As referred to in Clause 1.3 of the MSA, these Service Specific Terms set out the terms and conditions which apply specifically to the Cyber Security Services to be provided pursuant to an Order Form.

Unless otherwise defined in Annex A of these Service Specific Terms, all capitalised terms shall have the meanings set out in the MSA.

1. CYBER SECURITY SERVICES

1.1 Cyber Security Services will be delivered and be billed according to the Agreement including the Billing Guide, and as described in the relevant Order Form and Service Description. However, by default (in the absence of more specific provisions):

(a) services that involve the monitoring of assets will be Ready for Service immediately preceding the Supplier SOC has accepted the service into live operations.

(b) Professional Services will be delivered on terms that include (without limitation) the Professional Services SST and be billable as professional services according to the Billing Guide.

1.2 MSP Software is used by Supplier in the performance of the Cyber Security Services, and the use and provision of such MSP Software shall be governed by Section 6 of these Service Specific Terms.

1.3 Supplier reserves the right to:

(a) modify or replace (including hardware or software) any part of the Supplier's System, its network, system configurations or routing configuration; or

(b) modify or replace (including hardware or software) any Supplier Equipment used to deliver any Service,

provided that such changes have no material adverse impact on the core features and functionality of the Cyber Security Services. If such changes will have a material adverse effect, Supplier shall propose a change in accordance with the Change Control Procedure.

1.4 Supplier has the right to use any technical information Client provides to Supplier for any reasonable business purpose during and after the Service Term (including without limitation, for product support, improvement and development). Client acknowledges that the MSP Software includes monitoring capability that sends anonymous statistics about performance, device utilisation and network size remotely to Supplier. Save to the extent required for the effective performance of the Cyber Security Services, Supplier will not use such technical information in a form that could in any way identify Client.

2. SUPPLIER RESPONSIBILITIES

2.1 Supplier shall:

(a) provide the Cyber Security Services as set out in the Order Form;

(b) use commercially reasonable endeavours to follow the instructions of Client; and

(c) provide Client with all reasonably necessary co-operation in relation to the Cyber Security Services.

3. CLIENT RESPONSIBILITIES

3.1 Client shall:

(a) be responsible for obtaining and maintaining all Client Equipment and network connections necessary to access and use the Cyber Security Services, and for paying any applicable third party fees and charges incurred to access and use the Cyber Security Services;

(b) inform and keep Supplier updated regarding any of the critical information associated with any Cyber Security Incident;

(c) gather all relevant information prior to requesting assistance in respect of any faults or defects, including a detailed description of the fault or defect, the procedures required to replicate the issue, and any additional information which may help in the diagnosis of the fault or defect (e.g. network configuration details);

(d) provide Supplier with access to Client System via a secure broadband link operating at the industry accepted bandwidth for the purposes of remote diagnostics should such capability be required;

(e) ensure that Supplier is able to access the systems needed to provide remote support, including but not limited to remote desktop access or screen sharing system. Supplier can provide screen sharing capabilities via Microsoft Teams (or similar) but it is Client's responsibility to ensure that this works in their configuration or to provide another option. For the avoidance of doubt, remote access to the systems will take the form of a secure connection to the Client Equipment. The exact method of connectivity will be agreed but can take the form of a secure internet-based connection as required by Client's security guidelines;

(f) permit Supplier to install (i) the initial version of the MSP Software required to provide the Cyber Security Services, and (ii) where specifically stated in an Order Form, new releases or new versions of the MSP Software, and Client shall provide a reasonable level of assistance in implementation and testing;

(g) provide Supplier with reasonable advance notice of any intention to change applicable Client Equipment or Client Operating Environment or data-feeds which could affect Supplier's provision of the Cyber Security Services;

(h) procure as required any permission or services of third parties (including the providers of Client's internet access and other data communication services) for the purposes of ensuring that the Supplier can deploy Supplier Equipment, or MSP Software and perform the Services and allow Supplier, at Client's expense and with Client's prior

approval to make reasonable service requests of those third parties for cooperation and interconnectivity rights; and

(i) not jeopardise other services provided by Supplier to the Client. In the event of any such incident, Supplier will work with Client to assess and remedy the situation as quickly as possible, but Supplier shall not be liable to Client for any delay or failure in the provision of the Cyber Security Service or any other affected service, or for any other losses suffered by Client as a result of Client's failure to comply with this Clause 3.1(i). The Parties shall discuss and agree appropriate action (including the possibility of suspending the Cyber Security Services);

(j) provide the Supplier reasonable assistance in the performance of the Cyber Security Services, including, but not limited to, providing all technical and licence information that the Supplier requires for performing the Cyber Security Services, and access to Client Systems that Supplier must configure and manage as part of the Cyber Security Services;

(k) accept the baseline standards of configurations required by Supplier to enable the provision of the Cyber Security Services;

(l) provide accurate and up-to-date information, including name, email, landline, and mobile numbers (if applicable) for all Client's authorised points of contact;

(m) maintain the Monitored Assets and the environment in which the SIEM solution is located to a software and hardware version level supported by the relevant thidthird-party vendor or manufacturer;

(n) inform the Supplier of Client's internal changes that can reasonably be expected to affect the Cyber Security Services or the Supplier's ability to deliver the Cyber Security Services, including changes in identities, software versions and locations of Monitored Assets;

(o) have the minimum licence requirement to enable Supplier to deliver the Cyber Security Services, as advised from Supplier in writing from time to time;

3.2 Client shall not provide the Cyber Security Services to third parties without the prior written consent of Supplier. Client shall remain responsible for the use of the Cyber Security Services under its control, including any use by third parties that Client has authorised to use the Cyber Security Services.

3.3 Client acknowledges and agrees that, except as expressly provided in this Service Specific Terms, Client assumes sole responsibility for:

(a) results obtained from the use of the MSP Software and or the Cyber Security Services, as applicable and the Documents by Client, and for conclusions drawn from such use;

(b) all problems, conditions, delays, delivery failures (including any of those concerning transfer of data) and all other loss or damage arising from or relating to Client's or its agents' or contractors' (including any existing service provider's) network connections, telecommunications links or facilities, including the internet and acknowledges that the

Cyber Security Services and the Deliverables may be subject to limitations, delays and other problems inherent in the use of such connections, links or facilities.

4. OUT OF SCOPE; SERVICE EXCLUSIONS

4.1 Unless expressly stated in the Order Form, the following are out of scope under the Cyber Security Services:

(a) any other services not covered in the Agreement;

(b) training in use of any upgrades, updates or new releases to the MSP Software; and

(c) any legal advice, expert testimony or litigation support services of any kind or any services involving the collection of physical evidence, chain of custody collection of evidence for criminal or civil litigation purposes, or for admission in court, or providing evidence lockers or 'chain of custody' collection of evidence.

4.2 Supplier will have no responsibility or liability for:

(a) any equipment or other items that are not specifically included for such support outlined in the relevant Order Form;

(b) MSP Software that is no longer supported by the licensor;

(c) defects or repairs to, or the supply of any consumable items;

(d) faults or errors in MSP Software or the Client System (and in particular any customer facing component) resulting from:

(i) changes to the MSP Software except for changes implemented by, on behalf of or with the prior approval of Supplier;

(ii) failure to use MSP Software in accordance with the EULA or Supplier's instructions for use; or

(iii) faults in the hardware or any equipment on which the MSP Software is used, unless such equipment was supplied by Supplier (and then such support shall be limited to the relevant third-party manufacturer's warranty).

4.3 Supplier does not and cannot control the flow of data to or from its network and other portions of the internet. Such flow depends in large part on the performance of internet services provided or controlled by third parties. At times, actions or omissions of such third parties can impair or disrupt connections to the internet (or parts of it). Whilst Supplier will use commercially reasonable efforts to take all actions it deems appropriate to remedy and avoid such events, Supplier cannot guarantee that such events will not occur. Accordingly, Supplier disclaims any and all liability resulting from or related to such events and Client agrees to take such backups and provide such redundant systems as are prudent in the circumstances.

4.4 Supplier shall be under no obligation to provide the Cyber Security Services to Client in the following circumstances:

(a) unauthorised use of the MSP Software by Client or use otherwise than in accordance with the AgreeementAgreement; and

(b) where providing support for the Cyber Security Services to Client would have been unnecessary if Client had implemented update(s) and upgrade(s) supplied or offered to Client pursuant to the call for technical support.

5. CLIENT CONSENTS AND AUTHORISATIONS

5.1 Client authorises Supplier to carry out the following acts as necessary for the performance of the Cyber Security Services:

(a) Access any Client System;

(b) circumvent or overcome technological or physical measures which have been implemented to protect against unauthorised access to any Client System, as well as use or provide technology to achieve any such circumvention;

(c) intercept telecommunications and electronic communications;

(d) to the extent required to comply with Law, share information or take such actions with respect to any Client System required by law enforcement authorities or regulatory authorities. In such cases Supplier will use reasonable endeavours to the notify Client in advance, where it is permitted by such law enforcement and/or regulatory authorities to do so;

(e) retain for its business purposes any indicators of security compromise, malware or anomalies (including Client‘s Confidential Information or Client Content embedded in the same) found as part of, or related to the performance of the Cyber Security Services (“Vulnerabilities”); and

(f) anonymise and aggregate all data relating to Vulnerabilities to develop, provide and improve Supplier products and services.

5.2 Client acknowledges that the Cyber Security Services are being performed solely for the purposes of assessing and enhancing the effectiveness of Client’s security, and that Supplier is performing the Cyber Security Services at Client’s direction and has no intention of committing any breach of civil or criminal law.

5.3 Supplier shall use reasonable endeavours to carry out the Cyber Security Services in a manner which causes no impact or disruption to any Client System, however Client acknowledges that there is an inherent risk that the Cyber Security Services could result in operational or performance degradation, breach of Client’s internal policies or industry standards, or otherwise impair any Client System. Notwithstanding any other provisions in the Agreement, Supplier will not be liable to Client or its employees or third parties for such damage, breach or impairment arising out of provision or receipt of the Cyber Security Services.

5.4 Client represents, warrants and agrees that it has and will maintain all permissions, consents, licences, rights or authorizations necessary for Supplier to carry out the acts authorised in Section 5.1 in its performance of the Cyber Security Services.

5.5 Client shall defend, indemnify and hold Supplier harmless from and against all losses (including any actions, claims, costs, damages, expenses, fines, liabilities, penalties and sanctions, amounts paid in settlement, out-of-pocket expenses and interest) together with all reasonable legal expenses that Supplier incurs as a result of any action, claim, demand, proceeding, filing, objection or complaint from a third party or relevant authority arising in relation to the provision of the Cyber Security Services by Supplier (unless caused by Supplier's breach of its obligations).

6. MSP SOFTWARE

6.1 Any MSP Software supplied by Supplier is owned by the relevant licensor and not by Supplier. In no circumstances shall title to any MSP Software or any patents, copyrights, trade secrets and other worldwide proprietary and intellectual property rights in or related thereto pass to Client, which shall remain the exclusive property of the licensors.

6.2 Client agrees to be bound by and comply with the terms of the relevant end user licence agreement for any MSP Software (the "**EULA**"), which may be found at: (i) www.6dg.co.uk/terms, (ii) the relevant licensor's website, or (ii) which may be provided to Client as part of the Cyber Security Services. The EULA shall exclusively and independently govern the licensing and use of the MSP Software.

6.3 Supplier may at any time, with Client's prior written approval, incorporate licence management software into elements of the Cyber Security Services for the purposes of ensuring that software licence rights are not exceeded in respect of any MSP Software installed on Client's servers. Any costs relating to the incorporation of the licence management software shall be at Client's sole cost and expense.

6.4 Client shall promptly notify Supplier in writing upon discovery of any (i) non-compliance with the EULA, (ii) unauthorised use of the MSP Software, or (iii) infringement of the licensor's rights in the MSP Software.

6.5 The Parties agree that any failure to comply with the terms of this Section 6 shall be deemed a material breach of the Agreement for which injunctive and other equitable relief may be sought and Client shall indemnify and keep indemnified, defend and hold harmless Supplier from any associated claims, damages or liabilities and shall pay, at Supplier's current rates, any costs and expenses incurred by Supplier in respect of any breach of this Section 6 by Client.

6.6 Unless specifically stated in an Order Form, the Cyber Security Services shall not include new releases or new versions of any MSP Software. Where the Cyber Security Services specifically include the installation of new releases / new versions of the MSP Software, Supplier may upload such new releases and new versions in the event it receives the relevant patches or updates directly from the licensor. Supplier shall also use its reasonable discretion in deciding which patches and updates to install. Unless stated otherwise in an Order Form, Supplier will provide patches and updates only for industry standard environment Third Party Software licensed to Client, as outlined in the relevant Service Description and not for bespoke or business-specific software. Supplier shall use its reasonable endeavours to check MSP Software releases and versions are in working order and virus-checked prior to installation in the Client's System. Without limiting the generality of the limits in liability in the MSA, Supplier

shall not be liable for any damage or loss caused to the Client's System or business as a result of a fault, error, virus or other failure in the MSP Software.

7. PCI SSC DISCLOSURE REQUIREMENTS.

7.1 This Section applies only where the Cyber Security Services being provided by Supplier are in connection with a PCI DSS security assessment and Client authorises Supplier to release, directly to the PCI SSC, without any additional consent, approval or permission of Client:

(a) any ROC and related results generated in connection with Supplier's annual on-site PCI data security assessment, including but not necessarily limited to, working papers and other notes, and

(b) any and all additional agreements or other materials necessary to enable Supplier to comply with the disclosure compliance requirements mandated by the PCI SSC for all QSAs.

8. CHECK SECURITY TESTING

8.1 This Section applies only where CHECK Security Testing is to be performed. Where CHECK Security Testing is performed, Supplier will seek authorisation from CESG prior to commencement of the CHECK Security Testing. Client authorises Supplier to release, directly to the NCSC CHECK Scheme review panel, without any additional consent, approval or permission of Client:

(a) any Test Report and related results generated in line with the requirements of the Government Security Classification Policy, including but not necessarily limited to, working papers and other notes, and

(b) any and all additional agreements or other materials necessary to enable Supplier to comply with the Government Security Classification Policy requirements mandated by CESG under the NCSC CHECK Scheme.

9. EXIT PLAN

9.1 The Parties shall mutually agree and document an Exit Plan setting out the activities and timing of the steps required to successfully transition the Cyber Security Services to an Incoming Party. Supplier shall continue to provide the Cyber Security Services in the Exit Plan for a maximum period of ninety (90) days following termination or expiry of the Agreement.

9.2 Pursuant to the Exit Plan:

(a) Supplier shall provide to the Incoming Party reasonable cooperation, assistance and Professional Services (together the "**Transition Services**") in transitioning the expired or terminated Cyber Security Services upon Client agreeing to pay the Fees in respect of the said Professional Services at Supplier's then current rates of charge plus any reasonable additional costs and expenses incurred by Supplier that are related to the provision of the Transition Services during the Exit Plan.

(b) Fees for any Cyber Security Services still being provided shall continue to be levied in accordance with the relevant Order Form until such time as the Parties agree that the Cyber Security Services have been transitioned to the Incoming Party or (if applicable) to Client. Fees for Cyber Security Services will be reduced gradually for (and in direct accordance with) a gradual transition and reduction of Cyber Security Services.

(c) Client shall remain fully responsible and liable for the activities of the Incoming Party.

10. DEFINITIONS

10.1 Unless defined in this Clause 10, words and expressions used in the Cyber Security Service Specific Terms shall have the meanings given to them in the Master Services Agreement.

"CESG"	means the Communications-Electronics Security Group, a group within HMG;
"CHECK Security Testing"	means Security Testing to be carried out under the terms of the NCSC CHECK Scheme (as agreed between the Parties), by a NCSC approved company, employing penetration testing personnel qualified to assess HMG and other public sector bodies;
"Client Content"	means any software, content, materials, data and information supplied by Client, including but not limited to any Personal Data (if applicable);
"Client Equipment"	means equipment owned by Client or its suppliers, used in the provision of the Services to Client;
“Client System”	means all the equipment, hardware and software owned or operated by the Client in connection with its use of the Services, (including computer systems; servers; technology infrastructure; telecommunications or electronic communications systems and associated communications, assets and devices) and any data comprised within it (including settings and configurations, employee and business data, identification, authentication and credential data, IPR), and the premises in which it is located;
"Cyber Security Incident"	means an Event that triggers either one or more regulatory regime correlation directives or built in SIEM correlation directives, thereby creating an alarm within the SOC that is subsequently identified by the SOC as an organised attack;
"Cyber Security Services"	mean the specific cyber security services to be provided by Supplier to Client under an Agreement as set out and more fully described in the relevant Order Form;
"Deliverable"	means all Documents, products and materials developed by the Supplier or its agents, subcontractors, consultants and employees in relation to the Cyber Security Services in any form, including computer programs, data, reports and specifications (including drafts);

"Document"	means, in addition to any document in writing, any drawing, map, plan, diagram, design, picture or other image, tape, disk or other device or record embodying information in any form;
“Endpoint”	Means a user operated device;
"Event"	means a security event notification sent by a Monitored Asset that has been ingested by the USM;
"Exit Plan"	means the plan to be agreed between the Parties detailing the Transition Services;
“False Positive Rate”	refers to situations where the SIEM mistakenly identifies a benign action or event as a threat or risk;
“Incident Management System” or “IMS”	means the SOC system used to manage incidents, problems;
"Incoming Party"	means a replacement supplier appointed by the Client;
"Logger"	means a logger which can either be remote or installed on the Management Server and which securely archives raw event log data for forensic investigations and compliance mandates;
“Managed Service Operations Document” or “MSOD”	means the document which captures the Client’s contact and account details used by the SOC during the life of the service.
"Management Server"	means the centralised management system, aggregating and correlating the information gathered by the Sensors and provides a single point of reference to the Supplier for its monitoring, management, reporting and administration functions;
"Monitored Assets"	means the Client’s Hardware and software systems that are monitored by the Supplier as part of a Service;
"MSP Software"	means the software (including related documentation and any future updates provided by the Supplier or the relevant third-party manufacturer) that is used by the Supplier in the performance of the Cyber Security Services or that is provided by the Supplier for use by the Client as part of a managed Service for which title to the software license remains with the

	Supplier or the relevant third-party manufacturer and does not transfer to the Client (as opposed to software that is purchased by the Client as “Equipment”);
"National Cyber Security Centre" or **"NCSC"**	means the information security arm of GCHQ and the National Technical Authority for Information Assurance within the UK;
"NCSC CHECK Scheme"	means a special partnership between NCSC and industry that permits IT health check services to be provided by private sector companies to HMG in line with HMG policy;
“Organisational Artefact”	Means the brand, technology, and people within the Client’s organisation;
"Payment Card Industry Data Security Standard" or **"PCI DSS"**	means a proprietary information security standard for organisations that handle branded credit cards from the major card schemes (including but not limited to Visa, MasterCard, American Express, Discover and JCB) mandated by the card brands and administered by the PCI SCC;
"Payment Card Industry Security Standards Council LLC" or **"PCI SSC"**	means an organisation formed by card vendors to manage and administer the PCI DSS;
"Professional Services"	means consultancy services to be provided by the Cyber Security and Compliance group of the Supplier as more particularly described in the relevant Service Description and/or Order Form;
"Qualified Security Assessor" or **"QSA"**	means organisations that have been qualified by the PCI SSC to have their employees assess compliance to the PCI DSS standard;
"Report on Compliance" or **"ROC"**	means a comprehensive summary of assessment activities and information collected during the data security assessment undertaken by a QSA;
"Security Incident and Event Monitoring" or **"SIEM"**	means a service which provides (i) monitoring of security events generated by server and network infrastructure, attempts to identify correlations between those events, provides notification of events and incidents based on defined policies, provides structured reporting of events, and includes provisions for the storage of event and incident data;

"Security Operations Centre" or **"SOC" or "Cyber SOC" or "CSOC"**	means the combined staff and function provided by the Supplier at one or more locations by which security monitoring and management is performed on behalf of the Client by the Supplier pursuant to the relevant SoW;
"Security Testing"	means the process of carrying out security testing of the Client's System;
"Sensors"	means the security modules (that can either be remote from or installed on the Management Server) that perform asset discovery, vulnerability assessment, threat detection via the Network Intrusion Detection Service and behavioural monitoring (Netflow Analysis) and send related data to the Management Server;
"Supplier Equipment"	means equipment owned by Supplier or its suppliers, used in the provision of the Services to Client;
"Supplier's System"	means all the equipment, hardware and software used by Supplier or its suppliers, used in the provision of Services to Client (including computer systems; servers; technology infrastructure; telecommunications or electronic communications systems and associated communications, assets and devices) and any data comprised within it (including settings and configurations, employee and business data, identification, authentication and credential data, IPR), and the premises in which it is located;
"Test Report"	means the report produced by the Supplier detailing the results of the Security Testing;
"Third Party Software"	means any code or software programs written or provided by third parties which are used by the Client during the provision of the Services;
"Transition Services"	has the meaning in Clause 9.2(a);
"Unified Security Management Device" or **"USM"**	means the combination of the Management Server, the Sensors and the Logger from which all local policy configuration, event ingestion and correlation occurs in the performance of the Cyber Security Services.