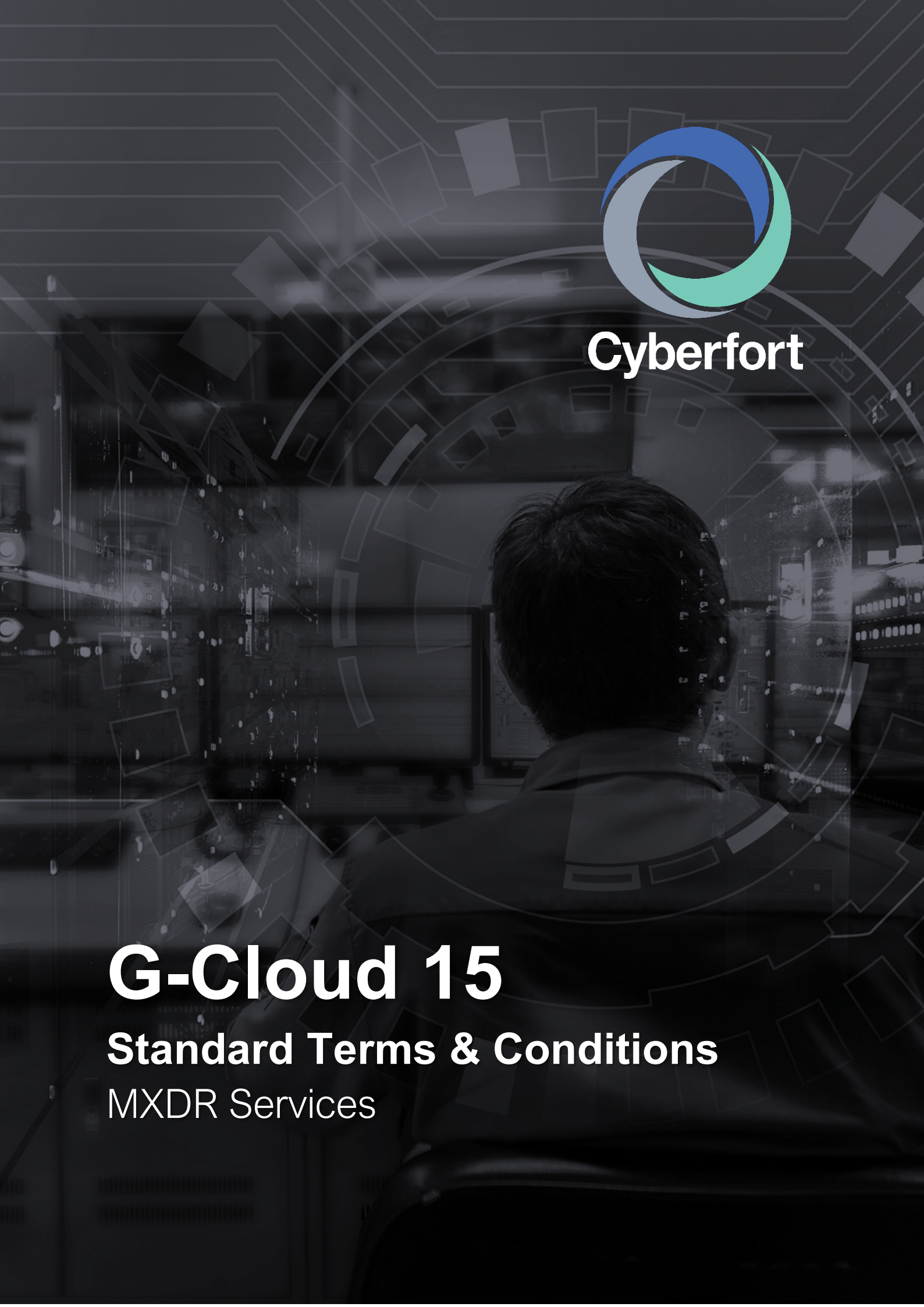

Cyberfort

G-Cloud 15

Standard Terms & Conditions

MXDR Services

1. Standard Terms & Conditions

The below Standard Terms and Conditions are applicable to the supply of the G-Cloud Framework and would form the Services to be supplied under the Call-Off Contract with the Customer/Buyer.

If you ultimately decide to purchase the Service(s) described with Cyberfort, then all terms and conditions will only be pursuant to a final and definitive written agreement between the Customer/Buyer and Cyberfort (including any amendments, if applicable).

For the avoidance of doubt, the final agreement will replace any other suggested terms and conditions.

Notwithstanding anything to the contrary, Cyberfort makes no representations, warranties, or covenants (including without limitation as to any products, services, service levels, third-party products or services or interoperability) separate from, in contravention of, or in addition to those contained in the final agreement, and any purported representation, warranty or covenant in this information document shall be of no force or effect.

Any information provided in below regarding the Service is for informational purposes only and is subject to change.

2. MXDR Services

1. Additional definitions

The definitions shall apply to these Terms and Conditions unless otherwise stated.

Customer/Buyer	means the individual(s) and/or organisation(s) that is ordering the Services;
Cyberfort	means Cyberfort Limited;
Applicable Law	all applicable laws, statutes, regulation and codes from time to time in force;
Consultant	means the individual(s) provided by Cyberfort for the performance of the Security Testing;
Contract	together, these Standard Terms and Conditions, the Order Form and its Schedules, the Framework Agreement and any other documents referred to in them;
Cyberfort Materials	all software programs (including the Software), applications, documents, processes, methods, know-how and data, including any modifications, enhancements and developments thereto, owned by or licensed to Cyberfort and used in the provision of the Service;
Data	the digital information provided by Customer/Buyer to Cyberfort through the use of the Software to be stored on Cyberfort servers as part of the Services;
Elastic Security Agent	means the agent deployed by the Customer/Buyer;
Order Form	means an order form agreed between the parties to request one or more of the Services;
MDR Service	means the Cyberfort Managed Detect and Respond (MDR) service as described in the Order Form;
Service	One or more of the Service(s) to be provided by Cyberfort to the Customer/Buyer pursuant to a Order Form;
Service Levels	the service levels applicable to each Service (if any) as set out in the Schedule to these Terms and Conditions as applicable or to the Order Form;

2. Cyberfort obligations

2.1 Cyberfort shall provide:

a) the Service with reasonable care and skill and materially in accordance with the applicable Order Form, including, where applicable, the Service Levels; and

b) such cooperation and information reasonably requested by the Customer/Buyer in respect of the Service.

2.2 In providing the Service, Cyberfort shall use reasonable endeavours to meet any performance dates specified in an Order Form but any such dates shall be estimates only and time for performance by Cyberfort shall not be of the essence of this Contract.

2.3 In providing the Service, Cyberfort shall comply with all Applicable Laws and regulations which apply to the provision of the Service and to the operation of Cyberfort's business.

2.4 Cyberfort shall use its reasonable endeavours to comply with any reasonable on-site security or health and safety policies made known to it by the Customer/Buyer when attending the Customer/Buyer's premises or using any Customer/Buyer Equipment.

2.5 Cyberfort shall have the right, without liability and without prejudice to Cyberfort's other rights (including termination), to immediately suspend, remove or disable access to or use of the Services if Cyberfort become aware of or have reasonable grounds to expect any abuse of such access and/or use (by the Customer/Buyer or any third party, for example through denial-of-service attacks, spamming or otherwise):

a) which interferes with the provision of the Service or any services provided by Cyberfort to third parties;

b) which would entitle Cyberfort to terminate this Contract; or

c) where Cyberfort are properly required to do so by Applicable Law, regulatory or governmental body.

The Customer/Buyer acknowledges and agree that Cyberfort have no obligation to monitor or actively seek facts or circumstances indicating any abuse or illegal activities.

2.6 Where possible Cyberfort will inform the Customer/Buyer of any steps taken in accordance with Clause 2.5 above as soon as legally and reasonably possible and may, but are not obliged to, advise the Customer/Buyer on actions that the Customer/Buyer should consider implementing to mitigate the risk of recurrence. The fact that Cyberfort do not take some or all of the steps set out in Clause 2.5 and / or provide any recommendations, does not waive or in any way affect Cyberfort's right to take such steps or invoke other rights that Cyberfort may have at any other time in response to the same or other events occurring.

2.7 Managed Detect & Response (MDR)

2.7.1 Cyberfort's MDR Service is an outsourced advanced security control service that will deliver enhanced defence intelligence capability and management of threats to protect Customer/Buyer data and assets from cyber-attacks.

2.7.2 Cyberfort's responsibilities in providing the Service will include:

2.7.2.1 provide dedicated engineering support to assist the Customer/Buyer with the deployment of the Elastic Security Agent;

2.7.2.2 ensure that all equipment connected to the Services by or on behalf of Customer/Buyer is technically compatible with the relevant Service(s) and any applicable specifications, and that Customer/Buyer's site and the equipment complies with and is used in accordance with any applicable legislation;

2.7.2.3 will have a default policy set on the Elastic Security Agents to auto-update when a new version or update is released by the vendor; and

2.7.2.4 ensure that the MDR Service systems and data are suitably backed up and secure. An up-to-date business continuity and disaster recovery plan is in place including technical recovery plans and this is regularly reviewed and tested. Cyberfort are not responsible for backing up Customer/Buyer equipment.

3. Customer/Buyer obligations

3.1 The Customer/Buyer shall:

a) co-operate with Cyberfort in all matters relating to the Service;

b) grant such access (whether remotely or otherwise) to the Customer/Buyer's staff, premises and data, and such office accommodation and other facilities, as is reasonably requested by Cyberfort for the purposes of performing its obligations under the Order Form;

c) provide in a timely manner such information as Cyberfort may reasonably request in relation to the Service, and ensure that such information is accurate in all material respects;

d) appoint a manager in respect of the Services to be performed, such person as identified in the Order Form. That person shall have authority to contractually bind the Customer/Buyer on all matters relating to the relevant Order Form (including by signing Change Orders);

e) obtain and maintain all necessary licences and consents and comply with all relevant legislation as required to enable Cyberfort to provide the Service, including in relation to the installation of the Cyberfort's Materials, the use of all Customer/Buyer Materials and the use of the Customer/Buyer's Equipment insofar as such licences, consents and legislation relate to the Customer/Buyer's business, premises, staff and equipment, in all cases before the date on which the Services under the applicable Order Form are to start;

f) Customer/Buyer shall ensure that Customer/Buyer Equipment, telecommunications, internet and other access lines shall be properly maintained and meet any minimum technical requirements specified by Cyberfort, and that all appropriate security precautions are taken with respect to Customer/Buyer systems and Data in order to receive the benefit of the Services; and

g) comply with all Applicable Laws and regulations applicable to the use and receipt of the Service and the operation of the Customer/Buyer's business.

3.2 Managed Detect & Response (MDR)

Customer/Buyer responsibilities in the provision of the Service will include:

3.2.1 ensure that suitably qualified and experienced operators are available to discharge the Customer/Buyer's responsibilities in connection with the Service including but not limited to replying to and executing such steps as are reasonably necessary to address a request by Cyberfort;

3.2.2 obtain appropriate consent from its ISP (Internet Service Provider) and any other relevant third-party supplier of the System for the MDR Service to be carried out and, when requested by Cyberfort, to provide evidence of such consent and to notify relevant employees that the MDR Service has been scheduled and that they may be monitored;

3.2.3 where the MDR Service is to take place on the Customer/Buyer's premises, the Customer/Buyer shall ensure that suitable accommodation and working conditions are provided for the Consultant which shall include network access and, where necessary, access to data centres, server rooms and/or switch rooms;

3.2.4 co-operate with Cyberfort and to provide it promptly with such information about its Systems, network, premises, equipment, data structures, protocols, software, hardware and firmware as are reasonably required by Cyberfort; and

3.2.5 obtain Customer/Buyer consents, for itself and on behalf of all group companies, to Cyberfort performing the MDR Service and that it has procured, where necessary, the consent of all its (and its group companies) employees, agents and sub-contractors that Cyberfort shall be permitted to carry out the MDR Service. Cyberfort will be carrying out the MDR Service in the belief that it has all appropriate consents, permits and permissions from the Customer/Buyer and its group companies (and their employees, agent and sub-contractors).

3.2.6 responsible for deployment of the Elastic Security Agent to in scope assets and timeframe as defined within the Order Form;

3.2.7 where Customer/Buyer chooses to opt-out of auto-updates, the Customer/Buyer will be fully responsible for updating the Elastic Security Agent within 5 (five) days (including weekends and public holidays) of being notified of the release. In the event that the Elastic Security Agent has not been updated by the Customer/Buyer, then Cyberfort will not continue to monitor the Customer/Buyer estate as they cannot guarantee the security posture;

3.2.8 advise Cyberfort in advance of any software or hardware changes it intends to implement that will or may affect a maintained system (including but not limited to changes to its network, systems, policies, etc.) regardless of how these are implemented (including by way of upgrade, policy change etc.). Failure to do so may relieve Cyberfort of its liabilities, warranties and/or obligations under this Contract;

3.2.9 prior to the start of the MDR Service commencing, provide Cyberfort with a complete and accurate list of assets which will fall under the scope of monitoring, the document will be referenced as the "customer asset register" and will form part of this Contract. This document will identify all Customer/Buyer assets including but not limited to IP address, hostnames, locations, operating system, applications and system/service criticality etc. Any and all updates to the asset estate including the commissioning or decommissioning of assets must be communicated to Cyberfort at the Customer/Buyer earliest opportunity or alternatively on an agreed scheduled basis;

3.2.10 shall not, except in the circumstances required to be permitted by applicable law, alter, rearrange, disconnect, remove, reverse engineer, repair or attempt to repair or tamper with Cyberfort Service (including any Cyberfort equipment) or cause, or allow, a third party to carry out these activities, without Cyberfort's prior written consent;

3.2.11 is solely responsible for selecting, supplying and maintaining its own facilities and equipment, unless outsourced to Cyberfort by purchasing an available service;

3.2.12 accepts that any circuit shifts and/or service changes required from time to time and requested by the Customer/Buyer shall, when the tail is in contract with Cyberfort, be at Cyberfort' sole discretion.

Customer/Buyer accepts liability for costs associated with circuit shifts during the first twelve (12) months of the relevant sales order form and/or services schedule.

4. Third Party Usage

4.1 Except as set forth in this service description, the Customer/Buyer may use the services only on infrastructure and assets owned by and registered to the Customer/Buyer, or for which the Customer/Buyer otherwise has the full right, power, and authority to consent to have the services.

4.2 The Customer/Buyer may not rent, lease, or loan the Cyberfort MDR Service, or any part thereof, or permit third parties to benefit from the use or functionality of the Service via timesharing, service bureau arrangements or otherwise.

4.3 In the event that endpoint agents are identified by Cyberfort as being installed on assets which are not owned, managed, and/or hosted by the Customer/Buyer then Cyberfort reserves the right to charge additional fees and/or cease monitoring the environment until the Customer/Buyer has rectified the issue. Cyberfort will not be held responsible for any related security incidents during this period.

5. Service Description

5.1 Email Reporting

5.1.1 Cyberfort will report on all alerts generated by the Security Information and Event Monitoring (SIEM) platform against agreed Service Level's. Alert details including any Customer/Buyer remediation activities will be sent via email to the designated Customer/Buyer contacts (or using the Customer/Buyer agreed escalation process). Alerts will typically contain the following information:

- Summary of Alert Discovered
- Affected Assets
- Details of the Alert
- Remediation Actions / Activities

5.2 Dashboard Reporting

5.2.1 The Service will provide the Customer/Buyer with two dashboards for their internal use as follows:

5.2.1.1 "Management Dashboard" will provide Senior Management with oversight of operational activities (including but not limited to); the number of assets being monitored, the number of alerts generated, number of critical, high, medium and low tickets that are open/in progress;

5.2.1.2 "Technical Dashboard" which will provide technical and operational teams with a granular view of alerts generated. The alerts will be defined by priority and severity, assets being monitored and the health of these devices including uptime. Drilldown capability will be supported providing the ability to interrogate alert details.

5.3 Service Support

5.3.1 A Service Desk is provided to deliver standardized management and tracking of incidents and reporting;

5.3.2 All calls to the Service Desk will be recorded using a call logging system and issued a unique tracking code. The team aims to resolve each reported incident in the shortest time possible. Service Targets are highlighted in Service Level Agreement (SLA) documentation;

5.3.3 This Service Desk is available during normal business hours; 09:00 to 17:30 Monday to Friday.

5.4 Service Change Requests

5.4.1 All requests for service changes will be recorded using a call logging system and issued a unique tracking code. The team aims to resolve each service change request in the shortest time possible. Service targets are highlighted in SLA documentation.

5.4.2 All requests for changes to the MDR SOC Service should be emailed to the Change Team, via the Service Desk.

5.5 Service Expansion and Adds, Moves and Changes

5.4.3 Cyberfort will adjust the service to meet Customer/Buyer business requirements subject to agreed Service Levels and commercial terms. We aim to process most service changes in line with the service change request process above, however service changes requiring step changes to the operating model will be delivered to negotiated timeframes.

5.6 Platform Maintenance & Software Release Management

5.6.1 Cyberfort MDR Service platform maintenance will be scheduled to be non-service affecting wherever possible. Should maintenance be required which will impact service delivery the Customer/Buyer will be notified by email of the time, work required and duration.

5.6.2 Cyberfort may upon five (5) working days' notice or, in an emergency (as determined by Cyberfort), as much notice as is reasonably practical under the circumstances, perform scheduled or emergency maintenance (including temporary suspension of Service where Cyberfort considers this necessary) to maintain or modify the network, network terminating equipment or the services and/or to prevent or resolve Incidents. Service suspensions for the purposes of scheduled or emergency network modification, or preventative maintenance, will not be counted as outage time for purposes of any SLA.

5.6.3 The Maintenance Window is on Monday to Friday (inclusive) each week. Where maintenance will result in degradation of Service, Cyberfort shall use reasonable endeavors to conduct such maintenance between 20:00-08:00 Hours (UK time). Where maintenance will cause an interruption to services, Cyberfort shall use reasonable endeavors to conduct such maintenance between 22:00-06:00 Hours (UK time).

5.6.4 It may be necessary from time to time for Cyberfort to schedule downtime for software updates or network enhancements. Unless stated otherwise in the individual Service Schedules, Cyberfort will use reasonable endeavors to give the Customer/Buyer a minimum of five (5) working days' advance notice of such events, and to schedule such events to cause minimum impact to the customer. For the avoidance of doubt, the Customer/Buyer acknowledges and agrees that it may not be practical to give such notice where downtime is necessary to deal with incidents occurring in connection with the service.

5.6.5 It may be necessary from time to time for Cyberfort to carry out emergency maintenance to the network to maintain appropriate levels of service quality, to resolve Incidents, or where there is a risk to the operation of the Service. For such events, the Customer/Buyer acknowledges and agrees that it may not be practical for Cyberfort to provide the Customer/Buyer with advanced notification.

5.6.6 At the beginning of December in each year Cyberfort will announce dates of the Network freeze. The Network Freeze is to allow for reduced engineering staff across the organizations themselves and those that support them. The direct effect is that orders for new services or changes to existing ones are effectively suspended for a period of time during December and January. This does not include scheduled or emergency maintenance. Support services continue during this period along with any necessary triage work, although workarounds will be employed rather than any changes to core infrastructure as much as possible.

5.7 Escalations

5.7.1 The first point of contact for all Customer/Buyer incidents or change requests should be the Service Desk via email or telephone quoting any reference code supplied. Should it be necessary for a Customer/Buyer to escalate incidents, service requests or any other service affecting issue, these may be made in accordance