business Models. Capacity is available in a reserved plus burst business model for Shared Equipment as specified in the Order.

    2. **Provider's Obligations.** The Provider is responsible for the following in accordance with industry best practices:

        1. Onboarding the Customer into the Provider's Cloud Services by giving access to the service and guiding the Customer through the process of deploying the service;

        2. Providing documentation, project management, and demonstrate the failover steps for a full site failover to the Customer on the Provider's test environment. In the event that a Customer would like the Provider to assist with design, implementation or testing of a partial site failover, additional i-Tech fees will apply;

        3. Providing ongoing support and education to the Customer about the Service upon request;

        4. Creating Virtual Data Center(s) consisting of compute, memory, storage infrastructure, and network bandwidth per specifications detailed in the Order;

        5. Maintaining the underlying cloud infrastructure components such as compute, memory, storage and networking by following the Provider's guidelines for managing these environments;

        6. Providing the Customer with the URL and authentication credentials to access the Customer's Cloud Resources;

7. Assigning external and internal IP addresses for the Recovery Site virtual router per the Customer-provided requirements;
8. In case of Provider-assisted Failover, assisting Customer with initiating Failover at-time-of-Disaster;
9. In the event of a Disaster and Failover to the Recovery Site, the Provider can, if needed, assist the Customer with Failback from Disasters to Customer Primary Site for additional i-Tech fees;
10. Fulfilling Customer requests for increased capacity and other change; and
11. Providing ongoing updates, patching and maintenance for all the Provider-supplied service components required for delivery of the 11:11 DRaaS for Cohesity service, to include:
    1. Infrastructure hosting the off-site replicas, and
    2. Software components used by the 11:11 DRaaS for Cohesity service.

3. **Customer's Obligations.** The Customer is responsible for the following in accordance with industry best practices (as applicable):
    1. Unless specified on the Order, implementing dedicated physical or virtual network security appliance, managing Firewall(s) including but not limited to the configuration of Network Address Translation (NAT) Access List, Virtual Private Network (VPN), Dynamic Host Configuration Protocol (DHCP), Load Balancing, and static routing;
    2. Providing compute, memory, storage and network requirements for each Virtual Data Center and creating Virtual Data Center network and role-based security policies;
    3. Ensuring that only VMware based Workloads are replicated to the Provider and that the Virtual Machine environment matches specifications as defined in the Provider's Product Compatibility Matrix. By purchasing this product, the Customer specifically acknowledges that workloads other than VMware vSphere are not supported;
    4. Configuring Cohesity Protection at the Primary Site; Creating Recovery Groups and initiating replication on Virtual Machines selected for replication;
    5. Notifying the Provider before making any changes to the Primary Site that might affect the DRaaS service, including but not limited to, any upgrades or patches to Cohesity, the underlying virtualization layer, or the network;
    6. Ensuring Virtual Machines match specifications as defined in the Provider's then-current Product Compatibility Matrix;

7. Creating and testing Recovery Plan;
8. Initiating Failover at-time-of-test and at-time-of-Disaster;
9. In case of Provider-assisted Failover, declaring a Disaster following the Provider's guidelines;
10. Maintaining operating systems and applications installed on the Customer's Virtual Machines or in the Customer's Virtual Data Center, including, but not limited to, providing support, patching, upgrades, updates and anti-virus software in accordance with industry best practices. Compatible firmware or software updates to all Customer-owned Cohesity hardware, and software used in production that replicates to the Provider's target;
11. Providing Virtual Machine and application log monitoring;
12. In the event of a Disaster and Failover to the Recovery Site, in order for the Customer to Failback to the Primary Site, the Customer needs to recreate the original environment in the Primary Site by providing similar compute, memory, storage and network resources, Virtual Machines on the Customer's hosts, Cohesity Cluster, enable site peering to Recovery Site, set up and configure Replication Groups and Policies before replicating data from Recovery Site. The Customer is responsible for paying the associated i-Tech fees if assistance from the Provider is required;
13. Promptly notifying the Provider if the Cloud Resources are compromised, accessed by a person lacking permission to access the Cloud Resources, or infected with a virus, worm or similar malicious code;
14. Informing the Provider at the time any of these changes occur in the Primary Site:
    1. Increasing resource capacity in Primary Site in relation to replicated Virtual Machines without increasing Cloud Resources at Recovery site, and
    2. Ensuring that there is enough bandwidth at Primary Site to enable initial replication and successive incremental changes of data to Recovery Site; and
15. Prior to the expiration or termination of any 11:11 DRaaS for Cohesity service, migrating and permanently deleting all of its Customer data residing on the Provider's target environment. Such data migration and deletion obligations are at the Customer's expense, unless otherwise agreed between the Customer and the Provider in a SOW for data migration services.

4. **Risks.**

1. Failing to notify Provider before making any changes to the Primary Site may impact the performance and functionality of the DRaaS service;

2. Testing can be interrupted and/or stopped by the Provider if a Testing event has run long enough to impact replication or the underlying infrastructure; and

3. Where Customer's utilization exceeds the specifications set out on the Order, Customer may experience performance degradation or errors caused by over allocation.

5. **Encryption.**

    1. Storage Encryption. Replication Storage is encrypted at rest with AES-256 CBC (Cipher Block Chaining).

6. **Service Levels.**

    1. Service Levels. Recovery Time Objective (RTO) and Recovery Point Objective (RPO) SLAs are accessible at https://1111systems.com/legal/sla/

7. **Recovery Testing.**

    1. All recovery testing should last no longer than seventy-two (72) hours. If the failover test is to exceed 72 hours, this will be considered a permanent failover, and the Customer must commit to migrating virtual machines from Replication Storage to IaaS Storage;

    2. If the Customer is unable to migrate failover workloads after seventy-two (72) hours

        1. The Provider holds the right to power down the failover test environment, and

        2. The Customer can ask for assistance from the Provider to migrate workloads for an agreed upon i-Tech fee.

46. **Network Assessment.** The terms and conditions of this Section 3.46 are applicable to each Order that includes the Provider's Network Assessment consulting services.

    1. **Provider's Obligations.** For network environments within scope, Provider is responsible for the following in accordance with industry best practices:

        1. Providing an audit of preexisting customer network documentation;

        2. Providing a review and analysis of overall network performance;

        3. Providing a review and analysis of overall network health;

        4. Providing a review and analysis of overall appliance health; and

        5. Providing a review and analysis of overall network security across OSI Layers 1 — 3.

2. **Customer's Obligations.** The Customer is responsible for the following in accordance with industry best practices (as applicable):
    1. Providing Provider's engineers full administrative access to network appliances, portals, and environments within scope;
    2. Providing Provider's engineers with one (or more) technical points of contact;
    3. Providing Provider with up-to-date network documentation for sites within scope (where available);
    4. Engaging and coordinating with Provider's engineers on any network changes required to facilitate the delivery of services; and
    5. Ensuring any necessary vendor support contracts and licensing required for completion of project objectives are in place and active.

47. **WAN Optimization.** The terms and conditions of this Section 3.47 are applicable to each Order that includes the Provider's Network Assessment consulting services.
    1. **Provider's Obligations.** The Provider is responsible for the following in accordance with industry best practices:
        1. Providing a review and analysis of WAN-specific firewall policies for each edge firewall appliance within scope;
        2. Providing a review and analysis of current and historical bandwidth trends for each edge firewall appliance within scope;
        3. Providing a review and analysis of current and historical bandwidth trends for each edge network appliance within scope;
        4. Providing a review and analysis of advanced WAN metrics (where applicable) for each WAN circuit or logical connection within scope;
        5. Providing a review and analysis of provider cost and resiliency posture against Provider's services for each WAN circuit within scope; and
        6. Providing a review and analysis of edge network appliance, circuit, and configuration redundancy across OSI Layers 1 — 3 for each site within scope.
    2. **Customer's Obligations.** The Customer is responsible for the following in accordance with industry best practices (as applicable):
        1. Providing Provider's engineers full administrative access to network appliances within scope;
        2. Providing Provider's engineers with (one or more) technical points of contact;
        3. Providing Provider with up-to-date network documentation for sites within scope (where available);

4. Providing Provider with necessary circuit details which are not discoverable; and

5. Ensuring any necessary vendor support contracts and licensing required for completion of project objectives are in place and active.

48. **Network Device Monitoring.** The terms and conditions of this Section 3.48 are applicable to each Order that includes Network Device Monitoring – Basic, or Network Device Monitoring – Advanced services.

    1. **Resources.** The Provider is responsible for the following in accordance with industry best practices:

        1. Network Device Monitoring - Basic. For each quantity of Network Device Monitoring – Basic on an Order, Provider shall provide 1 license capable of ICMP up/down monitoring for a single network endpoint;

        2. Network Device Monitoring - Advanced. For each quantity of Network Device Monitoring – Advanced on an Order, Provider shall provide 1 license capable of SNMPv3 monitoring for a single network endpoint;

    2. **Provider's Obligations.** The Provider is responsible for the following in accordance with industry best practices:

        1. 24x7 monitoring of network devices, with email notifications to Customer for critical events and thresholds as defined at https://success.1111systems.com/article/0rdysi

        2. Onboarding customer design requirements form;

        3. Adding monitored devices into Providers monitoring collection platform;

        4. Verifying connectivity to Customer;

        5. Configuring Customer email contacts within Providers monitoring collection platform; and

        6. Coordinating testing and monitoring notification with Customer during planned maintenance window.

    3. **Customer's Obligations.** The Customer is responsible for the following in accordance with industry best practices (as applicable):

        1. Completing Customer's onboarding form for network devices to be monitored;

        2. Providing compute resources for local probe collectors;

        3. Installing and configurating local probe collectors;

        4. Configuring SNMP configuration for monitored network devices;

5. Configuring local network and firewall policies as necessary to facilitate connectivity for local probe collectors and Provider monitoring collection platform;

6. Providing a list of Customer email addresses for monitoring notifications;

7. Notifying Provider of any changes to Customer email addresses;

8. Notifying Provider of any network device removals that are being monitored by Provider;

9. Notifying Provider of any new network devices to be monitored by Provider; and

10. Contracting for additional Network Device Monitoring resources as required for new network devices

4. **Compatibility.**

1. Network Device Monitoring - Basic. All make and model network devices with a layer 3 ipv4 address that can respond to ICMP ping requests are supported; and

2. Network Device Monitoring - Advanced. Refer to https://success.1111systems.com/article/0rdysi for a list of known supported network devices. Not all metrics or thresholds are guaranteed to be monitorable. Device metrics and available thresholds to monitor against may vary from device to device and may vary depending on the monitored network device SNMP version.

49. **Fortinet Firewall Migration.** The terms and conditions of this Section 3.49 are applicable to each Order that includes the Provider's Fortinet Firewall Migration consulting services.

1. **Scope.** The Fortinet Firewall Migration Service is comprised of the following:

1. Basic - Firewall migration of Access Control Lists (ACLs), Network Address Translations (NATs), Virtual Private Networks (VPNs), network objects, and routing configuration;

2. Advanced - Basic + Software-Defined Wide Area Network (SD-WAN), and Next-Generation Firewall (NGFW) security profile configuration; and

3. Complex - Advanced + third-party software integrations, complex/niche custom configurations, and any Basic/Advanced elements that require extensive manual modifications.

2. **Provider's Obligations.** The Provider is responsible for the following in accordance with industry best practices:

1. Assessing current network state via network discovery process;

2. Developing a migration plan in coordination with customer which includes: identifying required change procedures, plan phases, timeline, goals and requirements, network tests, and criteria for success;

3. Migrating firewall(s) based on migration planning; and

4. Providing up to four (4) hours of post-migration troubleshooting and support.

3. **Customer's Obligations.** The Customer is responsible for the following in accordance with industry best practices (as applicable):

    1. Providing full administrative access to network appliances, portals, and environments within scope to Provider's engineers;

    2. Providing one (or more) technical points of contact to Provider's engineers;

    3. Providing any points of contact necessary to facilitate firewall configuration and testing against Customer-managed resources (e.g., authentication services, remote VPN gateways, WAN circuits, etc.) to Provider's engineers;

    4. Providing up-to-date network documentation for sites within scope (where available) to Provider's engineers;

    5. Engaging and coordinating with Provider's engineers on any network changes required to facilitate the delivery of services; and

    6. Providing application testing plans and criteria for success to Provider's engineers.

4. **Assumptions and Risks.** The Provider utilizes purpose-built software for firewall configuration migrations. In some cases, the migration of certain configuration elements may not be supported. For all configuration elements supported, the below limitations apply:

    1. ACLs and firewall policies. In cases where manual modifications are needed, Provider's engineers will manually modify no more than twenty-five (25) rules per firewall;

    2. Network Objects. In cases where manual modifications are needed, Provider's engineers will manually modify no more than twenty-five (25) objects per firewall;

    3. Network Address Translations. In cases where manual modifications are needed, Provider's engineers will manually modify no more than twenty-five (25) NATs per firewall;

    4. Site-to-Site VPNs.

1. In cases where manual modifications are needed, Provider's engineers will manually modify no more than 5 VPNs per firewall, and

2. In cases where VPN parameters do not migrate identically one-for-one, Provider's engineers will use the vendor's default parameter set, unless otherwise requested by the customer;

5. Remote Access VPNs.

    1. In cases where manual modifications are needed, Provider's engineers will manually modify no more than 5 VPNs per firewall, and

    2. The customer will be responsible for all end-user related communications, processes, and technical requirements related to migration of remote-access VPNs;

6. Authentication mechanisms. None;

7. Centralized management platform/system. Provider does not support the migration of centralized management platforms (e.g. Palo Alto Panorama, or similar);

8. SD-WAN. None;

9. Routing protocols. None;

10. Static routes. In cases where manual modifications are needed, Provider's engineers will manually modify no more than twenty-five (25) static routes per firewall;

11. High Availability (HA). None;

12. Software version update. Provider's engineers will update the new/replacement firewall(s) to the latest vendor-recommended software version prior to migration, but not afterward;

13. NGFW security profiles. In cases where NGFW security profiles do not migrate identically one-for-one, Provider's engineers will implement the default security profile for each specific NGFW feature; and

14. Logging. None.

50. **Managed Public Cloud Services for AWS.** The terms and conditions of this Section 3.50 are applicable to each Order that includes Managed Public Cloud Services for AWS and are accessible at https://1111systems.com/legal/1111-managed-cloud-services-for-aws-service-terms/

51. **Managed Public Cloud Services for Azure.** The terms and conditions of this Section 3.51 are applicable to each Order that includes Managed Public Cloud Services for

Azure and are accessible at https://1111systems.com/legal/1111-managed-cloud-services-for-azure-service-terms/

52. **11:11 Cyber Vault for Cohesity.** The terms and conditions of this Section 3.52 are applicable to each Order that includes Cyber Vault for Cohesity services.

    1. **Resources.**

        1. Backup Policies. The policies that define the Cohesity Protection Policy that includes the Archive Schedule used for Cyber Vault for Cohesity. The policies define that a full archive is created with incremental updates thereafter to an external S3 target;

        2. Backup Groups. Backup Groups are a defined group of Virtual Machines and backup agents that are backed up according to a defined Backup Policy;

        3. Licensing. All required licensing from Cohesity (Cloud Archive licensing) is included in the service; and

        4. Business Models. Storage is available in a Reserved plus Burst model.

    2. **Provider's Obligations.** The Provider is responsible for the following in accordance with industry best practices:

        1. Configuring the external S3 target as specified by the Order;

        2. Providing ongoing support and education about the Service at the Customer's request;

        3. Maintaining the underlying cloud infrastructure components such as compute, memory, storage, and networking by following Provider's guidelines for managing these environments;

        4. Monitoring of archive job performance, SLAs, Backup Policies, and Backup Groups;

        5. Assisting the Customer with initiating the restore from the archive data upon request; and

        6. Creating and Maintaining the Archive Policy settings of a Backup Policy upon request.

    3. **Customer's Obligations.** The Customer is responsible for the following in accordance with industry best practices:

        1. Providing all information reasonably required and requested by Provider to fulfill its obligations including without limitation archive requirement details;

        2. Restoring archive. Provider will provide reasonable support with archive restoration upon request by Customer;

3. Not exceeding the reasonable data egress standard defined above and/or paying for data egress charges where the data egress standard is exceeded;

4. Promptly notifying the Provider if the Cloud Resources are hacked, accessed by an unauthorized third party, or infected with a virus, worm or similar code;

5. If the Customer provisions Reserved Resources in excess of the specifications set out on the Order, the Customer hereby acknowledges that the Provider is not responsible for any performance degradation, loss of archive data, or errors caused by over allocation, this includes the storage necessary for processing the archives, which could result in archive storage Burst charges; and

6. For the Customer to restore archived Virtual Machine data, the Customer must have sufficient storage available. If the Customer does not have sufficient storage available, the Customer may have to purchase more storage to make the restoration possible;

4. **Data Egress.**

    1. Data egress, from an acceptable use policy perspective, is comprised of two components: Data Retrieval API calls and Data Transfer out to the Internet;

    2. This service uses Amazon S3 Standard Infrequent Access class, data egress charges are included if usage patterns are deemed reasonable for the service offering. Reasonable data egress shall mean allowed egress of up to 50% of the highest of contracted or total stored data, measured in GB per month per region, within the Customer account; and

    3. The Provider reserves the right to charge for any data egress exceeding the reasonable data egress standard above.

5. **Serverless Compute Services.**

    1. This service uses Amazon Lambda serverless compute service. Request and duration charges are included if usage patterns are deemed reasonable for the service offering. Reasonable usage is limited to only include compute service usage required for archive processes within the Customer account; and

    2. If the Provider determines (in its sole discretion) that the Customer has exceeded the reasonable usage of Amazon Lambda services, the Provider will (1) notify the Customer of such usage, (2) advise the Customer to upgrade its Order in order to reflect the additional usage, and (3) invoice the Customer for the costs associated with the additional license usage during the corresponding period. If the Provider advises the Customer to upgrade its Order in the preceding sentence and the Customer does not upgrade its Order within 30

days after receiving that notice, the Provider reserves the right to unilaterally increase the number of resources on the Customer Order in order to true it up. The Customer agrees to pay any invoices or charges for any additional Amazon Lambda services or back charges allowed under this Section.

6. **Risks.**

    1. There may be times where the Provider's service is unable to perform archives. Reasons for archive job failures include, but are not limited to, situations where a job is unable to start during retry windows, services are temporarily unavailable, and conflicts occur between resources. Where such failure occurs, the Provider will use reasonable efforts to attempt to remedy any potential archive job failures, and Customer shall hold Provider harmless in the event that an archive job did not occur successfully.

53. **11:11 Co-Managed Firewall.** The terms and conditions of this Section 3.53 are applicable to each Order that includes Co-Managed Firewall services.

    1. **Provider's Obligations.** The Provider is responsible for the following in accordance with industry best practices:

        1. Providing the services as outlined in the applicable Basic and Advanced Managed Appliance Section 3.25;

        2. Maintaining monitoring, support, and management activities consistent with the selected service level, excluding responsibilities explicitly assumed by the Customer through administrative access;

        3. Provider reserves the right to audit configuration logs and system activity for the purposes of incident investigation and change attribution;

        4. Provider shall not be held liable for any data loss, corruption or cyber incidents resulting from Customer-made changes, including, but not limited to, deletion of firewall rules, logs, objects, or configurations;

        5. Provider reserves the right to revoke the Customer's administrative access in the event of a security incident, repeated misconfigurations, unauthorized access, or violations of this agreement. Administrative access may also be suspended during critical troubleshooting or remediation efforts;

        6. Provider shall not be held liable for any Service Level Agreement (SLA) or Service Level Objective (SLO) violations resulting from Customer-made changes;

        7. Provider reserves the right to enhance the co-managed service by adding change management capabilities into its customer portal or console platform in the future. As part of this enhancement, Provider may transition administrative access to a permission-based

interface and disable direct administrative rights to the firewall device(s). Customer will be notified in advance of such changes; and

8. Provider reserves the right to charge the Customer on a time and materials basis for extended or repeated outages, service degradation or false alerts caused by Customer-initiated changes that result in excessive troubleshooting or remediation efforts by the Provider. The Customer will be notified in writing in advance of such charges.

2. **Customer's Obligations.** The Customer is responsible for the following in accordance with industry best practices (as applicable):

    1. Making configuration changes in accordance with its internal change management policies and firewall(s) access rights;

    2. Assuming full responsibility for any changes made to the firewall device(s), including, but not limited to, any outages, performance degradation, misconfigurations, or security breaches resulting from those changes;

    3. Managing all user accounts and access permissions associated with the firewall(s), including, but not limited to, VPN, provisioning, deprovisioning, and auditing access on an ongoing basis;

    4. Providing, managing, and auditing its firewall configuration to ensure they align with the organization’s security, compliance, and operational requirements;

    5. If the firewall device becomes unreachable or unrecoverable, and there is no corresponding support ticket confirming the change was made by the Provider, the Customer will be deemed solely responsible for the resulting incident;

    6. Customer is fully responsible for any firewall configuration changes not associated with an open or documented Provider's support ticket;

    7. Customer must notify the Provider of any changes made to the firewall(s) by opening a support ticket with the Provider immediately following the change. This notification must include a brief description of the change and the time it was implemented;

    8. Performing a full backup of the firewall configuration immediately before and after each change. Provider is not responsible for restoring or recovering configurations unless the backup was performed prior to the change;

    9. Securely storing any pre-shared keys (PSKs), credentials, or other sensitive security parameters generated or modified by the Customer. Provider does not retain or manage customer-generated PSKs;

10. Customer is fully responsible for any changes, configurations, or access granted to third parties, including consultants, contractors, or other service providers; and

11. Maintaining an accurate and up-to-date change log that documents all configuration changes made to the firewall(s), including the date, time, nature of the change, and the user who performed it. This log must be maintained outside of the firewalls and made available to the Provider upon request for troubleshooting, audit, or incident investigation purposes.

54. **Microsoft Licensing.** The terms and conditions of this Section 3.54 are applicable to each Order that includes Microsoft software licensing.

    1. **Resources.**

        1. Licensing. Microsoft licensing as described in the Order; and

        2. Business Models. Licensing is available in a reserved only model.

    2. **Provider's Obligations.** The Provider is responsible for the following in accordance with industry best practices:

        1. Maintaining an active and valid SPLA agreement with Microsoft to ensure uninterrupted access to Licensed Software, for the duration of the Customer's subscription term;

        2. Submitting accurate monthly License Usage Reports (LURs) to Microsoft on behalf of the Customer, based on usage data provided by the Customer or collected through Provider's metering systems;

        3. Implementing reasonable measures to ensure Customer compliance with Microsoft's SPLA Terms and Conditions, Product Terms, and Online Services Terms, including notifying Customers of any identified non-compliance and assisting with remediation;

        4. In the event of a Microsoft audit, the Provider shall cooperate with Microsoft or its designated auditing firm, providing necessary usage data and documentation while coordinating with the Customer to address audit requirements; and

        5. Provider shall promptly notify the Customer of any discrepancies in reported usage and work with the Customer to resolve inaccuracies.

    3. **Customer's Obligations.** The Customer is responsible for the following in accordance with industry best practices:

        1. Complying with the Microsoft SPLA Terms and Conditions, Product Terms, and Online Services Terms, as applicable, governing the use of Licensed Software;

        2. Providing accurate user, device, or resource count data to the Provider for inclusion in monthly License Usage Reports, as required by Microsoft. Provider reserves the right to audit Customer's usage

of Licensed Software for compliance with Microsoft's SPLA terms, in coordination with Microsoft or its designated auditing firm;

3. Notifying the Provider of any changes in usage, such as additional users, devices, or cores, within five (5) business days to ensure accurate reporting;

4. Licenses provided under this Section are subscription-based, non-perpetual, and limited to use within Provider's hosted services or Customer's environments explicitly authorized in the Order;

5. Certain Licensed Software, such as Windows Server, may require SALs for each user or device accessing the software, regardless of whether the software is actively used; and

6. If the Provider determines (in its sole discretion) that the Customer has exceeded the reserved license count, the Provider will (1) notify the Customer of such usage and (2) advise the Customer to upgrade its Order to reflect the additional usage. If the Provider advises the Customer to upgrade its Order in the preceding sentence and the Customer does not upgrade its Order within 30 days after receiving that notice, the Provider reserves the right to charge for any additional licenses. The Customer agrees to pay any invoices or charges for any additional licenses under this Section.

55. **VMware Licensing.** The terms and conditions of this Section 3.55 are applicable to each Order that includes Broadcom software licensing for VMware Cloud Foundation and add-ons sold either under Section 3.13 (11:11 Flexible Cloud Environment) or standalone as part of Broadcom's Legacy White Label Program.

    1. **Resources.**

        1. Licensing. Broadcom VMware Cloud Foundation core licenses with a minimum of 16 cores per physical CPU socket as mandated by Broadcom, and add-on licensing as described in the Order;

        2. Business Models. Licensing is available in a reserved plus burst business model for VMware Cloud Foundation cores and a reserved only model for add-ons; and

        3. Software Downloads. Software downloads required for licenses on the Order are made available to Customer by the Provider.

    2. **Provider's Obligations.** The Provider is responsible for the following in accordance with industry best practices:

        1. Licensing Support. Providing support for VMware licensing issues, with escalation to Broadcom's Global Support Services (GSS) as necessary. Support includes guidance on license activation, usage metering, and compliance;

        2. VMware Support. Providing support for VMware operational issues for licensed products on the Order, with escalation to Broadcom's

Global Support Services (GSS) as necessary. Support includes guidance on installation issues, VMware management, updates and patching;

3. Usage Meter Configuration. Usage monitoring and reporting through the Broadcom VMware Usage Meter owned and operated by the Provider, ensuring accurate tracking and reporting of license consumption for billing and compliance;

4. License Key Creation. Providing Customer specific license key files for each version of VMware vSphere and add-ons to be licensed using an SLO of 5 days following order completion;

5. Core Burst Billing. Provider shall bill Customer for burst VMware Cloud Foundation core license usage at contracted rates up to a 20% overage and Month-to-Month pricing for any overages beyond 20% contract overage; and

6. For Flexible Cloud Environment.

    1. Should an Order contain VMware licensing, the Provider shall provide support exclusively for VMware licensing issues, with escalation to Broadcom's Global Support Services (GSS) as necessary. Support includes guidance on license activation, usage metering, compliance, guidance on installation issues and VMware management, and

    2. Should an Order contain VMWaaS, the Provider shall also provide support for VMware operational issues for licensed products on the Order, with escalation to Broadcom's Global Support Services (GSS) as necessary. Support includes guidance on installation issues, VMware management, updates and patching.

3. **Customer's Obligations.** The Customer is responsible for the following in accordance with industry best practices:

    1. Licensing Licensing all Broadcom VMware software in use and to work with the Provider to confirm accurate licensing requirements;

    2. License Compliance. Complying with Broadcom's General Terms, Software Exhibits, and Product Guide, as applicable, governing the use of VMware Cloud Foundation and related add-ons;

    3. License Minimums. Ensuring a minimum of 16 VMware Cloud Foundation cores are licensed per physical server CPU socket; and

    4. License Renewals. Ensuring timely payment of subscription fees, including any surcharges for late renewals as specified by Broadcom (e.g., a 20% surcharge on first-year subscription renewal fees for missed renewal deadlines).

4. **Licensing Restrictions.** The following restrictions apply when licensing VMware Cloud Foundation and add-ons:

    1. Licenses provided under this Section are subscription-based and do not confer perpetual rights. Customer may not renew support for existing perpetual VMware licenses through the Provider unless explicitly permitted by Broadcom;

    2. VMware Cloud Foundation core licenses include 1 TiB of vSAN entitlement per core, which may be aggregated across VMware Cloud Foundation core licenses only. Additional vSAN capacity may be purchased as needed;

    3. Customers are prohibited from applying maintenance releases, updates, patches, or enhancements to VMware software post-subscription expiration, except for critical zero-day security patches, as stipulated by Broadcom; and

    4. Provider reserves the right to audit Customer's VMware deployment for compliance with license terms, in coordination with Broadcom or its designated auditing firm.

5. **Fees and Billing.** The following apply when licensing VMware Cloud Foundation and add-ons:

    1. Subscription fees for VMware licenses are calculated based on the number of cores licensed, subject to Broadcom's minimum core requirements and pricing structure; and

    2. Provider shall be the configured Broadcom partner when Usage Meter reports usage data to Broadcom, and Customers agree to cooperate with usage verification processes.

56. **Infrastructure Recovery (also known as Hotsite).** The terms and conditions of this Section 3.56 are applicable to each Order that includes Infrastructure Recovery and are accessible at https://1111systems.com/legal/1111-infrastructure-recovery-service-terms/

57. **VMware-as- a-Service (VMaaS) under Lease Agreement Program.** The terms and conditions of this Section 3.57 are applicable to each Order that includes Broadcom software licensing for VMware Cloud Foundation and add-ons sold as part of the VMware-as- a-Service (VMaaS) under Lease Agreement Program.

    1. **Resources.**

        1. Licensing. Licensing covers Broadcom VMware Cloud Foundation core licenses with a minimum of 16 cores per physical CPU socket as mandated by Broadcom, and add-on licensing as described in the Order. For VCF EDGE environments, there is a maximum of 256 cores per site, with a minimum of 10 sites that shall be deployed within 12 months of the commencement date of the first Order containing VCF EDGE subscriptions;

2. Business Models. Licensing is available in a reserved plus burst business model for VMware Cloud Foundation cores and a reserved only model for add-ons; and

3. Software Downloads. Software downloads required for licenses on the Order are made available to Customer by the Provider.

2. **Provider's Obligations.** The Provider is responsible for the following in accordance with industry best practices:

    1. Licensing Support. Providing support for VMware licensing issues, with escalation to Broadcom's Global Support Services (GSS) as necessary. Support includes guidance on license activation, management, usage metering, and compliance;

    2. VMware Tier3 Support. Providing escalation support for VMware operational issues for licensed products on the Order, with escalation to Broadcom's Global Support Services (GSS) as necessary;

    3. Usage Meter Configuration. Usage monitoring and reporting through the Broadcom VMware Usage Meter owned and operated by the Provider, ensuring accurate tracking and reporting of license consumption for billing and compliance;

    4. License Key Creation. Providing Customer specific license key files for each version of VMware vSphere and add-ons to be licensed using an SLO of 5 days following order completion; and

    5. Core Burst Billing. Provider shall bill Customer for burst VMware Cloud Foundation core license usage at contracted rates up to a 20% overage and Month-to-Month pricing for any overages beyond 20% contract overage.

3. **Customer's Obligations.** The Customer is responsible for the following in accordance with industry best practices:

    1. Licensing Licensing all Broadcom VMware software in use and to work with the Provider to confirm accurate licensing requirements;

    2. License Compliance. Complying with Broadcom's General Terms, Software Exhibits, and Product Guide, as applicable, governing the use of VMware Cloud Foundation and related add-ons;

    3. License Minimums.

        1. Ensuring a minimum of 16 VMware Cloud Foundation cores are licensed per physical server CPU socket, and

        2. For VCF EDGE environments, there is a maximum of 256 cores per site, with a minimum of 10 sites that shall be deployed within 12 months of the commencement date of the first Order containing VCF EDGE subscriptions. In theevent that Customer does not meet the minimum

requirements after 12 months of the commencement of the first Order containing VCF EDGE subscriptions, Customer acknowledges that such subscriptions shall be replaced by the Provider using the standard VCF subscriptions with their corresponding rates;

4. License Renewals. Ensuring timely payment of subscription fees, including any surcharges for late renewals as specified by Broadcom (e.g., a 20% surcharge on first-year subscription renewal fees for missed renewal deadlines);

5. VMware Software Installation. Deploying and installing VMware software for licensed products on the Order;

6. VMware Tier 1-2 Support:Troubleshooting and supporting VMware operational issues for licensed products on the Order, including, but not limited to, VMware management, updates and patching;

7. Hardware. Monitoring, maintaining, patching and/or replacing any hardware used by the VMware deployment. This includes the leaseback hardware that is part of the Order and Lease Agreement. Customer shall maintain and enforce hardware support contracts and activities directly with their corresponding vendors;

8. Remote Access for Provider. Providing the Provider with the following in order to fulfill its obligations:

    1. A Customer-managed jump host that Provider can use to access the VMware environment. Provider will work with Customer to install an Atera-based remote access tool that Provider will use to access the Customer's VMware environment as needed to fulfill its obligations. This host shall be patched by the Customer using the Customer's existing tooling and adhering by the Customer's schedule,

    2. An administrator account for accessing the jump host,

    3. The root administrator account for all vCenter environments in scope of the VMaaS service,

    4. Notifying the Provider immediately after the administrator password changes due to standard password rotation practices or a different reason. This notification shall be conducted via a support ticked and provide the new credentials to the Provider,

    5. Providing access from the jump host to all environments, including access to Usage Meter, as well as Internet access to enable connections to Atera, and

    6. Informing the Provider of any core or other licensed resources that could warrant an amendment to the Order; and

9. Overages. Provider will measure license usage via Usage Meter. Any overages on top of the contracted amounts as defined in the Order, shall be invoiced at the corresponding Burst rates, also defined in the Order. For license subscriptions under the Bring Your Own category, any overages shall be charged as standard VCF licenses using their corresponding rates.

4. **Roles and Responsibilities.** The following Responsible-Accountable-Consulted-Informed (RACI) table summarizes the obligations described in Sections 3.57.2 and 3.57.3 above:

Task/Function
VMware licensing management, compliance and reporting
Providing VMware licenses
vSphere administrative access provisioning
Tier 3 VMware support
BAU operations for VMware
Hardware monitoring/support/replacement
Hardware support and maintenance
Providing remote access (Atera jump host)

5. **Licensing Restrictions.** The following restrictions apply when licensing VMware Cloud Foundation and add-ons:

    1. Licenses provided under this Section are subscription-based and do not confer perpetual rights;
    2. VMware Cloud Foundation core licenses include 1 TiB of vSAN entitlement per core, which may be aggregated across VMware Cloud Foundation core licenses only. Additional vSAN capacity may be purchased as needed;
    3. VMware Cloud Foundation EDGE environments are limited to 256 cores per site, with a minimum of 10 sites that shall be deployed within 12 months of the commencement date of the first Order containing VCF EDGE subscriptions;
    4. Customers are prohibited from applying maintenance releases, updates, patches, or enhancements to VMware software post-subscription expiration, except for critical zero-day security patches, as stipulated by Broadcom; and

5. Provider reserves the right to audit Customer's VMware deployment for compliance with license terms, in coordination with Broadcom or its designated auditing firm.

6. **Fees and Billing.** The following apply when licensing VMware Cloud Foundation and add-ons:

    1. Subscription fees for VMware licenses are calculated based on the number of cores licensed, subject to Broadcom's minimum core requirements and pricing structure; and

    2. Provider shall be the configured Broadcom partner when Usage Meter reports usage data to Broadcom, and Customers agree to cooperate with usage verification processes.