CyberCare Security Services

Introduction

The terms defined below shall have the meanings applied to them wherever they occur in the relevant Cloud Services Schedule under a SOW and under these terms ("**CyberCare Specific Terms**"), including any sections, references, schedules and annexes:

Interpretation & Definitions

1. The terms defined below shall have the meanings applied to them wherever they occur in the relevant CyberCare Security Services Schedule under a SOW and under these CyberCare Security Services Specific Terms, including any sections, references, schedules and annexes:

CHECK:	a security and penetration testing provider certified by the National Cyber Security Centre to conduct sensitive HM Government and Critical National Infrastructure network testing;
Client System:	the systems and networks which the Client requires to be security tested pursuant to the Agreement;
CyberCare Security Services:	the security services provided by Codestone as described in a SOW;
Partner:	the security operations centre services partner identified in the CyberCare Security Service Schedule in a SOW;
Security Breach:	a Security Impact that has resulted in unauthorised access to data, applications, services, networks and/or devices by bypassing their underlying security mechanisms;
Security Event:	a change in the everyday operations of a network or information technology service, which indicates that a security policy may have been violated or a security safeguard may have failed;
Security Impact:	a situation where an adverse impact has resulted from a Security Event;
Security Services Minimum Period:	means the minimum period specified in a Security Services Schedule;
Security Services Renewal Period:	means the renewal period specified in a Security Services Schedule;
Security Services Start Date:	means the start date specified in a Security Services Schedule;
Security Testing:	the process of carrying out security testing of the Client's System;
Test Report:	the report produced by Codestone detailing the results of the Security Testing.

CyberCare Security Services Specific Terms and Conditions

1. CyberCare Security Services

1.1 The Client agrees and accepts that, neither Codestone or its Partner gives any warranty or representation that, it can prevent a Security Event and/or Security Breach, and that in relation to the elements of Codestone's system:

(a) the Client controls or can control, the Client has sole liability for protecting those elements against a Security Event and/or Security Breach; and

(b) Codestone or its Partner controls or can control, Codestone or its Partner (as applicable) has sole liability for protecting those elements against a Security Event and/or Security Breach.

1.2 The Client must take reasonable measures to ensure it does not jeopardise services supplied to third parties on the same shared access infrastructure as notified to the Client by Codestone in writing. This includes informing Codestone promptly in the case of a Security Event and/or Security Breach. In the event of any Security Event and/or Security Breach, Codestone or its Partner (as the case may be) will work with the Client to alleviate the situation as quickly as possible but shall have no liability or responsibility for any liability incurred by the Client as a result of any Security Event and/or Security Breach unless such liability is incurred as a result of any negligent act or omission on the part of Codestone or its Partner (as applicable). The Parties shall discuss and agree appropriate action. For the avoidance of doubt, neither Codestone or its Partner shall be liable under this paragraph to the extent that it has advised and reported to the Client on a vulnerability, issue, account, action or service exposure that has led to a Security Event and/or Security Breach, and the Client has failed to take appropriate actions, or change security policies or procedures that have been reasonably recommended by Codestone or its Partner.

1.3 The Client shall ensure that all systems, software, and equipment used by the Client in connection with the CyberCare Security Services provided under the Agreement shall be maintained in accordance with good industry practice and further agrees to promptly implement any updates or security improvements recommended by Codestone or its Partner (as the case may be) to maintain such compliance promptly and, in any event within twenty (20) days or, in respect of critical updates, within forty eight (48) hours of such notification.

3.4 The Client acknowledges that certain conditions outside of Codestone or its Partner's control may adversely impact the ability of Codestone or its Partner (as the case may be) to perform functions of the CyberCare Security Services. Examples of such conditions are listed below:

(a) failure of Client hardware, software or operating system;

(b) partial or full failure of Partner Products or other third party services;

(c) network connectivity issues between local system components and Codestone or its Partner's platform;

(d) network connectivity issues between local system components and its third party's servers.

3.5 Codestone shall be under no obligation to provide the CyberCare Security Services to the Client in the following circumstances (unless specified under the SOW):

(a) unauthorised use of the CyberCare Security Services by the Client or use otherwise than in accordance with these CyberCare Specific Terms;
(b) the Client fails to complete recommended endpoint changes and/or updates documented by Codestone or its Partner (as applicable) within twenty (20) days of receipt of the recommendations in writing;
(c) the Client fails to remove disabled or compromised resources, endpoints, user accounts or update security policies to correspond with Codestone's or its Partner's reasonable recommendations within twenty (20) days of receipt of the recommendations in writing.

4. Responsibilities of Client

4.1 The Client shall, where appropriate:

(a) allow Codestone or its Partner (as the case may be) access to the Microsoft Connectors (or custom connectors) to enable Codestone or its Partner (as applicable) to undertake testing on the connector functions where applicable;
(b) provide Codestone or its Partner (as applicable) with a list of all required cloud services and endpoints that need to be protected by the CyberCare Security Services;
(c) provide appropriate hardware interface, software and access authorisation to enable remote diagnosis, should such capability be required;
(d) provide all information and make available all resources as reasonably requested by Codestone or its Partner (as applicable) in the execution of its obligations under the Agreement, save that the Client shall not be obligated to provide any additional resources or information beyond what is reasonably necessary for Codestone or its Partner (as applicable) to perform its obligations under the Agreement;
(e) permit Codestone or its Partner (as the case may be) to install the current version of software required to provide the CyberCare Security Services from time to time when upgrades or fixes occur and to provide a reasonable level of assistance in implementation and testing;
(f) provide Codestone or its Partner (as applicable) at least three (3) Business Days' notice in advance of any intention or move to change when applicable Client-side equipment or Client's operating environment or data-feeds that will directly impact the CyberCare Security Services. If such notice has not been received on time, Codestone or its Partner (as applicable) will have to make additional effort to return the Client's systems to an acceptable state for continued support, and will charge accordingly at its then standard charging rate;
(g) review and agree to pre-engagement checklists and action plans provided by Codestone, acknowledging their importance in the effective implementation of the CyberCare Security Services;
(h) deploying the supported endpoint agent(s) on the licensed volume, ensuring that Codestone or its Partner (as applicable) have sufficient visibility into the Client's platform;
(i) ensure the availability of sufficient network bandwidth required for the Security Service to be performed effectively;
(j) promptly notify Codestone of any changes related to cloud applications, endpoints, or any other modifications in the Client's IT environment that may impact the CyberCare Security Services; and

(k) accept all updates and upgrades to Codestone or its Partner's platform and the endpoint agent necessary for the proper functioning and security of the Security Service.

4.2 In the event that the Client is in material breach of any material obligation (including payment of the applicable fees) under the Agreement relating to the CyberCare Security Services then Codestone shall provide written notice of such breach, specifying in detail the nature of the breach and providing twenty (20) days' notice to remedy such breach if capable of remedy. If the Client fails to remedy such breach, Codestone shall be entitled to terminate or suspend the CyberCare Security Services without prejudice to any pre-existing rights and obligations of either Party. Codestone shall have no liability or responsibility should the CyberCare Security Services fail to comply with the SOW and/or Service Level Arrangements as a direct result of the Client (including without limitation any of its employees, subcontractors or any of its staff) being in material breach of a material term of these CyberCare Specific Terms.

4.3 In the event that the Client has experienced any form of Security Event and/or Security Breach, data exfiltration or data breach within the previous twelve (12) months of the Security Services Start Date, and this includes a Client or a previous service provider of the Client, the Client will remain liable for all costs and subsequent issues and liabilities resulting from any and all previous events. Codestone will not be liable for data exfiltration as a direct result of Client user credentials, personal details, personal information or data previously exfiltrated.

4.4 In the event that the Client is responsible and at fault for sharing user details, security credentials or user actions in engaging in phishing, quishing engagements, actions that lead to malware installation links being processed by user actions or not protecting credentials with best practice multi factor authentication, Codestone shall have no liability under the Agreement and will not indemnify the Client against any such losses.

4.5 In the event that the Client has experienced any form of Security Event and/or Security Breach, data exfiltration of data breach within the previous twelve (12) months of the Security Services Start Date, it remains the Client's responsibility to ensure additional dark web monitoring has been activated to protect the Client from the dissemination of harvested or stolen information. Codestone shall have no responsibility or liability resulting from any losses or claims under the Agreement and will not indemnify the Client against any such losses. No indemnity shall be provided by Codestone for the actions and previous incidents or breaches that may have occurred prior to the Security Services Start Date.

5. Support

5.1 The Client will be entitled to receive support according to the features and benefits provided under the applicable offering described in the SOW, subject to the terms and conditions of the applicable Service Level Arrangement (SLA).

5.2 The service commitment under the SLA does not apply to any unavailability, suspension, performance issue or termination of the Security Service caused by factors outside of Codestone or its Partner's reasonable control, including any Force Majeure events or internet access or related problems beyond the demarcation point of the Security Service that result from any actions or inactions of the Client or any third party, that result from Client equipment, software, or other technology and/or third party equipment, software, or other technology (other than third-party equipment within Codestone or the Partner's direct control), or arising from the suspension or termination of Client right to use the Security Service.

6. Exclusions, limitations of liabilities, warranties and indemnities

6.1 Codestone or its Partner (as the case may be) reserves the right to take any action that it reasonably perceives necessary to protect the Client's System even though this may impact on the Client's business activities. Codestone or its Partner (as applicable) will make reasonable endeavours to inform the Client by telephone or email in advance of such action, but such action will not be dependent on such notification having been given or acknowledged.

6.2 The Client accepts that where the CyberCare Security Services include protection against Security Events and/or Security Breaches (including reviews of the Client's cyber security resilience or readiness) or protection of data, there are circumstances outside of the control of Codestone or its Partner where such CyberCare Security Services will fail and that this cannot be predicted by Codestone or its Partner or prevented through delivery of the CyberCare Security Services. Codestone or its Partner will, however, make all reasonable efforts to prevent such failures. To the extent permitted by law, Codestone shall not be liable for any losses incurred as a result of a security or data loss incident unless such losses are as a direct result of any negligent act or omission on the part of Codestone or its Partner or caused by Codestone or its Partner's failure to adhere to good industry practice in relation to security standards.

6.3 The Client acknowledges and agrees that, except as expressly provided in the Agreement, the Client assumes sole responsibility for:

(a) 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 the 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 CyberCare Security Services may be subject to limitations, delays and other problems inherent in the use of such connections, links or facilities; and

(b) loss or damage arising from or relating to any Relief Event.

6.4 THE CYBERCARE SECURITY SERVICES AND ANY PARTNER PRODUCTS ARE PROVIDED "AS IS" AND "AS AVAILABLE". CODESTONE MAKES NO WARRANTIES, EXPRESS OR IMPLIED, WITH RESPECT TO THE CYBERCARE SECURITY SERVICES OR PARTNERS' PRODUCTS' FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. CODESTONE MAKES NO WARRANTY THAT THE CYBERCARE SECURITY SERVICES AND/OR PARTNER PRODUCTS WILL MEET THE CLIENT'S REQUIREMENTS, BE UNINTERRUPTED, TIMELY, SECURE OR ERROR-FREE, THAT DEFECTS WILL BE CORRECTED, OR THAT THE CYBERCARE SECURITY SERVICES AND/OR PARTNER PRODUCTS ARE FREE OF BUGS OR REPRESENTS THE FULL FUNCTIONALITY, ACCURACY, RELIABILITY OF THE MATERIALS OR AS TO RESULTS OR THE ACCURACY OF ANY INFORMATION OBTAINED BY CODESTONE THROUGH THE CYBERCARE SECURITY SERVICES AND/OR PARTNER PRODUCTS.

7. Term and Termination

7.1 The CyberCare Security Services unless terminated earlier in accordance with the terms of the Agreement:

a) will commence from the Security Services Start Date and continue for the Security Services Minimum Period; and

b) at the end of the Security Services Minimum Period, the CyberCare Security Services shall automatically continue for successive periods of the Security Services Renewal Period, unless written notice of termination of the CyberCare Security Services is given by the either Party at least 90 days' in advance of the end of the Security Services Minimum Period or the end of any subsequent Security Services Renewal Period.

7.2 In the event of termination of the Agreement between Codestone and its Partner, any then-current Client accounts may be transitioned by Codestone from its Partner to another Security Services Partner.

8. C.E.S.G (The Communications-Electronics Security Group)

8.1 This paragraph 8 applies only where Security Testing is to be performed under the CHECK Scheme. Where Security Testing is performed under the CHECK Scheme, Codestone or its Partner (as the case may be) will seek authorisation from CESG prior to commencement of testing. The Client authorises Codestone or its Partner (as applicable) to release, directly to the CESG CHECK Scheme review panel, without any additional consent, approval or permission of the 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 Codestone or its Partner (as applicable) to comply with the Government Security Classification Policy requirements mandated by CESG under the CHECK Scheme.

9. Non dealing

9.1 To protect the legitimate business interests of Codestone, the Client covenants with Codestone that during the term of the Agreement and for a period of twelve (12) months following its termination or expiry (howsoever caused), it shall not (except with the prior written consent of Codestone), directly or indirectly:

(a) have any business dealings with, solicit, approach, negotiate with or enter into any agreement or other arrangement for the supply of goods or services with any Partner introduced, disclosed or otherwise made known to the Client by Codestone in connection with this Agreement, where the purpose or effect of such action is to circumvent Codestone and/or to obtain goods or services directly from such Partner;

(b) the Client further undertakes not to take any action which would have the effect of causing, enabling, or assisting a Partner to deal directly with the Client in a manner that bypasses or undermines the commercial relationship between the Client and Codestone.