rackspace technology.

Customer First.
Cloud First.

Rackspace Sovereign Cloud Support Services Terms & Conditions for G-Cloud 15

RACKSPACE UK SOVEREIGN SERVICES PRODUCT TERMS

In addition to any other terms and conditions of Customer's Agreement with Rackspace, these Product Terms (inclusive of the Schedules), shall apply when Customer purchases Rackspace UK Sovereign Services ("**UK Sovereign Services**" or the "**Services**") for any of the Security Domain specific Services, e.g., Government Cloud UK, Healthcare Cloud UK, or Sovereign Cloud UK.

1. SERVICES OVERVIEW. Rackspace UK Sovereign Services are a suite of managed cloud offerings that are fully UK sovereign, hosted within the UK, and supported by UK-based security cleared staff. The design, execution and managed support of UK Sovereign Services by Rackspace is based upon the following considerations:

1.1. Deployment in UK Sovereign Dedicated Environments. Each of the respective Security Domains are deployed separately from Rackspace Technology's global platforms and data centres, with tightly controlled access and discrete segregation for each Customer deployment. Each Security Domain has dedicated Compute and Storage to ensure that no Customers of a given Security Domain (e.g., Healthcare Cloud UK) are hosted within the same nodes as any other Security Domain (e.g., Sovereign Cloud UK).

1.2. Secure Management. Customer environments are managed via Rackspace UK Sovereign Services Central ("**RSSC**"), an air-gapped management environment maintained to PSN service provision levels of assurance and aligned with NCSC guidance for secure third-party support. RSSC access is restricted to UK-Sovereign, security-vetted engineers who manage the Services with fully tenanted tooling, role-based access, and logged activity conducted via "edge node" servers.

1.3. Privacy and Compliance. Rackspace adheres to GDPR requirements in its role as processor and maintains policies, processes, and operational controls, as stated in the Agreement. Compliance certifications for UK Sovereign Services include ISO/IEC 27001:2013 (All global offices and data centres); ISO/IEC 9001:2015 (UK offices and data centres); Cyber Essentials + (UK corporate network); and PSN service provision (RGC Central - Secure Management Platform).

2. SECURITY AND COMPLIANCE. UK Sovereign Services are designed, deployed, and managed for UK public sector entities that need to host sensitive data in a secure manner and in compliance with applicable laws. Rackspace will provide the following Services (as further described herein): (1) Rackspace will implement and manage the Production Environment, including the hypervisor, for Customer-provided appliances and the OSI layer for all other Customer VMs; (2) to secure the Rackspace Network and Cloud Infrastructure, Rackspace will implement and conform the Services to the Compliance Baseline, which at a minimum, means a subset of the NIST SP 800-53 Revision 4 Moderate impact security controls, and the Services will be in aligned with the NCSC's 14 Cloud Security Principles (where applicable), and may also include additional overlays and/or Customer-defined controls; and (3) Maintenance and upgrade of the Cloud Infrastructure as reasonably necessary to comply with the descriptions herein and the terms of the Agreement. Compliance Baseline requirements for any software or program installed on top of the Rackspace-provided and managed OSIs are the sole responsibility of Customer.

3. SINGLE-TENANT VERSUS MULTI-TENANT. UK Sovereign Services are available in Single-Tenant and Multi-Tenant deployments, as described herein, and as further specified in Schedule 2.

4. MANAGED CLOUD INFRASTRUCTURE SERVICES.

(A) System Administration & Maintenance Services. Unless stated on the Rackspace Service Order, Rackspace provides system administration and maintenance services for all elements of the Services. Compute, storage, network, and OSIs are configured, hardened, and managed per pre-defined configuration management controls. Rackspace installs and implements Customer's Production Environment; and provides the maintenance, repair or replacement of all Cloud Infrastructure components of Customer's environment. Customer is solely responsible for all administration, maintenance, security,

and compliance management services required for any software or program installed on the Rackspace-provided and -managed OSIs. Rackspace shall attempt to schedule maintenance for a time that minimizes impact on Customer, and shall provide notice of Scheduled Maintenance.

(B) Single-Tenant Specification. For dedicated versions of the Services, Customers may specify the hardware host CPU clock speeds and/or memory type for the allocated cluster; additional Fees may be applicable and will be detailed in the Service Order.

(C) Multi-Tenant Specification. Rackspace provides the use of computing resources as vCores, vRAM and vDisk to support Customer's applications. Specification of virtual machines within a Customer environment are detailed within the Service Order. The underlying platform is managed and owned by Rackspace and the hardware layer is not accessible by Customer. Any additional hardware specifications (e.g., specified GPUs, additional vRAM, etc.) will be available on a monthly rental basis. Prices charged for virtual machines are based upon monthly pricing, and any device powered on for over 24 hours in a single month will count as a full unit, chargeable for the month. Any virtual machine replicated on a secondary site for disaster recovery (DR) purposes will be charged as a reservation fee, this fee guarantees capacity in the secondary location for these servers. Compute services are provided as highly resilient clusters in all cases to ensure adherence to SLAs.

(D) Service Restrictions. As part of the Sovereign platform, no access to, but not limited to the following list will be granted directly to a Customer for the multi-tenant versions of the product set; vCentre, multi-tenant firewall, host console, switch configuration. Only the dedicated Rack platform will be eligible for request to these features and will only be granted by exception.

(E) Bare Metal Services. Rackspace provides the use of computing hardware provided as a bare metal service. Specification of servers within a Customer environment are detailed within the Service Order. The underlying platform is managed and owned by Rackspace and the hardware layer will not be accessible by Customer, except as expressly described in the Service Order (on a custom basis) with written approval from the Sovereign Services GM.

(F) Cloud Storage Services. Rackspace provides a fully managed storage environment for OSIs, Customer Appliances, backups, and disaster recovery, separated at the Customer tenant level. Storage options are tiered for price and performance optimization, and provisioned and billed as provisioned storage as defined in the Service Order. Storage will be charged on a monthly basis as an average across the month.

(G) Capacity Planning. Customer may request alerts when pre-defined thresholds (documented in the SEAP) have been reached. These alerts shall proactively notify Customer that additional resources may be required to support their workloads. All requests for additional resources shall be made in writing, either via the ticketing method designated by Rackspace or executed Service Order. Rackspace will manage the underlying capacity of the Services' clouds and ensure that sufficient capacity is available for all contracted Services.

(H) Network Services. Rackspace provides highly available LAN configurations as well as redundant WAN connectivity through multiple Tier I internet service providers, including Rackspace Network links between data centres. Rackspace shall provide availability monitoring of all Rackspace Network components. Rackspace also implements denial-of-service (DoS) protection mechanisms at the network ingress and egress points. Customers are able to bring their own connections, charges for this are per physical port connected. Any cross connects required or connections from service providers are not included in a bring your own scenario and can be quoted separately.

(I) Network Capacity. Rackspace public and external network bandwidth is limited to the bandwidth capacity specified in the Service Order in megabits per second. In the case of a bandwidth transfer limit, Rackspace will charge an additional Fee for anything over the included GB amount. For unlimited data transfer connections, bandwidth capacity (i.e., size of connection) in megabits per second will be allocated

with fully unlimited data transfer; all managed connections within UK Sovereign Services are unlimited in data transfer unless stated otherwise in the Service Order.

5. OSI MANAGEMENT. Rackspace shall provide provisioning, hardening, encryption, administration, backups, monitoring, and alerting of the Production Environment OSIs deployed, as set forth in this section 5 and in the applicable Service Order for all UK Sovereign Services.

5.1. Provisioning. The Rackspace Cloud Server Management Implementation Service provides the implementation and initial testing of the monitoring, alerting, and O/S administration tools for the cloud servers deployed.

5.2. Hardening. Rackspace hardens OSIs (Red Hat Enterprise Linux and Microsoft Windows Server only) and network devices to its configuration baseline based on the Centre for internet security (CIS) benchmarks. Any Customer-defined hardening requirements in addition to, or in lieu of, the Centre for internet security (CIS) Benchmarks configuration baseline shall be identified and set forth in Services Order(s), inclusive of any additional implementation and management Fees, prior to being implemented and provided as part of the Services.

5.3. Encryption. Rackspace manages transparent FIPS 140-2 validated encryption at the storage layer. Compliance Baseline encryption requirements for any software or program installed on top of the Rackspace-provided and -managed OSIs are the sole responsibility of Customer.

5.4. Administration. Rackspace provides administration of OSIs, including routine preventative maintenance, monthly patching, and troubleshooting, and may include additional services, as defined in the Service Order.

5.5. Backups. Rackspace performs image-based Changed Block Tracking backups of Production Environment OSIs and Customer Appliances once per day. If file-level, database-level, or otherwise application-aware backups are required, Customer is responsible for providing a compatible backup solution – e.g., database-native backup to a local disk included in the daily image backup. Unless otherwise specified in the Service Order, the backups for Production Environment OSIs and Customer Appliances shall be available onsite for 14 calendar days, and the Production Environment backups shall be replicated from the primary backup location to the archival backup location available in the Disaster Recovery Site for the same 14-day period. Customer may request additional Services for longer retention periods, as defined in the Service Order. Any required restores shall only be created from Rackspace-provided disk images and presented to the OSI as a full disk. Customer may choose to replace the existing disk or mount as an additional disk; but all file-level, application or database recovery efforts are Customer's responsibility.

6. ACCESS MANAGEMENT AND ENVIRONMENTAL CONTROLS.

6.1. Access Control (AC). Rackspace's architecture and processes maintain controlled Privileged User access to the Cloud Infrastructure. Privileged Users shall access the Cloud Infrastructure via Rackspace Sovereign Services Central (RSSC, a PSN accredited, secure management platform). From the RSSC environment, Privileged Users access Customer workloads via dedicated "edge node" servers that are hosted within Cloud Infrastructure. All communications between the RSSC and Customer "edge nodes" are encrypted to NCSC recommendations, as follows:

(A) All Privileged User sessions may be recorded on the Customer "edge node" to provide a detailed activity log to support potential security incident analysis and response; this requires Customer approval due to the use of Customer storage resources.

(B) Rackspace shall be responsible for and shall have administrator control over the domain, forest, and/or organizational units that comprise the computer, user, and service accounts that pertain to, and provide access to, the Production Environment, unless agreed in writing with the Customer.

6.2. System and Communication Protection (SC). Rackspace separates user functionality from management functionality through physical and logical network segmentation and associated access management policies. The Cloud Infrastructure is separated into at least two security environments: 1) a management environment containing Rackspace's support tools, and 2) Customer's Production Environment. Customer may implement "non-production" environments. Access to each environment is controlled by a logical firewall. Access to the management environment is limited to only Rackspace personnel. Privileged Users access the Production Environment using multi-factor authentication into a jump host via an encrypted VPN connection. End users of Customer's application enter through Customer-managed, application-defined mechanisms.

6.3. Media Protection (MP). Rackspace utilizes accredited cryptographic mechanisms to encrypt all storage media within the Customer environment. All physical media transport outside of the data centre is prohibited. Unless set forth in a separate agreement, Rackspace shall not accept any Customer-furnished storage devices, and Rackspace shall not provide to Customer any Rackspace storage devices. All decommissioned disk drives and digital media are sanitized before any physical destruction, in accordance with the Compliance Baseline. Physical destruction of disks may incur an additional charge.

7. CONFIGURATION MANAGEMENT.

7.1. Configuration Management (CM). Rackspace uses a baseline configuration based on the CIS Benchmarks. Rackspace follows change and configuration management procedures detailed in the Configuration Management Plan as part of the A&A Package. As part of Rackspace's configuration management process, all proposed changes are recorded and analyzed for impact, and any Customer-impacting changes are coordinated with Customer. In addition, where Rackspace has responsibility for managing Customer's Active Directory, configuration tools automatically develop baselines when initially configured, and maintain those baselines by comparing any changes to the baseline, at least once per quarter, as the system is being used. Any Customer-defined hardening other than the Rackspace-defined configuration baseline shall be stated in any applicable Service Order(s), which shall include additional implementation and management Fees.

7.2. Customer-defined Controls. Other controls, as additions to, or in lieu, of the provisionally authorized controls may be mutually agreed upon and included, provided there is no conflict with Applicable Laws. All such controls shall be identified in the Service Order inclusive of any additional implementation and management Fees, prior to being implemented and provided as part of the Services.

7.3. Quarterly Configuration Compliance Scanning and Reporting. Rackspace scans the managed OSIs for compliance with the Rackspace-defined hardening configuration standard. The raw, unmodified compliance scan results shall be provided quarterly to Customer for each environment. Any Customer-defined hardening configurations, other than the Rackspace-defined configuration baseline, shall be stated in the applicable Service Order, which shall include additional implementation and management Fees. Any custom-configuration compliance scanning and associated reporting shall be stated in any applicable Service Order(s), which shall include additional implementation and management Fees.

8. FULLY MANAGED; SYSTEM INTEGRITY (SI); MONITORING AND ALERTING; SCANNING. Rackspace shall provide the items described in this section 8 for all devices with a fully managed service level. The service is provided and charged as a fully managed service unless otherwise stated on the Service Order. If Customer elected to remove the fully managed service level, additional charges may be applicable for individual components covered herein.

8.1. 24x7 Monitoring and Alerting. Rackspace monitors the performance, availability, and network connectivity of supported cloud servers 24x7. By default, all alerts are configured to go to Rackspace, but the SEAP can be updated to define Customer notification and escalation criteria. Any alert that results in an incident will automatically notify the Customer. Customers may access the monitoring portal directly to view the state of the Customer estate at any time.

8.2. Endpoint Security Management. Rackspace provides a centrally managed endpoint security software platform for all Customer OSIs within their environment. The endpoint security management solution provides centralized anti-virus, malware defense, and host-based intrusion prevention services. Rackspace provides ongoing management of the management servers; agents installed on OSIs; and associated configurations, updates, and policy management. In the event a security event is detected, Rackspace shall notify and collaborate with Customer to determine the appropriate actions. The facility is provided as part of the fully managed service with no access to the console of the anti-virus product.

8.3. File Integrity Monitoring. Rackspace provides an additional service which is a centrally managed File Integrity Monitoring (FIM) solution that monitors all Customer OSIs for file changes. The FIM solution monitors core OSI operating system files and identifies and reports on changes made to these files. Monitoring the integrity of Customer data and/or application files installed by Customer on OSIs is excluded from the Rackspace FIM solution monitoring scope of services. Rackspace provides ongoing management of the FIM management servers; agents installed on OSIs; and associated configurations, updates, and policy management. In the event a FIM event is detected, Rackspace shall notify Customer and shall collaborate with Customer to determine the appropriate actions.

8.4. Risk Assessment (RA); (Monthly Vulnerability Scanning). Rackspace performs monthly vulnerability scanning for each Rackspace managed Customer's OSIs within their environment(s). The scans are performed by Rackspace and the raw, unmodified vulnerability scan results shall be provided to Customer. Rackspace and Customer shall mutually agree on a monthly scanning schedule for the duration of the services agreement. Any custom vulnerability scanning activities and associated reporting requested by Customers shall be stated in any applicable Service Order(s), which shall include additional implementation and management Fees. Customer's security obligations include immediately remediating any known security vulnerability of any Customer Appliance, or any software or program installed on top of the Rackspace provided and managed hardware and software Services.

9. PERSONNEL SECURITY (PS).

9.1. Standard Personnel Screening. All Rackspace personnel with physical or logical access to the Cloud Infrastructure shall be resident citizens of the UK, commensurate with the Compliance Baseline requirements, and undergo pre-employment background checks, with a minimum of BS7858 as part of the on-boarding and application process. An employee's hiring is contingent upon internal investigations, such as background, credit, and reference checks.

9.2. Customer-requested Screening. If Customer requires personnel security approvals or clearances outside of Rackspace's standard background investigation, then Rackspace reserves the right to submit for approval and/or clearance its entire operations and security teams associated with the Services to enable adequate support. Customer shall bear the costs and expenses incurred by Rackspace in connection with obtaining approvals or clearances required to allow Rackspace to perform its obligations hereunder.

9.3. Personnel Awareness and Training (AT). All Rackspace engineering staff supporting the Cloud Infrastructure receive annual privacy and information security awareness training.

10. PHYSICAL ENVIRONMENT SECURITY (PE). Rackspace data centres and ARK data centres implement security safeguards to control access to areas within the facility that are officially designated as publicly accessible. Rackspace uses ID badges for all personnel with access privileges. Rackspace maintains a current list of personnel with authorized access to the areas where the Cloud Infrastructure resides, in addition to maintaining a separate list of personnel with authorized access to the Sovereign enclave area. The data centre floor incorporates badge, pin and biometric access controls, alarmed dual factor authenticated locked doors, CCTV, and 24x7 guards to enforce physical access authorizations at all access points. Physical security within the Rackspace office sites in the UK for the Sovereign operations center in Cardiff is specified as multi-factor authentication to all doors outside and inside the building. Certain areas within the building are part of a higher security level and are therefore controlled using a separated access control system with operating security team members vetted to at least BS7858, stationed within the UK and not connected to the globally accessible Rackspace security systems.

11. MAINTENANCE (MA).

11.1. Scheduled Maintenance. Rackspace shall coordinate maintenance windows to perform Scheduled Maintenance activities as required for the Cloud Infrastructure components that Rackspace supports. Rackspace shall notify Customer of Scheduled Maintenance at least five Business Days before maintenance is scheduled to occur. Scheduled Maintenance may be adjusted by Rackspace up to 24 hours in either direction (before or after the then-current maintenance schedule); however, to the extent Customer requires changes to the maintenance schedule, Customer shall coordinate such change within 24 hours of Rackspace notification.

11.2. Emergency Maintenance. On occasion, Emergency Maintenance may be required to maintain a security posture commensurate with the Compliance Baseline. Rackspace is authorized to perform all reasonable actions to meet or exceed requirements in connection with the delivery of the Services against the Compliance Baseline. Rackspace shall make every effort to provide advanced notification to Customers whenever possible, but specific circumstances may dictate immediate action without prior notification.

12. AVAILABILITY, CONTINGENCY PLANNING, BACKUP AND RECOVERY.

12.1. System Availability. Appliance availability and failover is accomplished via component resiliency at several levels. At the network level, WAN internet connectivity is delivered through Tier 1 internet service providers. The connectivity is available via Border Gateway Protocol (BGP), whereby Rackspace announces paths for public IPs amongst all carriers. In the event of a carrier, link, or device failure, traffic is automatically re-routed.

12.2. Redundant Architecture. From the edge WAN routers through to the host servers, all network devices and paths are redundantly meshed to prevent perceptible downtime in the event of the failure of any single device. Each host server has redundant path connections to both storage and production networks. Unless otherwise specified in a Service Order, the host servers powering the Production Environment are configured in an N+1 configuration featuring Rackspace Sovereign Clouds' high availability (HA) capability which shall restart any VM(s) from a failed host server on the remaining server nodes in the cluster.

12.3. Contingency Planning (CP). Rackspace maintains a Contingency Plan for the Rackspace Cloud Infrastructure as required by Compliance Baseline requirements. Rackspace shall support Customer Contingency Planning efforts by meeting the Recovery Point Objective and Recovery Time Objective in the event of a major disruption to the Production Environment. The SEAP shall be used to define the tools, processes, and procedures within the areas of responsibility of Rackspace and Customer. Rackspace shall provide one Disaster Recovery Test per year, upon Customer request with written notice 30 days prior. This can include turning on virtual machines at a secondary facility; running specific workloads at a secondary facility in a temporary, non-impactful way; verifying data backup integrity; or testing for hardware outages.

12.4. Disaster Recovery. Rackspace provides replication of Customer Production Environment OSIs and Customer Appliances to a Disaster Recovery Site. Rackspace manages the Disaster Recovery Site and provides disaster recovery support services in accordance with the SEAP. Upon a Disaster Declaration, replicated VMs are activated by Rackspace in the Disaster Recovery Site to seek to restore Services to support Restoration Success within the RPO and RTO. RTO does not include any third-party dependencies outside of Rackspace's control, including Customer application coming back online and time required for external third-party components and network protocols to be migrated by third-party providers. Any other application-level activities to recover and reconstitute the Customer Production Environment are the responsibility of Customer.

12.5. Relocation. Rackspace may move or relocate Customer's Production Environment and disaster recovery Services within or between data centre locations (located in the same country as the origin data centre and at the same security level). Additionally, Rackspace may make changes to the provision of the Services (including, but not limited to, changing the assigned IP addresses and DNS records and zones on Rackspace operated or managed DNS servers as Rackspace deems necessary for the operation of the shared network infrastructure). Rackspace would work with the Customer to migrate to any other location.

12.6. Data Replication Limitations, Warranty and Disclaimer.

(A) Customer Data. Rackspace makes no warranty as to the quality, contents, or formatting of Customer data. Customer accepts and acknowledges the limitations of data replication, specifically that data corruption and deletion within the Production Environment, both intentional and unintentional, will be replicated to the Disaster Recovery Site. As such, Disaster Recovery shall NOT be used as a replacement for application state and database backups, which remain the sole responsibility of Customer. Additionally, the rate at which the data in the Production Environment can be transferred to the Disaster Recovery Site shall vary depending on the rate of change, amount and type of data, constraints inherent in the Services, and fluctuations in bandwidth availability. Therefore, at any given time, the Disaster Recovery Site may not be completely up to date. In the event of a failover to the Disaster Recovery Site, data that has not yet completed transfer from the Production Environment shall be lost commensurate with the Recovery Point Objective. Customer also accepts and acknowledges that this same risk of data loss exists during execution of Disaster Recovery Testing. Rackspace is not liable for any data loss as a result of performing Customer initiated Disaster Recovery Testing, nor by executing Customer's instructions in the event of a legitimate Disaster Declaration.

(B) DR and Business Continuity. The Disaster Recovery Services provided are not a full business continuity solution. It is intended to be a component in a Customer managed and executed business continuity plan. As such, Rackspace takes no responsibility for, and does not guarantee, any business continuity capabilities as a result of Customer's use of the Disaster Recovery Services.

(C) Baseline RPO and RTO. Where Customer has not purchased DR, the Services shall be capable of meeting the RPOs and RTOs aligned with the Compliance Baseline; unless otherwise specified in a Service Order the default RPOs and RTOs are both 24 hours.

12.7. VM Replication Enhanced Edition. Solely where Customer purchases a DR service, then RPOs and RTOs shall not be set commensurate with the Compliance Baseline, but instead, the RPOs and RTOs shall be aligned with the Disaster Recovery Tier identified in the Service Order(s), as set out below:

Disaster Recovery Tier	RPO & RTO
Bronze	24 Hours
Silver	12 Hours
Gold	4 Hours
Platinum	1 Hour

12.8. Active-active. Alternatively, Customer can opt to deploy their Production Environments in an active-active manner, in which the Production Environment can always be running in the Disaster Recovery Site as well. Notwithstanding, Active-active configuration is a Customer responsibility, outside of the scope of the base Services configuration, and would typically require application-level support.

13. SUPPORT REQUESTS. Customer shall create a ticket using the method designated by Rackspace for all support requests, change requests, or incidents. Following the submission of the ticket, Rackspace's response time shall match the agreed-upon severity of the ticket, as described in section 15.1 Rackspace shall send an email notification to the requestor/creator of the ticket as well as the approver when a ticket is closed by Rackspace Support personnel.

14. INCIDENT RESPONSE. Management of an incident is subject to the following provisions:

14.1. Communication During Incident Management. Customer shall assist Rackspace in developing a SEAP that shall define the steps to be taken by Rackspace personnel when responding to incidents, tickets, and alerts.

During the incident management process, Rackspace and Customer shall communicate via means designated in the SEAP. Communications shall be made based on the timelines defined in the SLAs listed in section 15.

14.2. Cooperation. In the event that incident resolution requires Customer cooperation, such cooperation shall not be unreasonably withheld.

14.3. Rackspace Response. Upon incident receipt notification by phone call or Customer Portal, Rackspace shall respond to Customer via the ticketing method designated by Rackspace or phone call.

14.4. Post-incident Report. Rackspace shall use commercially reasonable efforts to provide the post-incident Customer incident report within two Business Days via email.

14.5. Point-of-Contact. Customer shall designate a primary point of contact to communicate with Rackspace regarding all technical issues that may arise during the term of any Service Orders in the agreement, including highlighting the priority and urgency of Customer tickets and requests.

14.6. Security Incident Response. In the event of a security incident in the Customer Infrastructure, such as a denial of service attack, Rackspace reserves the right to suspend Services without notice as necessary (e.g., powering off or network-isolating Customer Appliances and OSIs), until completion of remediation.

15. SERVICE LEVEL AGREEMENTS (SLA).

15.1. Initial Response Time. Customer is entitled to a credit of £250 or the failure of Rackspace to meet the section 15.1 Initial Response Time SLAs. The Initial Response Time begins upon the Rackspace system timestamp for submission of a ticket, resulting from a ticket being submitted by either (i) Customer or (ii) Rackspace Support through the Rackspace Support phone number.

Ticket Severity	Severity Definition	Initial Response Time
Severity 1	The total outage of service or availability of network connectivity (internet or internal), or mission-critical application availability, such that Customer cannot continue to operate its business due to the severity of the outage.	15 minutes
Severity 2	Either of the following: (i) A material degradation of service or availability of network connectivity (internet or internal), or network device failure, mission-critical application availability, or production hardware components, such that Customer can continue operating its business, but in a negatively impacted and degraded mode; or (ii) Any other support request not meeting the definition of Severity Level 1.	60 minutes

15.2. Availability SLAs. Rackspace guarantees 99.99% availability for Cloud Infrastructure averaged across the year. Customer shall be entitled to prorated monthly Fees for each full hour of downtime in excess of the Availability SLA.

15.3. Disaster Recovery SLA. Solely where Customer purchases the DR service, Rackspace guarantees that it shall meet the applicable RTO for the Disaster Recovery Tier. Rackspace makes no guarantee the RTO shall be achieved where the Customer does not purchase DR services; and in all circumstances Rackspace makes no guarantee that the RPO shall be achieved. Customer is entitled to a credit of £250 for the failure of Rackspace to meet the Disaster Recovery Time SLA.

15.4. Exceptions to the Credit Process. Credit shall not be issued due to failures that are, as determined by Rackspace, in its good faith reasonable judgment, the result of:

(A) Scheduled Maintenance or Emergency Maintenance;

(B) Written agreement between Rackspace and Customer confirming a change may be implemented without following the Change Control Processes;

(C) Customer-initiated work independently generated by Customer;

(D) Customer support requests not submitted through a method designated by Rackspace;

(E) Service interruptions requested by Customer;

(F) Violations of Rackspace's Acceptable Use Policy as may be updated from time to time at www.rackspace.com/information/legal/aup.php;

(G) Customer-required OSI revisions and hardware/software configurations that are not Rackspace tested/approved or that are out of support with the OSI or software vendor;

(H) Customer-created rules, objects, functional configuration errors, third-party software configuration, or other failure of Customer Appliances, software, or hardware, or third-party software or hardware;

(I) Events of Force Majeure;

(J) DNS issues outside the direct control of Rackspace;

(K) Patches or antivirus updates which contain code faults, flaws, or other errors attributable to the third-party vendors that created such code;

(L) Any suspension of the Services pursuant to the terms of the Agreement;

(M) A DoS attack or distributed denial-of-service attack (DDoS attack);

(N) Any actions or inactions of Customer, an end user, or any third party;

(O) Customer's equipment, software, or other technology and/or third-party equipment, software, or other technology (other than third-party equipment within Rackspace's direct control);

(P) Customer's failure to request SLA credits within 14 days of the applicable bill for which Services are invoiced; and/or

(Q) Manufacturer or safety code-related shutdowns required for safety compliance.

15.5. Service Level Credit Limitations. The SLA credit remedies contained in this section 15 are Rackspace's sole and exclusive liability and Customer's sole and exclusive remedy for any failure of Rackspace to meet an SLA. Customer must request SLA credits within 14 days of the applicable month for which Services are invoiced. The total credit available to Customer for all SLA failures in any particular calendar month shall in no event exceed the Monthly Service Fee for the environment in which the SLA failure occurred during that invoiced

month. Any credits available to Customer shall be applied to Fees due from Customer for the Monthly Services Fee and shall not be paid to Customer as a refund unless such credit pertains to the last month of Customer's service.

16. SERVICES LIMITATIONS AND RESTRICTIONS. Notwithstanding anything in the Customer Agreement (or other governing terms and conditions, if applicable): (i) Customer shall not use UK Sovereign Services in any situation where failure or fault of the Services could lead to death or serious bodily injury of any person, or to physical or environmental damage (including in connection with aircraft or other modes of human mass transportation, or nuclear or chemical facilities), (ii) the Services shall additionally be subject to the Rackspace Acceptable Use policy (as may be updated by Rackspace), which is located at: https://www.rackspace.com/information/legal/global/aup (iii) the Services shall additionally be subject to the Rackspace Global Security & Privacy Practices (as may be updated by Rackspace), which is located at: http://www.rackspace.com/information/legal/securitypractices; and (iv) the Services shall additionally be subject to the Rackspace End of Life terms (as may be updated by Rackspace), which is located at: https://www.rackspace.com/information/legal/eolterms.

17. AUDIT SUPPORT SERVICES. Upon at least 30 days of advance written notice, Rackspace provides up to 60 hours of security audit services for one security audit, per each 12-month period for each separate engagement following the Commencement Date of the applicable Service Order. Any additional security audit services required by Customer for each Project above this time cap, shall be available during Business Hours for £250 per person, per hour, if booked two or more weeks in advance. For less than two weeks of advance notice, additional security audit services shall be available during Business Hours for £350.00 per person, per hour. Additional security audit services requested outside of Business Hours are available for £450 per person, per hour. If the security audit is performed on behalf of an end Customer of Customer, Customer shall give Rackspace direct access to the end Customer and its auditors.

Schedule 1
ADDITIONAL DEFINED TERMS

"A&A Package" means the Assessment and Authorization set of documents, consisting of the System Security Plan, supporting security plans, test results, plan of action, and milestones.

"Applicable Law" means laws, Executive Orders, directives, policies, regulations, or other mandated compliance requirements.

"Available Hours" means the total number of hours in an applicable month less the number of Cloud Infrastructure downtime hours attributable to Scheduled Maintenance and Emergency Maintenance in the same month.

"Actual Uptime" means applicable monthly Available Hours less Customer Cloud Infrastructure downtime hours attributable to causes other than Scheduled Maintenance and Emergency Maintenance in the same month.

"Border Routers" means any routers that connect Rackspace's internal network to a transit or peering provider via Border Gateway Protocol (BGP). The external WAN interface uplinking the router to a third-party fiber or cross-connect provider is not included in this definition.

"Business Hours" means, for the sake of these Product Terms, 9:00 AM to 5:00 PM (Eastern Standard Time within the US, and Coordinated Universal Time within the UK), on Business Days.

"Compliance Baseline" means the defined set of security controls to which the Services are managed, as specified in the Service Order.

"Contingency Plan" means the artifact of the Compliance Baseline A&A Package required by all Cloud Service Providers. It denotes interim measures to recover information system services following an unprecedented emergency or system disruption. The Rackspace Contingency Plan is internal to Rackspace.

"Customer Access Switch" means the Rackspace-managed access switch uplinked to the Production Environment.

"Customer Appliance" means any Customer-owned and managed virtual machine (VM).

"Customer Portal" means Rackspace's Customer ticketing and/or notification portal.

"Cloud Infrastructure" means the hardware and software resources, which are located in enterprise-grade data centres, used to deploy the Services, including the host servers, switches, firewalls, hypervisor, and Operating System Instances (OSIs) provided by Rackspace, as set forth in Customer's Service Order(s). This excludes Customer Appliances.

"Disaster Declaration" means the submission by the authorized Customer representative of a ticket, via the ticketing method designated by Rackspace, declaring a disaster event and requesting that Rackspace initiate a restoration of the Production Environment at its Disaster Recovery Site.

"Disaster Recovery Site" means the secondary site where Customer production data will be replicated.

"Disaster Recovery Testing" means verifying the processes and services in place through simulated recovery of a mutually agreed-upon portion of the Production Environment in the Disaster Recovery Site.

"Emergency Maintenance" means any critical unforeseen maintenance or upgrades needed for the security, redundancy, or performance of the Production Environment, Rackspace infrastructure, and/or the Rackspace Network.

"Minimum Level Resources" means the committed minimum capacities for each resource used to provide the Services specified in the Service Order(s).

“Monthly Services Fee” means those monthly Fees incurred by Customer that are related to the Services provided by Rackspace under these Product Terms.

“Operating System Instance (OSI)” means an independent, functional virtual or bare metal server running an operating system that is both supported by the operating system manufacturer and offered by Rackspace. This excludes Customer Appliances.

“Parties” means Rackspace and Customer collectively. “Party” means Rackspace or Customer individually.

“Production Environment” means the total Customer environment, encompassing the entirety of contracted Services being delivered to Customer in support of Customer’s production cloud solution, but explicitly excludes any resources designated “non-production” and/or “dev/test”. This is inclusive of Cloud Infrastructure, Customer Appliances, OSIs, Compliance Baseline, and any optional Services as provided by Rackspace and set forth in Service Order(s).

“Privileged User” means any user of the Customer environment with access authority greater than users of the environment’s applications. Privileged Users include application, database, network, system, and security administrators.

“Recovery Point Objective” or **“RPO”** means the maximum period of permitted data loss upon Restoration Success, measured in hours preceding the time of failure.

“Recovery Time Objective” or **“RTO”** means the duration of time, measured in hours, between Rackspace confirmation of a Disaster Declaration and Restoration Success.

“Restoration Success” means that the Operating System Instances at the Disaster Recovery Site are online and available for Customer to use.

“Rackspace Equipment” means the Rackspace hardware used to provide the Services as set forth in these Product Terms.

“Rackspace Network” means the internal LAN-side Ethernet interface of the Border Routers to the Customer Access Switch via all Rackspace-owned and -managed networking hardware.

“Rackspace Support” means the 24 hours a day, seven days a week, year-round support made available by Rackspace via the ticketing method designated by Rackspace or by phone (at 0333 003 4000 or such other phone number as Rackspace may designate in the future).

“Scheduled Maintenance” means any planned maintenance or upgrades (including tech refreshes) needed for the security, redundancy, or performance of the Production Environment, Rackspace infrastructure, and/or the Rackspace Network.

“Security Domain” refers to the maintenance each of the UK Sovereign Services, e.g., Healthcare Cloud UK (and all Customer Cloud Infrastructure within each of the Services) with its own separate infrastructure and its own set of security controls.

“Solution Escalation Action Plan (SEAP)” means the jointly prepared Customer management plan that shall define the steps to be taken by Rackspace personnel when responding to incidents, tickets, and alerts. Specific monitoring thresholds are also documented in the SEAP.

“System Security Plan” means the main document of the A&A Package detailing how a Cloud Service Provider manages the security controls throughout the lifecycle of the Services, in accordance with the Compliance Baseline. In addition to the narrative of the security control implementation, it also includes a system description of the components and services inventory, and depictions of the system’s data flows and authorization boundary.

“vCore” means a unit of server compute resources.
“Fully Managed” Means Rackspace fully managing up to and including the guest operating system, deployment and licensing of Anti-virus, Monitoring & Vulnerability scanning services.

Schedule 2

Single-Tenant versus Multi-Tenant

	Single Tenant	Multi-Tenant
Racks and Cabinets	Dedicated Customer cabinets with full access management and auditing.	Dedicated cabinets to UK Sovereign Services Security Domain with full access management and auditing.
Sovereign Cloud Infrastructure	Dedicated Sovereign Cloud infrastructure and storage.	Choice of dedicated or shared hypervisors (Within the same Security Domain) Shared storage within the same Security Domain.
Power Redundancy	Fully resilient dual-DC design with fully managed Disaster Recovery.	Fully resilient dual-DC design with fully managed Disaster Recovery.
Active Directory and OS Hardening	NCSC-compliant AD policy with OS hardening as standard.	NCSC-compliant AD policy with OS hardening as standard.
VM Management and Tooling	Automatic enrolment of all VMs in management tooling.	Automatic enrolment of all VMs in management tooling.
Firewall	* The single-tenant environment is protected by Common Criteria 'PP Compliant' (EAL4+) firewall pairs to provide a hardened boundary within the Rackspace data centre. * Firewalls are fully managed to ensure network traffic always follows pre-defined routing and that the firewall configuration is maintained per NCSC guidance.	* Physical, multi-tenanted firewalls are deployed at the top level for complete segregation of Customer domains and access controls, and multiple failsafe's are in place to ensure there is no possibility of cross talk between tenants. * Top level platforms are protected by Common Criteria 'PP Compliant' (EAL4+) firewall pairs to provide a boundary within the Rackspace data centre. * Firewalls are fully managed to ensure network traffic always follows pre-defined routing and that the firewall configuration is maintained per NCSC guidance. * A software firewall is provided as standard for each Customer tenant (fully managed and pre-templated with EAL4+ standards), and upgradable to a physical device if required, at additional cost.
Switching	Underlying switch infrastructure is dedicated to the single tenant	Underlying switch architecture is dedicated to Sovereign services with individual pod's tenanting within it.

RACKSPACE GOVERNMENT CLOUD ON MICROSOFT AZURE

In addition to any other terms and conditions of Customer's Agreement with Rackspace, these Product Terms shall apply when Customer purchases Rackspace Government Cloud on Microsoft Azure Services.

1. ADDITIONAL DEFINED TERMS.

"**Applicable Data Protection Law**" means all applicable laws, rules, regulations, orders, ordinances, regulatory guidance, and industry self-regulations in relation to data privacy, including but not limited to the EU General Data Protection Regulation ((EU) 2016/679).

"Azure Services" means the online services, software, devices, or professional services that Microsoft makes available to Rackspace for its distribution or resale.

"**Azure Services SLA**" means the applicable Service Level Agreement provided by Microsoft for the Azure Services (presently found at the following URL: http://www.aka.ms/csla), as may be updated by Microsoft.

"**Azure Subscription**" means Customer's Azure account(s) on which Rackspace is identified as Customer's CSP partner.

"**Azure VM**" means the virtual machines deployed on the Azure Services for which Customer has purchased enhanced support from Rackspace.

"**Controller**", "**Processor**", "**Data Subject**", "**Personal Data**", and "**Process**" or "**Processing**" shall all have the meanings set out in Applicable Data Protection Law. "**Customer Data**" means all data, including all text, sound, video, image files, and software that are provided to Microsoft or Rackspace by, or on behalf of, Customer through use of the Azure Services.

"**Compliance Baseline**" means the defined set of security controls to which the Services are managed, as set out in the Service Order.

"**Customer Success Manager**" means Rackspace personnel tasked with providing general relationship support and guidance to Customer related to Azure Services purchased pursuant to these Product Terms.

"**Disaster Recovery Site**" means the secondary site where Customer production data shall be replicated.

"**Disaster Declaration**" means the submission by the authorized Customer representative of a ticket via the Customer portal declaring a disaster event and requesting that Rackspace initiate a restoration of the Production Environment at its Disaster Recovery Site.

"**Emergency Maintenance**" means any critical unforeseen maintenance or upgrades needed for the security, redundancy, or performance of the Production Environment, Rackspace infrastructure, and/or the Rackspace Network.

"**Landing Zone**" means an assured 7-security domain landing zone.

"**Lead Cloud Engineer**" means a named Rackspace cloud engineer with credentials certifying engineering expertise on Azure Services.

"**Microsoft Customer Agreement**" means the applicable regional version (based on Customer's location) of the agreement that Microsoft uses to convey or provide Azure Services to Customer (presently found on the

following URL: https://docs.microsoft.com/en-us/partner-center/agreements), as may be updated by Microsoft from time to time.

"**PII**" means personally identifiable information as defined by the Applicable Data Protection Law.

"**Privileged User**" means any user of the Customer environment with access authority greater than users of the environment's applications. Privileged Users include application, database, network, system, and security administrators.

"**Production Environment**" means the Customer Configuration excluding any resources designated as "non-production", "dev/test" or identified with similar language.

"**Rackspace Network**" means the TCP/IP stack of all Rackspace-owned and -managed networking hardware and software.

"**Recovery Point Objective**" means the maximum period of permitted data loss upon Restoration Success, measured in hours preceding the time of failure.

"**Recovery Time Objective**" means the duration of time, measured in hours, between Rackspace confirmation of a Disaster Declaration and Restoration Success.

"**Restoration Success**" means that the operating system instances at the Disaster Recovery Site are online and available for Customer to use.

"**Reserved Instances**" means a pre-paid commitment by Customer to purchase specific Azure Services within a distinct region in exchange for receiving a discount on those Azure Services purchased, or any other comparable Azure Services discounting mechanism.

"**Scheduled Maintenance**" means any planned maintenance or upgrades (including tech refreshes) needed for the security, redundancy, or performance of the Production Environment, Rackspace infrastructure, and/or the Rackspace Network.

"**Solution Escalation Action Plan (SEAP)**" means the jointly prepared Customer management plan that shall define the steps to be taken by Rackspace personnel when responding to incidents, tickets, and alerts. Specific monitoring thresholds are also documented in the SEAP.

"**Technical Account Manager**" means Rackspace personnel tasked with providing support and guidance to Customer on Azure Services purchased pursuant to these Product Terms.

2. ITIL SERVICE MANAGEMENT.

2.1. Personnel Security (PS). All Rackspace personnel with access to the Customer environment shall meet the personnel security requirements set out in the Service Order. An employee's assignment to any such Customer workloads is contingent upon achieving relevant security screening as set out in the Service Order. If Customer requires personnel security approvals or clearances outside of Rackspace's standard background investigation, then Rackspace reserves the right to submit for approval and/or clearance its entire operations and security teams associated with the Services to enable adequate support at Customer cost.

2.2. Awareness and Training (AT). All Rackspace staff receive annual data privacy and information security awareness training. In addition, all Rackspace engineering staff supporting the Production Environment shall be appraised of the applicable Customer-security policies.

2.3. Customer Success Manager. In addition to service desk support, Rackspace shall provide access to a Customer Success Manager including for service reporting, problem management and incident management.

2.4. Technical Account Manager. Rackspace shall provide access to a Technical Account Manager for Customer to contact, via phone and ticket, regarding possible Azure Services infrastructure modifications and to conduct quarterly account reviews with Customer.

2.5. Lead Cloud Engineer. Rackspace shall provide a Lead Cloud Engineer to assist Customer with support and cloud development activities on an ongoing basis, as mutually agreed between Customer and Rackspace. Specific deliverables provided pursuant to these Services shall be mutually identified and agreed between Customer and the Lead Cloud Engineer at the start of these Services, and shall be updated and revised at regular intervals, in accordance with Customer's purchased support tier. Customer's Lead Cloud Engineer is a shared resource. The number of other Rackspace customers with whom Customer shares the Lead Cloud Engineer is determined by Customer's purchased support tier. All support requests made pursuant to these Services from any Rackspace customer to which the Lead Cloud Engineer is assigned are prioritized on a first come, first served basis. Response times for these Services are not subject to any SLA. Based on the support tier selected by Customer, the named lead cloud engineer shall be shared between a set number of other Rackspace customers, as further detailed in the Service Order. In order to request services from Customer's assigned Lead Cloud Engineer, Customer must submit a ticket request through the Rackspace customer portal or call the Rackspace support team.

2.6. Configuration Management (CM). Rackspace uses a baseline configuration based on Compliance Baseline. Rackspace follows ITIL aligned change and configuration management procedures detailed in Customer's service runbook. As part of Rackspace's configuration management process, all proposed changes are recorded and analyzed for impact, and any Customer-impacting changes are coordinated with the Customer using the runbook change management process. Customer is not entitled to a credit under any SLA if Customer confirms in writing that a change may be implemented without following, or if Customer implements a change in contravention of, any change management procedure set out in the runbook. In addition, automated deployment tools automatically apply the Rackspace assured baselines when VMs are deployed, and maintain those baselines by comparing any changes to the baseline, at least once per quarter, as the system is being used. Any Customer-defined hardening, other than the Rackspace-defined configuration baseline, shall be stated in any applicable Service Order(s), which shall include additional implementation and management fees.

2.7. Maintenance (MA). Rackspace shall coordinate maintenance windows to perform Scheduled Maintenance activities as required for the Customer Configuration components that Rackspace supports. Rackspace shall notify Customer of Scheduled Maintenance at least five Business Days before maintenance is scheduled to occur; notification shall be via Customer portal. Scheduled Maintenance may be adjusted by Rackspace up to 24 hours in either direction (before or after the then-current maintenance schedule); however, to the extent Customer requires changes to the maintenance schedule, Customer shall coordinate such change within 24 hours of Rackspace notification. On occasion, Emergency Maintenance may be required to maintain a security posture commensurate with the Compliance Baseline. Rackspace is authorized to perform all reasonable actions to meet or exceed requirements in connection with the delivery of the Services against the Compliance Baseline. Rackspace shall make every effort to provide advanced notification to Customer whenever possible, but specific circumstances may dictate immediate action without prior notification. Customer is not entitled to a credit under any SLA resulting from Scheduled Maintenance or Emergency Maintenance.

3. AZURE CSP MANAGEMENT.

3.1. Azure Services. If Customer purchases Azure Services from Rackspace, pursuant to these Product Terms, default settings shall be applied to the Azure Services (including Azure Subscriptions) provisioned by Rackspace on Customer's behalf. Customer acknowledges that if Rackspace resells the Azure Services to Customer then Customer's use of those Azure Services is subject to the Microsoft Customer Agreement, which is effective without signature. Microsoft is a third-party beneficiary under the Agreement to the extent necessary to exercise its rights under and enforce Customer's compliance with the Microsoft Customer Agreement. Notwithstanding the foregoing, Microsoft may decline to provide Azure Services to Customer in its sole discretion, and/or Microsoft may require Customer's direct acceptance to the Microsoft Customer Agreement prior to providing Azure Services. Customer releases Rackspace from any and all liability whatsoever arising out of or in connection with the Azure Services, Microsoft's provision, management, operation of, or failure to provide the Azure Services, and Microsoft's exercise of its rights in the Microsoft Customer Agreement or

Customer's breach thereof. Notwithstanding anything to the contrary, Azure Services are excluded from the definition of "Services", and Fees for Azure Services are excluded from any limitation on damages calculation.

3.2. Provisioning. Rackspace may resell to Customer a subscription for the Azure Services and help Customer to provision its Azure account(s).

3.3. Environment Management. Rackspace shall provide support for the Customer's Azure Services. Rackspace will provide technical and operational support for billing inquires, cost optimization inquiries, and for issues arising out of the Azure Services purchased under these Product Terms (e.g. general to expert-level inquiries on specific Azure Services). Customer must submit support requests directly to Rackspace. If Rackspace determines the root cause of an issue is related to Azure Services, Rackspace will escalate directly to Microsoft.

4. AZURE LANDING ZONE MANAGEMENT.

4.1. Design & Deployment. Unless specified to the contrary in the Service Order, Rackspace shall also deploy a Landing Zone in accordance with the Compliance Baseline.The number of Landing Zones shall be as set out in the Service Order.

4.2. Identification and Authentication (IA). The Rackspace management environment maintains a separate Active Directory to the general Rackspace corporate environment, the Rackspace Government services environment, and Customer environments. Rackspace engineers are issued with unique access accounts for the management environment that are separate to their Rackspace corporate account. When connecting to Customer Configuration, Rackspace engineers are issued with Customer domain accounts to enable the Customer to ensure security controls are enforced and that activity is tracked according to Customer acceptable use and security policies.

4.3. Audit and Accountability (AU). Rackspace configures all elements of the Landing Zone to feed audit information into the SIEM that provides near-real-time log collection, indexing, and management dedicated to the Customer including (i) system security logs, (ii) IDS logs, (iii) firewall logs. Customer's SIEM logging service provides Rackspace security engineers and analysts with a suite of automated and manual tools to extract audit information. Logs are collected and retained online for 12 months. Customer is responsible for retaining application and database audit records online, in order to provide support for after-the-fact investigations of security incidents and to meet their respective regulatory and organizational information retention requirements. Customer may purchase additional Services to store their logs, and Customer retains all responsibility for configuration and management of these additional log sources. In the event of a security incident or suspected incident, logs assist in determining: (i) if there was an incident, (ii) who was involved in the incident, (iii) when the incident took place, (iv) what type of incident took place, and (v) how the incident occurred.

4.4. Maintenance. Rackspace shall control and manage all changes to the Landing Zone. Customer is not permitted to make changes to the Landing Zone, but may submit requests to Rackspace for changes which shall be assessed by Rackspace as to conformity with the Compliance Baseline. Rackspace shall not be responsible or liable (including under any SLAs) for any changes made by Customer to the Landing Zone unless specifically authorized by Rackspace in the Service Order, or otherwise by an authorized representative of Rackspace in writing, and may charge fees at Rackspace standard rates for any remediation of unauthorized Customer changes. Rackspace shall provide all information reasonably requested by Customer in support of Customer's annual assurance testing.

5. PROACTIVE OPERATIONAL MANAGEMENT. Rackspace shall provide the following additional security Services. Compliance Baseline requirements for any software or program installed on top of the Rackspace provided and managed hardware and software Services, are the sole responsibility of Customer.

5.1. Tooling. Rackspace shall provision an access management tool to be utilized in provisioning of short-lived, access-limited, fully audited secure access servers within Customer's Azure Services, and which shall be used by Rackspace when engaging in environment support and OS management activities.

5.2. System and Communication Protection (SC). Rackspace utilizes a dedicated secure management environment to provide all support functions for the Services. This management environment is maintained as an environment totally separate from the Rackspace corporate network and the Customer's Production Environment in accordance with the Compliance Baseline. The managed Customer Landing Zone is made up of seven distinct network zones to maintain separation between Customer production areas. Access to each environment is controlled by a central logical firewall. Rackspace support staff cannot connect directly to the Customer's Production Environment and must use a dual-hop authentication path from any endpoint device. Customer is responsible for controlling access to production services through Customer-managed, application-defined mechanisms.

5.3. Access Control (AC). Rackspace will utilize a management environment to provide audited and controlled Privileged User access to the Production Environment. All connections into the Production Environment will be made using dedicated secure VPN tunnels to Rackspace 'edge node' server clusters that are built in accordance with configuration security policies and controls. All Rackspace engineer Privileged User access accounts shall be granted according to Customer policy agreed with Rackspace. All Rackspace engineer Privileged User access to the Production Environment is recorded and logged for Rackspace internal audit purposes, and to aid in any security incident analysis and response. Rackspace shall be responsible for and have administrator control over the domain, forest and/or organizational units that comprise the computer, user and service accounts that pertain to, and provide access to the Production Environment.

5.4. Azure Portal Management. Rackspace shall provide Azure portal management. The Customer can be provided with read-only access to the Azure portal upon request to Rackspace. Rackspace must be provided with owner-access to Azure subscription at all time during the Term.

5.5. Guest OS Management. Rackspace shall provide Azure VM instance creation, deletion, maintenance (including patching and troubleshooting) and change of supported Linux and Windows operating systems on behalf of Customer.

5.6. Firewall Management. Rackspace shall provide firewall management. Customer shall not have firewall access.

5.7. Quarterly Configuration Compliance Scanning and Reporting. Rackspace scans the managed Customer Configuration for compliance with the Rackspace-defined hardening configuration standard. Rackspace shall conduct these scans on a quarterly basis.

5.8. Endpoint Security Management. Rackspace provides a centrally managed endpoint security software platform for all Customer VMs under Rackspace management. The endpoint security management solution provides centralized anti-virus, and malware defense. If specifically set out in the Service Order, Rackspace shall also provide host-based intrusion prevention services. Rackspace provides ongoing management of the management servers, agents installed on VMs and associated configurations, updates, and policy management. If a security event is detected, Rackspace shall notify and collaborate with Customer to determine the appropriate actions.

5.9. Risk Assessment (RA). Rackspace will perform monthly vulnerability scanning for each managed Landing Zone. The scans are performed by Rackspace and reports can be provided to the Customer upon request. Rackspace and Customer shall mutually agree on a monthly scanning schedule for the duration of the Services. Any custom vulnerability scanning activities and associated reporting requested by Customer shall be stated in any applicable Service Order(s), which shall include additional implementation and management fees.

Customer's security obligations include immediately remediating any known security vulnerability of any software or program installed on top of the Rackspace provided and managed hardware and software Services.

5.10. 24x7 Monitoring and Alerting. Rackspace shall enable automated alert monitoring on Customer's Azure Services. Alerts settings shall be configured by Rackspace, in conjunction with Customer, during the on-boarding process. Rackspace monitors the performance, availability, and network connectivity of supported

Customer servers 24x7. By default, all alerts are configured to go to Rackspace, but the SEAP can be updated to define Customer notification and escalation criteria.

5.11. Disaster Recovery. Rackspace provides replication of Customer's Production Environment operating system instance and any Customer owned and managed application to a Disaster Recovery Site to seek to enable the ability to meet a Recovery Point Objective and Recovery Time Objective commensurate with the Compliance Baseline. Unless otherwise specified in a Service Order, the default Recovery Point Objective and Recovery Time Objective are both 24 hours. Rackspace manages the Disaster Recovery Site and provides disaster recovery support services in accordance with the SEAP. Upon a Disaster Declaration, replicated instances are activated by Rackspace in the Disaster Recovery Site to restore Services to support Restoration Success within the Recovery Point Objective and Recovery Time Objective. Recovery Time Objective does not include any third-party dependencies outside of Rackspace's control, including Customer application coming back online and time required for external third-party components and network protocols to be migrated by third-party providers. Any other application-level activities to recover and reconstitute the Customer Production Environment are the responsibility of the Customer. Alternatively, the Customer can opt to deploy their Production Environments in an active-active manner, in which the Production Environment can always be running in the Disaster Recovery Site as well. Active-active configuration is a Customer responsibility, outside of the scope of the base Services configuration, and would typically require application-level support.

6. SUPPORT HOURS AND REQUIREMENTS.

6.1. Support Hours. Support for Rackspace Government Cloud on Microsoft Azure Services (including technical and operational support) shall be provided 24*7*365 as follows: (i) Rackspace engineer support for the Azure Services shall be available 7am to 6pm during Business Days; and (ii) outside of these core support hours, support shall be provided on an 'as available' basis by on-call engineers for Emergency severity level SLA incident. If Rackspace requires Customer cooperation to provide support, such Customer cooperation shall not be unreasonably withheld or delayed or conditioned.

6.2. Available Microsoft Regions. Notwithstanding anything to the contrary in the Agreement, available Microsoft regions shall be restricted to the regions stated in the Service Order. Rackspace may further limit the included offerings due to compliance and/or functional requirements.

6.3. Digital Partner of Record. If Customer provides its own license for the Azure Services, Customer acknowledges and agrees to designate Rackspace as the "Digital Partner of Record" during the term of the applicable Service Order.

6.4. Agent for Third Party Software. Rackspace may agree to install third-party software (e.g., from the Azure Portal) as part of the Services. Where such activity requires the acceptance of any TPS Agreements (or similar terms), Customer hereby authorizes Rackspace to accept such TPS Agreements on Customer's behalf, and Customer agrees to be bound by and adhere to such terms, and acknowledges that Customer, not Rackspace, is bound by such terms. Rackspace shall notify Customer via ticket when Rackspace accepts any TPS Agreements on Customer's behalf and direct Customer to a copy. Rackspace will not engage in negotiation on Customer's behalf.

6.5. Support Services Limitation. For issues involving Customer's third party suppliers and vendors other than Microsoft, Rackspace may identify the issue and assist Customer by participating in conference calls with the third party supplier, but all communications must be initiated and coordinated by Customer. Customer also acknowledges and agrees that Rackspace is not liable for services or support provided by or to Customer's third party supplier(s).

7. SLAs.

7.1. SEAP. Customer shall assist Rackspace in developing a SEAP that shall define the steps to be taken by Rackspace personnel when responding to incidents, tickets, and alerts.

7.2. Initial Response Time. Rackspace shall provide an initial response to Customer's support requests submitted to Rackspace via ticket in the following timeframes. All support requests must be made directly to Rackspace, and Rackspace shall escalate to Microsoft directly, if needed. Support requests may be submitted 24x7 and will automatically be assigned a "Standard" severity level, which may be adjusted by Rackspace as necessary. Support requests initiated by telephone will be logged as tickets by Rackspace support, as necessary. Customer may submit support requests directly to Rackspace by telephone or ticket using the contact information provided in the Guide, provided that the service level guarantee in this Section 7.2 only applies to ticket based requests. Customer agrees not to submit support requests directly to Microsoft. Rackspace will not respond to and does not make any service level guarantees regarding support requests Customer submits directly to Microsoft.

Severity	Definition	Contact Method	Initial Response Time
Emergency	Business-critical system outage / extreme business impact	Automated alert or phone	15 minutes
Urgent	Business critical system outage / extreme business impact / production system outage / significant business impact	Automated alert, ticket, or phone	60 minutes
High	Production system Impaired / Moderate Business Impact	Automated alert, ticket, or phone	4 hours
Normal	Issues and requests / minimal business impact	Automated alert, ticket, or phone	12 hours
Low	General information, questions, and guidance	Ticket or phone	24 hours

7.3. Remedy. If Rackspace fails to meet the time initial response times in Section 7.2, Customer is entitled to a credit of $250 per event, up to 100% of Customer's monthly recurring support fee for the calendar month. If Customer is paying for Customer Services in a currency other than US Dollars, this credit shall be converted to the currency in which Customer pays for its Services as of the date of the invoice on which the credit is applied. Customer is not entitled to a credit under this Section 7.3 if the event giving rise to the credit occurred because of the unavailability of Customer's Microsoft Azure Services or because of Rackspace's inability to access Customer's Microsoft account (if such inaccessibility is caused by Customer or Microsoft). Customer is not entitled to a credit if Customer is in breach of the Agreement (including Customer's payment obligations to Rackspace) at the time of the occurrence of the event giving rise to the credit. Customer must request a credit through Customer's Rackspace account within seven days following the event giving rise to the credit.

7.4. Microsoft Azure Services SLA. Microsoft provides an Azure Services SLA to Customer that may be periodically updated by Microsoft. Customer may not go directly to Microsoft with service level inquiries or requests for remedies. If Customer makes an SLA claim, Rackspace will promptly escalate the claim to Microsoft or review. Customer must notify Rackspace of any service level requests by the end of the billing cycle in which the service incident giving rise to the SLA claim occurred. Rackspace shall apply any credits granted under the Microsoft Customer Agreement pursuant to a SLA claim within 60 days of receipt. Credits cannot exceed the total monthly estimated retail price of the affected Azure Service.

8. ACCESS TO CUSTOMER'S CUSTOMER DATA AND CUSTOMER ACCOUNT INFORMATION. By using the

Rackspace Government Cloud on Microsoft Azure Services, Customer acknowledges that Rackspace and/or Microsoft may have access to Customer Data. Customer acknowledges that Microsoft may collect, use, transfer, disclose, and otherwise process Customer Data, including PII, as further described in the Microsoft Customer Agreement. Personal Information (as such term is defined in the Rackspace Privacy Statement) that Rackspace collects about Customer (other than Customer Data) during the purchase, account sign-up, use or maintenance of Customer's account, shall be processed by Rackspace in accordance with its then-current Privacy Statement, a current version of which is located at www.rackspace.com/information/legal/privacycenter.

9. DATA PRIVACY.

9.1. Customer agrees that Customer is the Controller and primary Processor of Customer Data. Customer consents to the processing of Customer Data in, and the transfer of Customer Data into, the Microsoft regions selected by Customer. Customer may specify the Microsoft regions in which Customer Data will be stored and accessible by Customer and its end users. Rackspace shall not move Customer Data from Customer's selected Microsoft regions without Customer's instructions and without notifying Customer, unless required to comply with the law or requests of governmental entities. Such Processing of Customer Data is subject to this Agreement and the Microsoft Customer Agreement.

9.2. Customer shall and shall require its end users to process any Customer Data that includes PII in compliance Applicable Data Protection Law. Customer agrees that if the Microsoft region Customer selects for storing Customer's PII is outside of Customer's or its end users own state, province, country or other jurisdiction, then Customer's and its end users obligations to comply with Applicable Data Protection Law includes an obligation to comply with the law of the state, province, country or other jurisdiction in which the PII is stored. Customer shall not, by any act or omission, place Rackspace or its Representatives in breach of Applicable Data Protection Law.

10. FEES.

10.1. Offer Fees. Rackspace shall charge Customer the current Azure pay-as-you-go rates for Customer's use of the Azure Services if purchased from Rackspace. Rackspace shall obtain Customer's Azure usage and billing information directly from Customer's Azure account. Customer will be responsible for all fees and charges accrued under Customer's Azure subscription(s), regardless of whether such fees and charges accrued before or after the date of transfer to Rackspace.

In addition to the fees payable for Azure Services, Customer shall pay fees for Rackspace Government Cloud on Microsoft Azure support services as follows: (i) Customer shall be charged a monthly recurring fee for the Lead Cloud Engineer support tier selected, as stated in the Service Order; (ii) Customer shall be charged a monthly recurring fee for each Landing Zone, as stated in the Service Order; (iii) Customer shall be charged a utility fee for actual Service usage based on the number of Azure VMs. Utility fees are subject to change on a monthly basis depending on Customer's actual usage, and the fees stated in the Service Order.

10.2. Billing Details. Recurring Fees (including utility fees) shall be billed monthly in arrears, and any one-time Fees shall be billed immediately as incurred. Because Fees are billed in arrears, Customers may receive invoices for Services after decommissioning a device. Rackspace may continue to bill Customer after the termination or expiration of these Product Terms or applicable Service Order for Fees incurred prior to such termination or expiration. If Customer has arranged for payment by credit card or direct debit or ACH, Rackspace may charge Customer's card or account on or after the invoice date.

11. RESTRICTIONS. Unless otherwise conspicuously stated in Customer's Agreement, Customer is prohibited from reselling the Services. Customer is prohibited from selling, transferring, or sublicensing Customer's Rackspace or Azure Services account credentials to any other party (except to agents and subcontractors performing work on Customer's behalf).

12. CHANGES TO AGREEMENT. **Notwithstanding anything in the Agreement to the contrary, Rackspace may change the terms of this Agreement at any time, effective immediately as required to comply with the**

reseller agreement between Microsoft and Rackspace or in response to changes made by Microsoft to the reseller agreement between Microsoft and Rackspace. This includes changing the fees applicable to the Services. Additionally, Rackspace may suspend or terminate these Services (including Azure Services), any Service Order for these Services, and/or the Agreement immediately if Rackspace or Microsoft determine such suspension or termination is necessary to comply with law or regulation, if otherwise permitted under the Microsoft Customer Agreement, or if Microsoft no longer permits resale of the Microsoft Service.

13. TERM. The Initial Term of the Services will be as defined in, and commence upon the earlier of Customer's signature of the applicable Service Order or Customer's first use of the Services; however notwithstanding anything to the contrary in the Agreement, the Initial Term shall be no less than 12 months. Upon expiration of the Initial Term, the Services will renew for consecutive, rolling 90 day terms unless: (i) otherwise stated in the Agreement, (ii) the parties enter into an agreement for a Renewal Term, or (iii) either party provides the other with written notice of termination at least 90 days prior to the expiration of the then current term.

14. TERMINATION. Customer will have access to Customer Data following termination of Azure Services in accordance with the Microsoft Customer Agreement.

15. DISCLAIMERS.

15.1. To the extent permitted by law, Rackspace disclaims all liability for damages under this Agreement, whether direct or indirect, incidental or consequential, arising from Customer's use of the Azure Services or other related Microsoft products.

15.2. Unless conspicuously stated to the contrary, Customer is solely responsible for managing and maintaining any and all backups of Customer's data, performing and testing restores, and testing Customer's systems and monitoring the integrity of Customer's data.

UK Sovereign Services

SOVEREIGN SECURE PRODUCT TERMS

In addition to any other terms and conditions of Customer's Agreement with Rackspace, these Product Terms shall apply when Customer purchases (or accesses) Rackspace Sovereign Secure as described herein, at either the Bronze Services tier or the Silver Services tier, (individually, "**Sovereign Secure Bronze**" or "**Sovereign Secure Silver**", and collectively, "**Sovereign Secure**" or the "**Services**").

1. ADDITIONAL DEFINED TERMS.

"**Add-on Services**" means the Rackspace add-on Services available to Customer for purchase and use with Rackspace Sovereign Cloud.

"Sovereign Secure" refers to Rackspace Managed SOC & SIEM 24x7x365 managed security service designed to protect, detect, and respond to cyber threats and malicious activity detected on Endpoints within Customer's on-premises, Rackspace Sovereign Cloud or multi-cloud environment, as further described herein.

"Business Hours" with respect to Sovereign Secure means 24 hours a day, 7 days a week for incident management / response and 9x5 Mon-Fri for changes.

"Covered Environment" means the set of Endpoints compatible with and supported by Sovereign Secure and documented to be within scope of the Services during the implementation process.

"Endpoint" means a physical or virtual device that connects to and exchanges information through the Customer network, identified as within scope of the Services during deployment. Endpoints may include but are not limited to physical machines, network, virtual machines, embedded devices, and servers, deployed either on-premises, Rackspace Sovereign Cloud or within hybrid cloud or multi-cloud environments and provided with either an IP address or Fully Qualified Domain Name (FQDN).

"Endpoint Detection & Response" or "EDR" means the technology and/or platform that is leveraged to collect and analyze data from Customer's Endpoints to detect and report any suspicious activity back to the Sovereign SOC for further analysis and response.

"Endpoint Detection & Response Agents" or "EDR Agents" means the agents deployed on designated Endpoints within the Covered Environment to provide the EDR functions.

"**SIEM**" means security incident and event management and refers to the approach and/or platform used to address cybersecurity. A SIEM platform collects, aggregates, and analyzes security-related data from various sources within an organization's IT infrastructure.

"**Sovereign SIEM**" means the centralized platform used by Sovereign Secure that collects, aggregates, and analyzes security data from various sources to detect, investigate, and respond to security incidents in real-time.

"**Security Operations Center**" or "**SOC**" means a centralized unit that continuously monitors, detects, analyzes, and responds to cybersecurity incidents using advanced tools and threat intelligence to protect an organization's IT infrastructure.

"**Sovereign Security Operations Center**" or "**Sovereign SOC**" means the centralized function and operations center provided by Sovereign Secure that continuously monitors, detects, analyzes, and responds to cybersecurity incidents by leveraging the information from the Sovereign SIEM.

"**Rackspace Managed Endpoint**" means an Endpoint that is under the full administrative control of Rackspace, which includes the access rights and credentials to change policy, alter security posture, and generally exercise full control of the Endpoint.

"**Customer Managed Endpoint**" means an Endpoint that remains under the full administrative control of Customer (or Customer delegate, such as a third party retained by Customer).

"**Rackspace Sovereign Cloud**" or "**Sovereign Cloud**" means the computing environment provided with Rackspace UK Sovereign Services, as described in the applicable Product Terms, as may be updated, and presently located at: https://www.rackspace.com/information/legal/UK-sovereign-services.

"**Designated Customer Contact**" means a Customer contact that is authorized to submit and manage, on behalf of Customer, Customer support tickets, software policy, escalation requests, and who is generally authorized leverage the support resources available under Sovereign Secure. Customer may designate a reasonable number of Designated Customer Contacts to interface directly with Rackspace as required to effectively manage the Services.

2. OVERVIEW. Sovereign Secure Silver provides a 24x7x365, Rackspace-managed SOC & SIEM platform, staffed with Rackspace security resources, to monitor, detect, analyze and respond to cyber threats and malicious activity within the Covered Environment (as further described in section 3). Sovereign Secure Silver consists of Endpoint protection with physical machines, virtual servers and network devices, and scope of Services includes Customer on-premises deployments, and Rackspace Sovereign Cloud, hybrid cloud and multi-cloud environments. Sovereign Secure Bronze, provided at no charge, provides Customers with centralized log streaming to the Sovereign SIEM for forensic analysis during onboarding to the Rackspace Sovereign Cloud platform (as further described in section 4).

3. SOVERESIGN SECURE SILVER SERVICES. At the Sovereign Secure Silver tier, Rackspace shall provide implementation and setup of the EDR Agents in the Covered Environment, and active management of Services by the Sovereign SOC as follows:

3.1. Deployment Services. The implementation and setup includes the following deployment-related professional services:

3.2. Service Deployment Kick-off Process. Initial onboarding and Customer orientation to the Rackspace support model. During the kick-off, deployment project plan, key milestones and deliverables, and Designated Customer Contacts, are reviewed and agreed upon by the parties.

3.3. Environment Discovery. The discovery workshops to identify and develop deployment requirements, and to ensure that deployment requirements are mutually understood. Customer participation is required, and Customer will provide points of contact, key stakeholder contacts, and escalation points (if different than the Designated Customer Contacts) as needed for the Services deployment and operations.

3.4. Infrastructure & EDR Agent Deployment. Rackspace shall configure Sovereign Secure for Customer onboarding and deploy the EDR Agents onto designated Endpoints within the applicable Covered Environment (as indicated within the Service Order), subject to compatibility with the Rackspace Configuration Requirements. as may be reasonably communicated to Customer by Rackspace.

3.5. Additional EDR Agent Deployments. If, following the initial deployment, additional EDR Agents are requested or introduced into the Covered Environment, Rackspace will evaluate the additional target systems and/or Endpoints to determine if the existing policy design and deployment methodology can be utilized. If customization or additional environmental discovery is needed, additional fees may apply.

3.6. Detection and Correlation. Rackspace shall deploy and configure the detection and correlation rules available from the EDR ruleset, along with enrichment data sources as available.

3.7. Automation Runbook Configuration. Rackspace shall deploy a default runbook that activates automatic notification to the Sovereign SOC when a security alert or event occurs that requires investigation or a response. Rackspace shall develop and deploy additional runbooks to automate pre-approved actions that can assist in the security incident response process.

3.8. Assessment, Validation and Signoff. Rackspace and Customer shall hold Service deployment validation workshops to ensure that the Sovereign Secure tooling has been appropriately deployed and configured. Customer may be informed when the Sovereign Secure tooling has been successfully deployed.

3.9. Dashboards and Reporting. Rackspace shall configure and deliver reports, as may be agreed from time to time with Customer. The use-cases for the creation of these reports will be agreed between the parties.

3.10. Log Retention. Logs shall be retained for 365 days.

3.11. EDR Agent Health. Rackspace will proactively monitor and manage the health of EDR Agents deployed in the Covered Environment. If the health of an EDR Agent and/or connector is compromised, Rackspace will use its asset management footprint to proactively remediate to ensure continuity of the Services. If Rackspace does not have administrative level access to the in scope Endpoint, the Sovereign Service support desk will notify Customer and provide Customer with the guidance required to return the EDR Agent(s) footprint back to a healthy status.

3.12. Event Triage. The Sovereign SOC shall conduct monitoring of the Covered Environment for malicious behavior and shall investigate each resulting incident to determine the validity of the incident and assign security incident priorities. This process includes both manual and automated techniques to collect contextual data and determine whether the incident is a true positive, false positive or benign positive. Security incident priorities (i.e., P1, P2, P3, P4) shall be assigned determined per the ITIL standard (Information Technology Infrastructure Library) by combining the 'Impact' and 'Urgency' criteria, as described in the following section 3.13.

3.13. Priority Level Assignment. Per ITIL, 'Urgency' is a measure of how quickly a resolution is required based upon the nature of the incident (i.e., potential for rapid escalation of damage, criticality of affected operations, etc.). For Customer-submitted tickets, Customer will initially designate the 'Urgency' level, which may be reasonably modified by Rackspace. Per ITIL, 'Impact' is a measure of the extent of the incident and of the potential damage which may be caused by it before it can be resolved; Impact is initially determined by Rackspace but may be reasonably modified by Customer subject to mutual agreement.

Table 1.

Security Incident Prioritization: Urgency & Impact

			Impact		
			High	Moderate	Low
			Priority Level		
Urgency	High	**Priority Level**	P1 – Critical	P2 – High	P3 – Moderate
	Moderate		P2 – High	P3 – Moderate	P4 – Low
	Low		P3 – Moderate	P4 – Low	P4 – Low

3.14. Service Level Agreement. Rackspace shall respond to security incidents and provide updates in accordance with the SLA in Appendix 1.

3.15. Service Reviews. Customers will be provided with Services review on a quarterly basis to assess the health of the Covered Environment configuration, the notification responsiveness, the Endpoint susceptibility, and event trends.

3.16. Root cause Analysis (RCA). Upon request, Rackspace will perform a root cause analysis for purposes of identifying the cause of an incident within the Covered Environment. When available, Rackspace can provide and interpret forensics information for activities discovered within the Covered Environment as part of the RCA process. If the cause of an incident is determined then, to the extent practicable, Rackspace shall perform mitigation to prevent recurrence, or if Rackspace is not enabled and authorized to perform the mitigation (i.e., a Customer Managed Endpoint), Rackspace will advise Customer accordingly. To qualify for the RCA service: (i) the incident must be ticketed; (ii) the incident must be a severity level of P2 or higher; and (iii) the incident cannot be the subject of a prior RCA.

3.17. RCA Disclaimers. Customer acknowledges that incidents are inherently complex, involving numerous variables, factors, and potential causes. As such, it may not always be possible to determine the precise cause of an incident. In some cases, identifying the ultimate cause may be impractical. Furthermore, even when a cause is identified, it may not be feasible to remediate all vulnerabilities or endpoints. Consequently, not all incidents can be fully mitigated or resolved. The RCA service is limited to no more than three RCAs within a single monthly billing cycle.

3.18. Remediation. In response to an incident notification, Rackspace Sovereign Secure service will provide the following remediation services:

(A) Guided Remediation. Rackspace will investigate to identify the affected Endpoint(s) and determine an appropriate response strategy and provide guidance to the Customer for response to Endpoint and malware events ("**Guided Remediation**"). Except as specified under section 3.18(C) (i.e., Active Remediation), Customer is responsible for executing the remediation and/or mitigation guidance provided by Rackspace.

(B) Automated Response. In accordance with industry practices, Rackspace will utilize automated tools to respond to known threats with predefined remediations, when such automated responses are available within the tooling ("**Automated Response**"). If an automated response is insufficient to return an Endpoint to a recovered state, Rackspace will provide either Guided Remediation or an Integrated Response, depending on the service level available to the Customer.

(C) Active Remediation. When the required remediation falls within the scope of the Customer's other separately contracted Rackspace Services, then Rackspace shall undertake the remediation for Endpoint and malware events ("**Active Remediation**"), provided however that Rackspace is authorized and enabled to perform the required configuration changes in the Covered Environment.

3.19. Custom and On-Demand Services. The following Services are not within the scope of Rackspace Sovereign Secure but may be available to Customer from Rackspace at additional cost under a separate Service Order.

(A) Additional Service Reviews. Service reviews more frequent than once per quarter.

(B) Custom Policies. For Customers seeking to deploy non-standard policies to fit preferences, the Rackspace professional services organization, upon request, may be able to accommodate more advanced or customized policies.

(C) Customer SIEM Integration. Upon Customer request, Rackspace can connect the Rackspace Sovereign Secure platform to Customer's SIEM or other security operations platforms, where supported. As reasonably determined by Rackspace, Rackspace shall work with Customer to ensure usability of the ingested data and information within the Customer's SIEM.

4. SOVEREIGN SECURE BRONZE SERVICES. Sovereign Secure Bronze, provided at no charge provides Customers with centralized log streaming to the Sovereign SIEM for forensic analysis during onboarding to the Rackspace Sovereign Cloud platform. **Automatic notification shall be limited solely to anti-virus alerts**, and logs are retained for 30 days. No other Services are included with Sovereign Secure Bronze and without limiting the generality of the foregoing, the following items are expressly excluded: (i) SIEM alerting will be not be enabled

as part of Sovereign Secure Bronze; (ii) SIEM tuning will not be enabled as part of the Bronze service; (iii) SOC alerting for security is not provided with Sovereign Secure Bronze (except for other than anti-virus alerts); and (iv) no SLAs are associated with Sovereign Secure Bronze.

5. CUSTOMER REQUIREMENTS AND RESPONSIBILITIES.

5.1. General Requirement. Customer shall provide Rackspace with all information required to setup, maintain, and manage the Covered Environment and with all required assistance, in a timely manner, which may include points of contact, authorizations and access credentials, configuration data and coordination of maintenance windows. Additionally, Customer will assist with validating the implementation, and Customer will provide permission to create test environments, if required. To any extent that Customer does not provide information or cooperation as required, (i) Rackspace is excused from its dependent obligations, (ii) Rackspace may invoice Customer to the extent of additional costs or expenses resulting from non-cooperation (e.g., platform costs, infrastructure and/or environment expenses), and (iii) if such delay continues for 90 days or longer, the Initial Term of Services shall commence and Rackspace will begin to charge the monthly Services Fee as described in section 8.

6. SERVICES LIMITATIONS AND COMPLIANCE.

6.1. Out of Scope. Rackspace will only provide the Services described in section 3 (with respect to Sovereign Secure Silver) and section 4 (with respect to Sovereign Secure Bronze). Services not detailed in those sections are not within scope of Sovereign Secure and are specifically excluded from performance obligations of Rackspace and its Representatives. Customer acknowledges that not all Customer Endpoints are compatible with and supported by the Services (e.g., legacy operating systems, platforms no longer receiving support from the manufacturer, etc.).

6.2. Remediation Limitations. Notwithstanding anything described in section 3.18(C) with respect to Active Remediation, Rackspace will not be obligated to conduct Active Remediation if Rackspace cannot reasonably access the Covered Environment, or if any required, pre-approved actions or if any required notifications and/or escalations prevent or unreasonably interfere with Rackspace's ability to conduct Active Remediation.

6.3. Compliance. While the Services can be used to assist Customer in complying with legal and regulatory compliance requirements, Customer acknowledges that Rackspace make no representation or warranty that the Services will meet Customer's legal or regulatory compliance needs or be sufficient to maintain Customer's compliance requirements. Additionally, Rackspace makes no representation or warranty that the Services shall be sufficient for, or capable of, completely mitigating the threats posed by malicious third parties. Customer acknowledges that no service can eliminate the inherent risks to confidentiality and security that result from internet connectivity.

6.4. Custom Configurations. For any customizations, Rackspace will not be able to support triage or malware response activities as described within the service description, unless previously agreed in writing by a Rackspace authorized representative. Additionally, to the extent Rackspace management or support obligations are impaired or affected by any such customization, then Rackspace will be relieved of its obligations and responsibilities for the Services to the extent impaired or affected.

7. CHANGES TO PRODUCT TERMS. Notwithstanding anything in the Agreement to the contrary, Rackspace may change these Product Terms at any time, effective immediately in response to: (i) changes to applicable law; (ii) changes made to any third party supplier product or services upon which these Services depend; (iii) operational changes to the Services which are generally effective to customers, or which are required (in Rackspace's reasonable determination) for the ongoing performance or proper functioning of the Services.

8. FEES, INVOICING AND PAYMENT.

8.1. Fees. Fees for Rackspace Sovereign Secure Silver are based upon the following Services components:

(A) Onboarding Fee. An initial one time, fixed Fee for deployment of the Services.

(B) Sovereign Secure Silver. The monthly Services Fees for Sovereign Secure Silver are based upon two metrics: (i) the number of Endpoints required to ingest data into the Services; and (ii) the events per second ("**EPS**"). Each chargeable device that ingests data into the platform is entitled to three EPS. This allocation is considered "at large," meaning the EPS can be distributed across the entire service rather than being restricted to individual Endpoints. For example, if Customer purchases 10 Endpoints, they are entitled to a total of 30 EPS, which can be utilized across the entire Covered Environment. If Customer's EPS consumption exceeds the entitlement, then Rackspace reserves the right to either: (i) increase the number of Endpoints on Custmer's Service Order (above those actually ordered), to increase the EPS entitlement; or (ii) remove Endpoints from the reporting and the Services so that Customer's EPS consumption remains within the entitlement. Rackspace will engage with Customer to mutually agree on the appropriate course of action. If a resolution is not otherwise achieved within 30 days of an exceeded EPS event, Customer shall be charged the full amount for the excess Endpoint consumption (at then-current rates), and Rackspace will increase the number of Endpoints on Customer's Service Order and any additional Endpoints will be co-termed to Customer's existing Service Order term.

(C) Custom Services and On-Demand Fees. Fees for custom and on-demand services as outlined in section 3.19.

8.2. Pricing. Pricing for all Services components will be in accordance with the then-current rates applicable to the Rackspace and third-party Services components, as indicated in Customer's Service Order. Subject to pricing increase as may be permitted by the Agreement, Customer pricing for initially ordered Endpoints shall remain in effect throughout the term, until expiration of the applicable Service Order; Endpoints added during the term will be priced, per the then-current Services pricing; and upon renewal, pricing for all Endpoints may be increased to the then-current Services rates.

8.3. Invoicing and Payment. Customer's onboarding fees (or other one-time Fees indicated in the Services Order) will be invoiced upon execution of the Services Order. The monthly Services Fee, and Fees for custom or on-demand Services will be invoiced on monthly recurring basis in arrears. Invoicing will begin when the Services are active and made accessible to Customer. All Fees are non-refundable and are payable in accordance with the terms of the Agreement.

9. TERM & TERMINATION.

9.1. Term; Renewal Term. The Initial Term of these Services shall be identified in the applicable Service Order, and thereafter these Services shall renew in accordance with the terms of the Agreement. Additional Endpoints added to Customer's Services, and any additional devices, will be co-termed to Customer's then active term (i.e., either an Initial Term, Renewal Term or Auto Renewal Term).

Appendix 1
Service Level Agreements

As referenced within these Product Terms, Sovereign Secure Services are supported by SLAs for: (i) Issue Response (non-security); and (ii) Incident Response & Update Interval, as further described herein.

1. ADDITIONAL DEFINITIONS.

"**Priority Level**" means the priority designation of an issue or incident, and each of the respective Priority Levels are more generally defined per the table below. Additionally, provided that alignment with these parameters and generally accepted best practices is maintained, specific conditions, circumstances, or contingencies applicable to the Covered Environment will be assigned Priority Levels as agreed between the parties during the Service transition phase.

Priority Level		Definition
1	**Critical**	• Severe disruption with potential to impact life, safety, security, environment, or business critical transactions. (ITILv4) • Business-critical system outage causing direct impact to Customers revenue or core business objectives.
2	**High**	• Service is interrupted, degraded or unusable with no acceptable alternative. (ITILv4) • Impact affects a moderate business function or the ability of a large group of End Users to work effectively. • Intermittent degradation of a critical business function which has the potential to impact Customers revenue or brand
3	**Moderate**	• Issue prevents the user from performing critical time sensitive functions. (ITILv4) • Production system impaired and moderate business impact with minimal impact to end users.
4	**Low**	• Issue prevents user from performing a portion of their duties. (ITILv4) • Issues and requests and minimal business impact.

2. ISSUE RESPONSE (Non-Security).

2.1. Performance Standards. For general technical support and for non-technical services requests (i.e., not requests with respect to security incidents) the performance standards for response times based upon priority levels is as indicated below. The Initial Response Times in this section 2.1 apply only to requests Customer makes via ticket or telephone. The times in this section 2.1 are response times, not resolution times; Rackspace does not guarantee resolution times.

Priority Level		Initial Response Time
1	**Critical**	15 minutes
2	**High**	30 minutes
3	**Moderate**	4 hours
4	**Low**	12 hours

2.2. Credit Remedy; Initial Response Time. If Rackspace fails to achieve at least 70% compliance with the indicated response time in the aggregate in any given month (and subject to a minimum of 20 or more ticketed

events per month), Customer is eligible to request a credit of US$250 per ticketed event, up to 50% of Customer's monthly recurring service fee in the applicable calendar month.

2.3. Credit Remedy; Resolution Time. If Rackspace fails to achieve at least 70% compliance with the indicated resolution time in the aggregate in any given month (and subject to a minimum of 20 or more ticket event per month), Customer is eligible to request a credit of US$250 per ticketed event, up to 50% of Customer's monthly recurring service fee in the applicable calendar month.

3. INCIDENT RESPONSE & UPDATE INTERVAL.

3.1. Performance Standards. The response times and update intervals for security incidents is based upon Priority Level as indicated in the table below. The Initial Response Times and Maximum Update Intervals stated in this section 3.1 apply only to requests Customer makes via ticket or telephone. The times in this section 3.1 are response and update times, not resolution times; Rackspace does not guarantee resolution times.

Priority Level		**Initial Response Time**	**Maximum Update Interval**
1	**Critical**	15 minutes	30 min
2	**High**	60 minutes	4 hrs
3	**Moderate**	8 hours	1 day
4	**Low**	24 hours	As required

3.2. Credit Remedy; Initial Response Time. If Rackspace fails to achieve at least 70% compliance with the indicated response time in the aggregate in any given month (and subject to a minimum of 20 or more ticketed events per month), Customer is eligible to request a credit of US$250 per ticketed event, up to 50% of Customer's monthly recurring service fee in the applicable calendar month.

3.3. Credit Remedy; Maximum Update Interval. If Rackspace fails to achieve at least 70% compliance with the indicated update interval time in the aggregate in any given month (and subject to a minimum of 20 or more ticketed events per month), Customer is eligible to request a credit of US$250 per ticketed event, up to 50% of Customer's monthly recurring service fee in the applicable calendar month.

4. SERVICE LEVEL CONDITIONS, EXCLUSIONS & TERMS. The foregoing performance standards and credit remedies and subject to the following conditions, exclusions, and terms:

4.1. Service Level Maintenance Exclusions. With respect to all indicated SLAs, Customer is not eligible for a credit remedy if an SLA failure results from Maintenance. "**Maintenance**" means:

(A) Rackspace Maintenance Windows. Modification or repairs to shared infrastructure (such as core routing or switching infrastructure) and fleet management activities (such as firmware updates for Customer's network appliances) that Rackspace has provided notice of at least 72 hours in advance and that occurs during off peak hours in the time zone where the data center is located;

(B) Scheduled Customer Maintenance. Maintenance of the Customer Configuration that Customer requests and that Rackspace schedules with Customer in advance (either on a case-by-case basis, or based on standing instructions), such as hardware or software upgrades, and including periods during which Customer sets or requests an Alert suppression on the Customer Configuration; and

(C) Emergency Maintenance. Critical unforeseen maintenance needed for the security or performance of Customer's Hosted System or Rackspace's network.

4.2. Technical Restraint. Rackspace will provide a resolution or mitigation plan and timeline only where the implementation of a resolution cannot be delivered within the defined resolution time due to technical limitation

or constraints. (e.g., insufficient, or inaccurate information provided by a third party, or inadequate back-ups that preclude effective or efficient system recovery or restoration). In this scenario, the incident is removed from performance measurement.

4.3. Global Exclusions. With respect to all indicated SLAs, Customer is not eligible to request a credit for a failure to meet an SLA which results from denial-of-service attacks, viruses, or malware, hacking attempts, or any other circumstances that are not reasonably within Rackspace's control. Customer is not eligible for a credit remedy if Customer is in breach of its obligations under the Agreement, including any payment obligations. Customer is not eligible for a credit during the on-boarding phase of the Services. To be eligible for a credit, Customer's use of the Services to which the applicable SLA applies must be adversely affected. If a single event results in Customer being eligible for multiple SLA credit remedies per these Product Terms and/or the Agreement, then only the SLA with the largest credit amount will apply. Credit remedies identified in specific currency amounts are awarded in the amount matching the currency on the Customer's invoice. Sections 2 and 3 state Customer's sole and exclusive remedy for Rackspace's failure to meet the SLA performance standards described in these Product Terms.

4.4. Credit Request Process. Customer shall request a credit in writing via a support ticket no later than 7 days following the relevant event. Rackspace shall contact Customer within 30 days to approve or reject the claim or to request more information. If the claim is approved, the credits will be applied to future invoices. Unused credits shall not be refunded. Credit determination will be based upon time periods as measured by the Rackspace ticket system. Response time for incidents will start with the ticket creation timestamp and will end at the timestamp of the first analyst action; the maximum update interval is measured from the timestamp of previous update in the ticket. If Rackspace opens the ticket on behalf of Customer during support requested via telephone, there may be delay in opening the ticket.

WAF & DDoS PROTECTION PRODUCT TERMS

In addition to any other terms and conditions of Customer's Agreement with Rackspace, these Product Terms shall apply when Customer purchases (or accesses) Sovereign WAF as a Service and/or Sovereign DDoS Protection as a Service as described herein, (individually, "**Sovereign WAF**" or "**WAFaaS**", and "**Sovereign DDoS**" or "**DDoSaaS**", and collectively, as used within these Product Terms, "**WAFaaS & DDoSaaS**" or the "**Services**").

1. ADDITIONAL DEFINED TERMS.

"**Cloudflare Solutions**" means the Cloudflare add-on features made available to Customer for purchase from Rackspace, as may be updated, and as currently located: https://www.Cloudflare.com/plans/, but specifically excluding Cloudflare's Content Delivery Network (CDN), DDoS Protection, Web Application Firewall (WAF), and Domain Name Services (DNS).

"**Cloudflare**" means Cloudflare, Inc., a Rackspace supplier and Representative located at 101 Townsend St., San Francisco, California 94107.

"**Cloudflare Terms**" means, collectively, as may be updated: (i) Cloudflare's Enterprise Subscription Terms of Service currently located at: https://www.Cloudflare.com/enterpriseterms/; (ii) Cloudflare's Security Policy currently located at: https://www.Cloudflare.com/security-policy/; (iii) Cloudflare's Privacy Policy currently located at: https://www.Cloudflare.com/en-gb/privacypolicy/; (iv) Cloudflare's service specific terms currently located at: https://www.Cloudflare.com/en-gb/service-specific-terms-overview/; and (v) Cloudflare's Trademark Use Terms currently located at: https://www.Cloudflare.com/en-gb/trademark/.**

"**Covered Environment**" means the Rackspace-managed, Hosted System and/or Customer Configuration identified in Customer's Service Order as within scope of the Services.

"**Implementation Manager**" mean the Rackspace role responsible for orchestrating the Services implementation as described in in section 3.1.

"**Managed Domain(s)"** means one or more domains (or a subdomain which is configured to have an administrative or configuration boundary separate from the parent or root level domain) within scope of the Services, as defined and agreed between Rackspace and Customer, which are either owned by Customer or supported by Customer on behalf of its End Customer.

"**Rackspace Sovereign Cloud**" or "**Sovereign Cloud**" means the computing environment provided with Rackspace UK Sovereign Services, as described in the applicable Product Terms, as may be updated, and presently located at: https://www.rackspace.com/information/legal/UK-sovereign-services.

2. OVERVIEW. Sovereign WAF and Sovereign DDoS provide web application security for customer Sovereign Cloud environment The Services consists of the provisioning and deployment of Web Application Firewall (WAF) and Distributed Denial of Service (DDoS) protection (with Customer option to add certain Cloudflare Solutions as described herein) . The Services include an Implementation Manager and Services are initiated via a kickoff meeting to guide the project and for configuration of firewall blocking, rate limiting, and managed rulesets. Sovereign WAF is priced on a per site basis; and Sovereign DDoS is priced per public IP address.

3. SERVICES AND DELIVERABLES.

3.1. Implementation Manager. The Services include assignment of any Implementation Manager to oversee the completion of the pre-requisite onboarding questionnaire, coordinate the scheduling of the kickoff meeting,

and serve as the primary liaison between the Customer and the implementation engineer. Rackspace, at its sole discretion and at any time, may replace an Implementation Manager named on the Service Order, or an Implementation Manager initially assigned to Customer.

3.2. Kickoff Meeting. The Services will include an initial kickoff meeting (not to exceed one hour) for the following purposes: (i) outlining the project and timelines; (ii) identify Customer's Services owner, key stakeholders and contributors, and the operations team; (iii) setup of applicable Services accounts for Customer and Rackspace; and (iv) review of the onboarding questionnaire and validation of assumptions consistent with the Customer obligations indicated in section 4. Additionally, an initial Long Range Planning (LRP) session will be held to define the working backlog and milestones, if any.

3.3. Scope of Services & Deliverables. As applicable to the respective Services (either the Sovereign WAF and/or the Sovereign DDoS), the Services consist of the provisioning of the Sovereign WAF and/or Sovereign DDoS for up to five Customer sites with the following deployment phases and deliverables:

(A) Onboarding. Rackspace will onboard the Customer's Services through either Rackspace's data center networks (or Cloudflare's global network, if Customer elects the Cloudflare Solutions), defining hostnames specific to the WAF platform. This process involves configuring the Customer's origin servers, establishing base content handling behaviors, and transitioning from staging to production environments. Support for Customer-initiated DNS cut-over is also provided.

(B) Based Protections. Base protections will be configured, including IP/Geo firewall blocking, rate limiting (if licensed), and DDoS protections. If Customer elects Cloudflare Solutions, these protections will be configured using Cloudflare's security features and rule sets.

(C) Rulesets. The Services will be enabled and configured with either the OWASP ModSecurity Core Rule Set (for Rackspace's existing platform) or Cloudflare's Managed Rulesets (if Customer elects Cloudflare Solutions), and with enhanced protection against web-based attacks for common technologies such as Drupal CMS, Adobe Flash, Joomla CMS, Magento CMS, PHP, WHMCS, and WordPress CMS.

(D) Soak Testing & Review. Following initial configuration, Rackspace will perform two weeks of soak testing during which the WAF configuration will be monitored under normal traffic conditions. Then, recommendations from the security engine will be reviewed, accepted, or denied, and blocking will be enabled. Next, a follow-up, one-week soak period will then be conducted, with a second recommendations review cycle to validate non-impact (i.e., the blocking of only malicious traffic without false positives or disruption to intended/legitimate traffic).

(E) Cloudflare Portal Access. Customers with Cloudflare Solutions may additionally be provided with limited access to the Cloudflare Solutions dashboard subject to the terms in section 4.4.

3.4. Handoff. A handoff meeting with participation from Customer Success management, the implementation engineer, and the Customer is held to transfer access to the Services, including enablement and authorization of Customer's credentialed users. If Customer has elected Cloudflare Solutions, this will include provision of appropriate Cloudflare dashboard access. As applicable, a summary of the work performed will be provided together with configuration information, and any additional technical information required by Customer to utilize and maintain the Services (i.e., as applicable, any major components such as DNS status, DoS protection, firewall, and WAF will be identified). CF services includes portal access …

4. CUSTOMER OBLIGATIONS.

4.1 General Requirements and System Access. Customer shall provide Rackspace with all information and access required to setup, maintain, and manage the Covered Environment in a timely manner, including: (i) access credentials, accounts, systems, and applications; (ii) technical documentation and configuration data; (iii) domain information for Managed Domains (including DNS records in BIND or other agreed format); (iv) points of contact and authorizations; (v) coordination of maintenance windows; and (vi) validation assistance and test environment

permissions as required. If Customer fails to provide required information or cooperation: (i) within three Business Days of request, Rackspace may suspend performance of the Services without affecting Customer's payment obligations; (ii) Rackspace is excused from dependent obligations and may invoice Customer for resulting costs (e.g., platform, infrastructure, or environment expenses); and (iii) if delays continue for 90 days or longer, the Initial Term commences, and monthly Services Fees begin per section 9.

4.1. Rackspace Configuration Requirements & Compatibility. The Services are only available for Customer Hosted Systems within Rackspace Sovereign Cloud. If Customer elects Cloudflare Solutions, the Services may also protect applications and systems hosted outside the Sovereign Cloud, subject to Customer's compliance with applicable data sovereignty requirements. Before completing the provision of the Services, Rackspace shall perform a final check of the Customer Configuration to determine compatibility with the Services and compliance with the Rackspace Configuration Requirements. Certain traffic types and hardware configurations are not compatible with the Services. Customer understands and agrees that if the Customer Configuration does not meet the Rackspace Configuration Requirements, Rackspace may cancel Customer's order and refund any unused fees previously remitted to Rackspace for the Services. IF CF - Data localization suite… for CF

4.2. Changes to IP Address(es). Customer shall notify Rackspace if Customer wishes to modify the IP addresses that are being protected by the Services.

4.3. Change to Customer Configuration. If, after implementation of the Services Customer makes changes to its Customer Configuration that are not supported by the Services (or which otherwise impact the functionality of the Services), then Rackspace shall advise Customer of Services' limitations resulting from such changes. Following such advice from Rackspace Customer may elect to continue the Services subject to such limitations, or Customer will have the option, for limited a period of 90 days, to elect discontinuation of the Services upon 90-days' notice.

4.4. Cloudflare Solutions Portal Access.

(A) Access Levels. Rackspace may grant Customer limited access to the Cloudflare Solutions dashboard subject to with either read-only or limited write permissions. No Super Admin or user management rights will be granted. As a condition for granting such access Rackspace requires Multi-Factor Authentication (MFA) for all users. SSO integration is available if Customer meets security prerequisites, as reasonably determined by Rackspace for the Covered Environment. Customer acknowledges that access is subject to immediate revocation if any such access compromises Rackspace's administrative rights.

(B) Customer Responsibilities. Customer accepts full responsibility for: (i) all configuration changes made through portal access; (ii) any resulting costs, overage fees, or performance issues; and (iii) compliance with Cloudflare Terms, as indicated in section 6.1. Customer shall promptly notify Rackspace when access is no longer required.

(C) Sovereign Onsite WAF Service Access. Rackspace may, by exception and at its sole discretion, grant Customer read-only access to Sovereign onsite WAF service management interfaces, and such access is limited to viewing configurations and logs only; and such access may be revoked at any time without notice. Customer acknowledge that such access is not a standard part of the Services and is subject to the terms in section 6.2.

5. SERVICES LIMITATIONS & EXCLUSIONS.

5.1. Out of Scope. Rackspace will only provide the Services described in section 3. Services not detailed in that section are not within scope of the Services and are specifically excluded from performance obligations of Rackspace and its Representatives (unless covered by an active Sovereign Secure (SOC / SIEM) contract). Customer acknowledges that not all Customer sites are compatible with and supported by the Services (e.g., legacy operating systems, platforms no longer receiving support from the manufacturer, etc.). Without limiting the generality of the scope limitation in this section 5.1, Customer expressly acknowledges that: (i) ongoing

management (i.e., monitoring, responses, additional configurations, alerts, etc.) is not within scope; and (ii) except when expressly granted by the Sovereign Services team in writing, the Services do not include access or visibility into native platform dashboard. Notwithstanding the foregoing, Cloudflare Solutions Customers may be granted limited access per section 3.3(E) and other sections of these Product Terms.

5.2. Cloudflare Solutions. If Customer elects to use Cloudflare Solutions, Customer acknowledges that: (i) Cloudflare operates a global anycast network and Customer Data may be processed in any of Cloudflare's global data centers; (ii) certain Cloudflare Solutions may not be available in all jurisdictions; and (iii) Customer is responsible for ensuring that it's use of Cloudflare Solutions complies with any data residency or localization requirements applicable to Customer. Rackspace will provide guidance on Cloudflare's available data localization options, but Customer retains ultimate responsibility for compliance with geographic restrictions.

5.3. Custom Configurations. For any customizations, Rackspace will not be able to support triage or malware response activities as described within the service description, unless previously agreed in writing by a Rackspace authorized representative. Additionally, to the extent Rackspace management or support obligations are impaired or affected by any such customization, then Rackspace will be relieved of its obligations and responsibilities for the Services to the extent impaired or affected. This limitation applies regardless of whether Customer uses Rackspace's existing platform or Cloudflare Solutions.

5.4. Feature Limitations, Insufficient Mitigation & Traffic Blocking. Customer understands and agrees that due to the complexity and sophistication of DDoS attacks, not all DDoS attacks will be effectively detected and/or mitigated within all Customer Configurations and that not all Services configurations will be adequate to address all DDoS attacks. If Customer believes that DDoS Protection is not satisfactorily detecting and/or mitigating against DDoS Attacks, then, upon Customer request, Rackspace will engage with Customer on a reasonable efforts basis to provide support, troubleshooting and/or Services reconfiguration. Customer understands and agrees that absolute protection against a DDoS attack may not be possible without interference with Customer's legitimate network traffic, and that Rackspace will seek to achieve an acceptable level of malicious traffic blocking without unreasonable interference with Customer's normal, intended network traffic. If, in Rackspace's sole judgment and discretion, the reconfiguration of Customer's Services as requested or required, is excessively complex or time consuming, then Rackspace may charge Customer its then-active professional rates for these Services. If Customer elects to use Cloudflare Solutions, Customer acknowledges that certain features available in Rackspace's existing platform may not have direct equivalents in Cloudflare Solutions, and vice versa.

5.5. Remediation Limitations. Notwithstanding anything described in section 3 or in the Appendix 1, Rackspace will not be obligated to provide a response if Rackspace cannot reasonably access the Covered Environment, or if any required, pre-approved actions or if any required notifications and/or escalations prevent or unreasonably interfere with Rackspace's ability to respond. If Customer elects Cloudflare Solutions, Rackspace's remediation capabilities may be further limited by the features and APIs available in the Cloudflare platform.

5.6. Mitigation Capacity. Rackspace does not set limits on mitigation capacity on a per-customer basis. The limits to Rackspace's mitigation capacity depend on the type and nature of attacks and varying limitations across overall network capacity, data center architecture and the particulars of the Customer Configuration. If Customer elects Cloudflare Solutions, mitigation capacity will be subject to Cloudflare's network capacity and the specific Cloudflare plan selected by Customer.

5.7. Traffic Blocking. If an attack impedes Rackspace's ability to operate the Rackspace network or negatively impacts other Rackspace customers, Rackspace may null route Customer's traffic, engage in upstream blocking, suspend access to the Customer Configuration, or take other measures as necessary to protect Rackspace's network and other customers (collectively "**Traffic Blocking**") without prior notice. If Rackspace has determined that Traffic Blocking is imminently necessary or if Rackspace has already initiated Traffic Blocking, then Rackspace shall notify Customer promptly and engage with Customer to consider measures, to the extent available and practicable, to re-establish attack mitigation and connectivity to the Customer Configuration. If Customer uses Cloudflare Solutions, Traffic Blocking may also be initiated by Cloudflare pursuant to the Cloudflare Terms.

5.8. Platform-Specific Limitations. If Customer uses Rackspace's existing platform, the Services are limited to protecting resources within the Rackspace Sovereign Cloud. If Customer elects Cloudflare Solutions: (i) Customer acknowledges that Cloudflare operates as a reverse proxy service and certain architectural differences may affect how protections are applied; (ii) Customer is responsible for ensuring that its use of Cloudflare Solutions complies with any applicable data sovereignty requirements; (iii) certain Cloudflare features may require additional licensing from Cloudflare; and (iv) Rackspace's ability to customize or modify Cloudflare's core security rules may be limited. * Cloudflare non-compliant with UK sovereignty requirements

6. COMPLIANCE.

6.1. Compliance with Cloudflare Terms. Customer access to and use of the Cloudflare Solutions is subject to the Cloudflare Terms (which will be effective without signature).

6.2. Sovereign Onsite WAF Service Access Compliance. For any Sovereign onsite WAF service access granted under section 4.4(C), Customer acknowledges and agrees that: (i) such access is solely for Customer's internal business purposes in connection with the Services; (ii) Customer shall not modify, reverse engineer, decompile, disassemble, or create derivative works from any Sovereign onsite WAF service software or interfaces; (iii) Customer shall not transfer, sublicense, or provide access to any third party; (iv) Customer shall not attempt to access any software code or functionality beyond the read-only interface provided; (v) such access does not constitute a transfer of software under Rackspace's supplier agreement; (vi) access is limited to viewing configurations, logs, and status information necessary for Customer's interaction with the Services only; (vii) Customer may not export software or modify configurations; and (viii) such access is provided "as-is" without any warranty from Rackspace or the appliable vendor. Customer's failure to comply with these restrictions shall constitute a material breach of these Product Terms.

6.3. Customer Compliance Requirements. Rackspace does not provide compliance certification for any portion of the Services. Rackspace makes no representation or warranty as to the compliance readiness of any portion of the Services. Customer understands and agrees that compliance readiness is a system wide endeavor, and the compliance readiness of the Services can fail if a single aspect of the environment is not compliant. Customer retains ultimate responsibility for meeting all regulatory requirements and compliance standards.

6.4. Cloudflare Solutions. As indicated in section 4.4, Customer is responsible for ensuring that it’s use of Cloudflare Solutions complies with any data residency or localization requirements applicable to Customer.

6.5. Resale Prohibited. Resale is prohibited except where Rackspace has allowed resale in writing. Except as expressly described in Appendix 1, Customer is prohibited from reselling these Services, in whole or in part, and may only utilize these Services for its own internal business purposes. Additionally, Customer is prohibited from selling, transferring, providing, or sublicensing Customer’s Rackspace credentials to any other party (except providing access to those agents and subcontractors performing work on Customer’s behalf). Customer is responsible for use of the Services by any third party to the same extent as if Customer were using the Services. To the extent that resale is permitted, Customer accepts full responsibility for all Services Fees generated by End Customer use of the Services, per terms applicable to resale as indicated in Appendix 1; all Services Fees are due and payable to Rackspace for End Customer’s use regardless of whether Customer receives payment from the End Customer.

7. CHANGES TO PRODUCT TERMS. Notwithstanding anything in the Agreement to the contrary, Rackspace may change these Product Terms at any time, effective immediately in response to: (i) changes to applicable law; (ii) changes made to any third party supplier product or services upon which these Services depend; (iii) operational changes to the Services which are generally effective to customers, or which are required (in Rackspace’s reasonable determination) for the ongoing performance or proper functioning of the Services.

8. SERVICE LEVEL AGREEMENT. Rackspace shall respond to security incidents and provide updates in accordance with the SLA in Appendix 1. SLAs apply to Rackspace's performance of the Services only and do not apply to any third-party platform performance, including Cloudflare's platform availability or performance.

9. FEES, INVOICING AND PAYMENT.

9.1. Fees. Sovereign WAF and Sovereign DDoS are based upon the following Services components:

(A) Onboarding Fee. An initial one time, fixed Fee for deployment of the Services.

(B) Monthly Services Fee. The monthly Services Fees for the Services are determined based on either the number of sites for Sovereign WAF, and/or the number of IP addresses for Sovereign DDoS, as stated in Customer's Service Order. During the term, For purposes of determining the number of sites, environments such as Prod, Test, Dev, QA, Stage, etc. are treated as separate sites. Number of Sites. Customer may add new sites to its Customer Environment (up to a total of five sites, for Sovereign WAF), and additional IP addresses (for Sovereign DDoS) in which case the Fees will be increased accordingly. Customer may also remove sites from its Covered Environment, in which case the Fees will be decreased accordingly, except that a Customer with a term commitment for a minimum number of sites may not reduce the number of sites during the term. For Customer with a term commitment, any increase or decrease in the number of sites, will be co-termed to the term of Customers initial Service Order.

(C) Custom Services and On-Demand Fees. Fees for custom and on-demand services as emerge from the Services or as otherwise agreed by the parties.

(D) Cloudflare Solutions. The minimum ordering term for Cloudflare Solutions is 12 months. If Customer elects Cloudflare Solutions, Customer shall pay applicable licensing fees as specified in the Service Order. Cloudflare Solutions fees are subject to change upon renewal and may include charges for bandwidth overages or additional features as set forth in the Cloudflare Terms.

9.2. Pricing. Pricing for all Services components will be in accordance with the then-current Services rates, as indicated in Customer's Service Order. Subject to pricing increase as may be permitted by the Agreement, Customer pricing for initially ordered sites and Services shall remain in effect throughout the term, until expiration of the applicable Service Order; sites added during the term will be priced, per the then-current Services pricing; and upon renewal, pricing for all sites and Services may be increased to the then-current Services rates. Cloudflare Solutions licensing fees may be subject to different pricing terms as specified in the Service Order.

9.3. Invoicing and Payment. Customer's onboarding fees (or other one-time Fees indicated in the Services Order) will be invoiced upon execution of the Services Order. The monthly Services Fee, and Fees for custom or on-demand Services will be invoiced on monthly recurring basis in arrears. Cloudflare Solutions licensing fees will be invoiced as specified in the Service Order. Invoicing will begin when the Services are active and made accessible to Customer. All Fees are non-refundable and are payable in accordance with the terms of the Agreement.

10. TERM & TERMINATION.

10.1. Term; Renewal Term. The Initial Term of these Services shall be identified in the applicable Service Order, and thereafter these Services shall renew in accordance with the terms of the Agreement. If Customer elects Cloudflare Solutions, the term shall be coterminous with the Services term unless otherwise specified in the Service Order.

10.2. Platform Changes. Customer may request to change from Rackspace's existing platform to Cloudflare Solutions (or vice versa) by providing 90 days' written notice. Such change will require a new Service Order and may incur additional onboarding fees. Platform changes are subject to Rackspace's approval and technical feasibility assessment.

10.3. Effect of Termination. Upon termination of the Services: (i) if Customer uses Rackspace's existing platform, standard termination procedures apply; (ii) if Customer uses Cloudflare Solutions, Customer acknowledges that Rackspace will coordinate with Customer to transition Cloudflare Solutions as appropriate,

but Customer remains responsible for any direct relationship with Cloudflare if Customer wishes to continue using Cloudflare services independently.

Appendix 1
Service Level Agreements

The Services are supported by SLAs for incident response & update interval, as further described herein. These SLAs apply to Rackspace's performance only and do not cover third-party platform availability or performance.

1. ADDITIONAL DEFINITIONS.

"**Priority Level**" means the priority designation of an issue or incident, and each of the respective Priority Levels are more generally defined per the table below. Additionally, provided that alignment with these parameters and generally accepted best practices is maintained, specific conditions, circumstances, or contingencies applicable to the Covered Environment will be assigned Priority Levels as agreed between the parties during the Service transition phase.

Priority Level		Definition
1	**Critical**	• Severe disruption with potential to impact life, safety, security, environment, or business critical transactions. (ITILv4) • Business-critical system outage causing direct impact to Customers revenue or core business objectives.
2	**High**	• Service is interrupted, degraded or unusable with no acceptable alternative. (ITILv4) • Impact affects a moderate business function or the ability of a large group of End Users to work effectively. • Intermittent degradation of a critical business function which has the potential to impact Customers revenue or brand
3	**Moderate**	• Issue prevents the user from performing critical time sensitive functions. (ITILv4) • Production system impaired and moderate business impact with minimal impact to end users.
4	**Low**	• Issue prevents user from performing a portion of their duties. (ITILv4) • Issues and requests and minimal business impact.

2. INCIDENT RESPONSE & UPDATE INTERVAL.

2.1. Performance Standards. The response times and update intervals for security incidents is based upon Priority Level as indicated in the table below. The Initial Response Times and Maximum Update Intervals stated in this section 2 apply only to requests Customer makes via ticket or telephone. The times in this section 2 are response and update times, not resolution times; Rackspace does not guarantee resolution times.

Priority Level		Initial Response Time	Maximum Update Interval
1	**Critical**	15 minutes	30 min
2	**High**	60 minutes	4 hrs
3	**Moderate**	8 hours	1 day
4	**Low**	24 hours	As required

2.2. Credit Remedy; Initial Response Time. If Rackspace fails to achieve at least 70% compliance with the indicated response time in the aggregate in any given month (and subject to a minimum of 20 or more ticketed events per month), Customer is eligible to request a credit of US$250 per ticketed event, up to 50% of Customer's monthly recurring service fee in the applicable calendar month.

2.3. Credit Remedy; Maximum Update Interval. If Rackspace fails to achieve at least 70% compliance with the indicated update interval time in the aggregate in any given month (and subject to a minimum of 20 or more ticketed events per month), Customer is eligible to request a credit of US$250 per ticketed event, up to 50% of Customer's monthly recurring service fee in the applicable calendar month.

3. SERVICE LEVEL CONDITIONS, EXCLUSIONS & TERMS. The foregoing performance standards and credit remedies and subject to the following conditions, exclusions, and terms:

3.1. Service Level Maintenance Exclusions. With respect to all indicated SLAs, Customer is not eligible for a credit remedy if an SLA failure results from Maintenance. "**Maintenance**" means:

(A) Rackspace Maintenance Windows. Modification or repairs to shared infrastructure (such as core routing or switching infrastructure) and fleet management activities (such as firmware updates for Customer's network appliances) that Rackspace has provided notice of at least 72 hours in advance and that occurs during off peak hours in the time zone where the data center is located;

(B) Scheduled Customer Maintenance. Maintenance of the Customer Configuration that Customer requests and that Rackspace schedules with Customer in advance (either on a case-by-case basis, or based on standing instructions), such as hardware or software upgrades, and including periods during which Customer sets or requests an Alert suppression on the Customer Configuration; and

(C) Emergency Maintenance. Critical unforeseen maintenance needed for the security or performance of Customer's Hosted System or Rackspace's network.

(D) Third-Party Platform Maintenance. If Customer elects Cloudflare Solutions, any maintenance performed by Cloudflare on its platform.

3.2. Technical Restraint. Rackspace will provide a resolution or mitigation plan and timeline only where the implementation of a resolution cannot be delivered within the defined resolution time due to technical limitation or constraints. (e.g., insufficient, or inaccurate information provided by a third party, or inadequate back-ups that preclude effective or efficient system recovery or restoration). In this scenario, the incident is removed from performance measurement. This includes limitations inherent in third-party platforms such as Cloudflare.

Global Exclusions. With respect to all indicated SLAs, Customer is not eligible to request a credit for a failure to meet an SLA which results from denial-of-service attacks, viruses, or malware, hacking attempts (including Cloudflare platform issues). Customer is not eligible to request a credit for issues caused by Customer changes, or any other circumstances that are not reasonably within Rackspace's control. Customer is not eligible for a credit remedy if Customer is in breach of its obligations under the Agreement, including any payment obligations. Customer is not eligible for a credit during the on-boarding phase of the Services. To be eligible for a credit, Customer's use of the Services to which the applicable SLA applies must be adversely affected. If a single event results in Customer being eligible for multiple SLA credit remedies per these Product Terms and/or the Agreement, then only the SLA with the largest credit amount will apply. Credit remedies identified in specific currency amounts are awarded in the amount matching the currency on the Customer's invoice. Section 2 states Customer's sole and exclusive remedy for Rackspace's failure to meet the SLA performance standards described in these Product Terms.

3.3. Credit Request Process. Customer shall request a credit in writing via a support ticket no later than 7 days following the relevant event. Rackspace shall contact Customer within 30 days to approve or reject the claim or to request more information. If the claim is approved, the credits will be applied to future invoices. Unused credits shall not be refunded. Credit determination will be based upon time periods as measured by the Rackspace ticket system. Response time for incidents will start with the ticket creation timestamp and will end at the timestamp of the first analyst action; the maximum update interval is measured from the timestamp of previous update in the ticket. If Rackspace opens the ticket on behalf of Customer during support requested via telephone, there may be delay in opening the ticket.