Services Agreement

Service-Specific Terms

(incorporated into the Services Agreement Order Form and incorporating the Services Agreement Standard Terms, any Annex and any Order Form Services Addendum, all together the "Services Agreement")

Alphabetical Order

Supplier will provide Customer the following Service(s) as set forth on the Order Form:

1. **SaaS Platform Services**

The following services are available under the Supplier's SaaS platform. The specific services to be provided to Customer shall be those expressly set out in the applicable Order Form. Each service plays a part in protecting Customer's business from new and existing threats and, as a whole, the platform provides continuous visibility of Customer's security profile.

A. **Asset Profile**

Supplier will provide access to Customer to define its digital assets profile which assists in defining the attack surface and allows Supplier to automatically align threats to Customer's unique attack surface. Customer will add assets to ensure the correct threat intelligence feeds align to Customer‘s environment.

B. **Breach Monitoring**

Supplier will provide an automated monitoring solution performing surface web, deep web and dark web scans 24 hours a day for Customer's designated business data which includes Supplier's comprehensive source feeds -- IRC chatrooms, bin sites, data dumps, social sources and dark web sites, to detect sensitive data efficiently.

C. **Cyber Health Check**

Supplier will provide access to an online self-assessment tool that enables Customer to assess its current cyber security and information security posture by answering a series of questions based on modules covering a range of best practice cyber/information security controls, following completion of which Customer will receive an online report of its current status using a RAG (red, amber, green) indication which can be downloaded, and any threats identified will be automatically fed into the platofroms Threat Dashboard. For each successfully passed question module, Customer may download a pass certificate. Customer may choose which modules to take and can re-take any of the assessment modules at any time.

D. Endpoint Protection

Supplier will provide Endpoint Protection software and the SaaS platform to manage the endpoints. Supplier will also provide staff to manage, tune and support the platform. The following are included:

Windows – FileScan; ContentControl; UserControl; Application Backlisting; DataProtection; TrafficScan; AntiPhishing Firewall; BehavioralScan; MailServers (Exchange - only servers); DeviceControl; AntiExploit.

Mac – FileScan; Update Server; and Content Control with TrafficScan + Antiphishing

Linux – FileScan; and Update Server

Customer will install the software to secure endpoints and/or entry points on Customer's end-user devices to prevent file-based malware and detect and block malicious activity through automated vulnerability scanning.

E. Microsoft Office 365 Monitoring

Supplier will provide access to the automated Microsoft 365 Monitoring feature which will automatically create threats, escalating the highest risks to Customer and provide remediation advice. Customer will provide support and necessary secure access to Customer's MS Office 365 account with privileges for the Supplier to ingest data and alert on threats identified.

F. Panic Button

Supplier will provide a 24x7x365 emergency help button which allows Customer to raise potential security incidents with our trained, experienced team. Supplier provides fast-tracked preliminary incident response advice for all types of security events and cyber incidents including, but not limited to, suspected data breaches, ransomware attacks, insider threat, suspicious network activity and known vulnerability exposure. This service is intended to triage potential security incidents and provide practical advice for resolution, but does not include any remediation work from the Supplier.

G. Phishing Simulator

Supplier will provide access to the Phishing Simulator feature, which enables Customer to send safe phishing emails to test Customer staff's vigilance and identify any weaknesses in their security knowledge. Customer will use the platform to schedule and select the appropriate campaign per team, track results and take remediation steps following the outcome of the test. Customer will setup whitelisting of Supplier IP addresses and email domains as defined in Supplier provided help guides

H. Security Information and Event Management (SIEM)

Supplier will provide a SaaS based centralised log management to aggregate all log data in a single location and into a common format. Supplier will store log data for 12 months in an archive and provide 90 days of logs for immediate searching. Customer will install with support of Supplier the relevant software and virtual hardware to support the delivery of the service.

I. Security Support

Provision of a Supplier helpline, including audio and/or messaging, that offers first level response, general guidance and assistance to Customer, within 24 hours of a logged service request (excluding where the response due time falls within a weekend or national holiday), for cyber security questions Supplier deems to be common and frequently asked.

J. Threat Dashboard

Supplier will provide functionality in a single interface that displays threats across all the services provided. Threats are automatically populated by each feature, such as live threat intelligence tailored to Customer. Once threats have been populated, the platform provides powerful features to allow Customer to manage each threat and allocate threats to specific individuals for remediation. The platform will assign risk levels and allow the businesses to drill down into specific threat information and understand the business impact. Customer will action threats and perform remediations as identified by the platform or will take action to accept risk or acknowledge threats as false positives.

K. Threat Intelligence

Supplier will provide Customer a customised list of cyber threats, continually updated by experts based on the latest intelligence from commercial, opensource and custom-built feeds. Customer will define assets to ensure the correct intelligence is supplied relevant to Customer's environment.

L. Threat Recon

Supplier will provide access to Threat Recon which presents the attack surface of Customer's business to highlight risks. Threat Recon will automatically perform predefined tests that are used by attackers to test the exposure of the business. These checks include sub-domain detection, port scanning of top 20 ports, network information gathering, SSL validation, potential risk based on site popularity, email spoofing protection checks, block list lookup, security best practices assessment and other checks as offered by Supplier. Customer will provide all relevant internet facing web domains as the scope for the checks.

M. Training Videos & Exams

Supplier will provide a range of standard training courses covering varied cyber security, information security and compliance topics. These are delivered through a range of videos and associated exams which, along with built in reporting, allow Customer to track adoption.

N. Vulnerability Scanning

Supplier will provide a platform to allow Customer to run automated Vulnerability Scans of the most common ports with the option to customise to Customer's requirements, to assess systems or applications for known security flaws and weaknesses. Supplier will provide threats that can be managed, allocated, assigned and risks accepted in addition to actionable remediation advice. The service will allow Customer to identify assets that are prone to attacks. Customer will define the scope of the automated scans and take measures to patch or remediate the threats as provided by Supplier's automated process.

2. Consultancy Services

Supplier will remotely provide Customer advice and support covering information security topics, including, without limitation, frameworks such as ISO 27001, NIST, CIS, ISO22301 and General Data Protection Regulation (GDPR) data protection. Where specified, Supplier will assist Customer to work toward improvement of its business performance in terms of operations, management, structure and/or strategy regarding cyber security and/or GDPR compliance. On-site visits may be arranged with Customer in exceptional circumstances.

A. Cyber Security Assessment

Supplier will provide an experienced Information Security Consultant to assess the current level of information/cyber security in Customer's organisation. This will be based on the NIST CSF and ISO 27001/27002 controls and the output will be a report detailing the level of compliance against each of the requirements along with recommendations on how to achieve compliance.

B. Data Privacy Advisor (DPA)

Supplier will provide Customer access to up to 2 hours per month of remote support for queries and questions relating to GDPR and data privacy matters. Customers can contact the DPA service via a centralised mailbox initially and then queries can be dealt with via email, phone or video conferencing.

C. GDPR Audit

Supplier will provide an experienced GDPR consultant to audit the current level of compliance to GDPR. The output of the audit will be a report that will outline any non-

conformities. During the audit, which will be conducted remotely, Customer will need to provide access to key staff, documentation and evidence to support the audit.

D. GDPR Gap Analysis

Supplier will provide an experienced GDPR consultant to undertake a gap analysis against the requirements of GDPR. The output of the gap analysis will be a report detailing the current level of compliance to each of the requirements along with a document review (which will include a maximum of 20 GDPR related policies, procedures or documents) with recommendations and an action plan outlining what needs to be done to achieve compliance. During the gap analysis, which will be conducted via a series of online interviews with key stakeholders, Customer will be required to provide documents, e.g., policies and procedures that are currently in place for assessment.

E. GDPR Implementation

Supplier will provide an experienced GDPR consultant to deliver the GDPR implementation project. The service, which will be delivered remotely, will include preparation of all required documentation along with advice and support on how to ensure current processes are compliant. Customer will be required to play an active part in the implementation through interviews and workshops.

F. ISO 27001 Gap Analysis

Supplier will provide an experienced ISO 27001 consultant to undertake a Gap Analysis against, as appropriate, the version of the ISO 27001 standard ISO requested by Customer in accordance with the agreed scope. The output of the gap analysis will be a report detailing the current level of compliance to each of the requirements of ISO 27001 with recommendations on what needs to be done to achieve compliance. During the Gap Analysis, which will be conducted via a series of online interviews with key stakeholders, Customer will be required to provide documents, e.g., policies and procedures that are currently in place for assessment.

G. ISO 27001 Implementation

Supplier will provide an experienced ISO 27001 lead implementer to deliver an ISO 27001 implementation project to enable Customer's readiness for certification by an external UKAS accredited certification body. The implementation service, which will be delivered remotely, will include training of all staff on the Information Security Management System the consultant is implementing and preparation of all required documentation. Customer will be required to play an active part in the implementation through interviews and workshops.

H. ISO 27001 Internal Audit

Supplier will provide an experienced ISO 27001 auditor to conduct an internal audit against the agreed requirements and scope of the Information Security Management System. The output of the internal audit will be a report, written in accordance with the requirements of the ISO 27001 standard that will outline any non-conformities and opportunities for improvement. During the audit, which will be conducted remotely, Customer will need to provide access to key staff, documentation and evidence to support the audit.

I. Managed Phishing Campaigns

Supplier will perform tailored Phishing simulations (campaigns) to test Customer staff's vigilance and identify any weaknesses in their security knowledge. Supplier will provide a report documenting the results of the Phishing Campaigns through a secure portal. Customer will work closely with Suppliers to agree the scope, requirements of the test, schedule, track results and take remediation steps following the outcome of the test. Customer will provide target employee details including, e.g., their email address, role and full name.

J. Payment Card Industry Data Security Standard (PCI DSS) Consultancy

Supplier will provide an experienced information security consultant to provide a range of PCI DSS consultancy services to ensure Customer has implemented all the necessary policies, procedures and technical controls to achieve PCI DSS certification. Where available, Customer will be required to provide an asset inventory for systems in scope for PCI along with a network diagram and data flow diagram along with any other relevant supporting policies, procedures and documentation.

K. Service Organisation Control (SOC) 2

Supplier will provide an experienced information security consultant to provide a range of SOC2 consultancy services to assist Customer in the implementation of all necessary policies, procedures and technical controls in preparation for an audit by a Certified Public Accountant (CPA).

L. Training

Supplier will provide a range of standard training courses covering both cyber security awareness and GDPR awareness. These can be delivered through an online portal with a range of videos and associated exams which, along with built in reporting, allows Customer to track that staff have watched the videos and completed their exams. Other delivery methods include on-site training and virtual training using video conferencing tools. Bespoke training courses covering specific cybersecurity or GDPR topics can also be developed and delivered for Customers in any format, be that video, online training or, where agreed, physically on site. Supplier will provide a copy of any training materials to Customer in pdf format upon completion of the training.

3. Cyber Essentials

Supplier will assist Customer to achieve certification under the NCSC Cyber Essentials scheme. Support is provided in line with the level of service Customer has contracted for as per the following:

Feature	Certification only	Essentials	Essentials Plus
Cyber Essentials certification	Included	Included	Included
Cyber Essentials Plus certification			Included
Up to 25k FREE cyber insurance (i)	Included	Included	Included
Free additional cyber protection tools (ii)		Included	Included
Tailored policy documents			Included
Remote support (iii)		4h included	4h included
Free retest		1 free retest	1 free retest per certificate

Supplier in addition will provide:

A. Free cyber insurance available to UK companies if the basic certification covers the entire organisation.

B. Additional cyber protection tools as specified on the Order Form such as: vulnerability scanning, endpoint protection, online training and exams and Asset Profile.

C. Remote support via telephone, email or video conferencing. Additional support time required is available at our standard rate.

*Cyber Insurance:

Free cyber insurance, provided by a third party insurer, is provided to UK companies as part of the scheme if the basic certification covers the entire organisation.

Customer acknowledges that the Cyber Essentials scheme is intended to reflect that the certificated organisation has established the cyber security profile set out in the Cyber Essentials scheme documents only and that receipt of a scheme certificate does not indicate or certify that the certificate holder is free from cyber security vulnerabilities. Customer acknowledges that Supplier has not warranted or represented the Cyber Essentials scheme or certification under the Cyber Essentials scheme as conferring any additional benefit to Customer.

D. Cyber Essentials (excluding Cyber Essentials Plus)

After purchasing Cyber Essentials, Customer will be required to confirm via email when they are ready to complete their assessment. The Cyber Essentials team will send an email after initial purchase, asking to be informed when Customer is ready to proceed. Customer will not be given access to complete their assessment until a response is received.

Customer shall complete and submit the self-assessment form within a month of being added to the portal.

Customer shall comply with the Cyber Essentials scheme documentation and all reasonable directions made to Customer by the Authority, a Cyber Essentials Partner or a certification body.

Subject to Customer's completion of a Cyber essentials self-assessment (the "Questionnaire"), Supplier will assess the Customer-completed Questionnaire against the Cyber Essentials Scheme criteria.

The Questionnaire account will remain open and accessible for six (6) months. If Customer has not submitted the Questionnaire within 6 months, the assessment will expire and no refund will be permitted. If Customer wishes to complete the Questionnaire after expiration, it will be required to order Cyber Essentials again.

If the completed Questionnaire assessment meets the Cyber Essentials scheme criteria (which Supplier shall assess in accordance with the IASME marking scheme)

Supplier will notify Customer and, subject to Customer meeting its obligations, Supplier will arrange for the issue of a IASME Certificate to Customer.

If a certification only service has been purchased by Customer, no support will be provided by Supplier other than assistance gaining access to the Questionnaire.

If Customer has not submitted its application after a month of being added to the portal, reminders will be sent to Customer as follows:

- After 4 weeks of inactivity – one reminder email will be sent to the main contact on the application.
- After another 2 weeks a second reminder will be sent if Customer has still not submitted its application.
- After another 2 weeks a third reminder will be sent if Customer has still not submitted its application.
- After another 2 weeks a fourth and final reminder will be sent if Customer has still not submitted its application.

If all the above reminders do not result in a reply with either an offered date or a submission, this will be marked by the assessor as a Customer 'fail' and the Fees will be invoiced.

Where Customer's order has not been completed within 12 months from the date it was placed, the assessment will be marked as a 'fail' and Customer will be invoiced.

Cancellation of orders is not possible due to the systems and third parties involved in providing the service. Therefore, incomplete applications will be marked as a 'fail' and Customer will be invoiced.

E. Cyber Essentials Plus:

Customer must achieve an additional cyber essential level within 90 days of certifying against Cyber Essentials (excluding Plus). Any free retest offerings must be used within the 90-day deadline for completing Cyber Essentials Plus.

If Customer is unable to pass within that time through no fault of Supplier, the application will be marked as a 'fail'.

Where Customer fails the Cyber Essentials Plus test, Customer will have 30 days to remediate any issues found and get a retest (within the 90 days).

Where Customer refuses or fails to provide the access required to conduct the test, the test will be marked as a 'fail'.

If Customer wishes to move their assessment date, Customer must provide Supplier with at least 48 hours' notice. Failure to provide the requisite notice to Supplier will incur cancellation charges in line with the Services Agreement Standard Terms.

4. Incident Response

Supplier will provide Customer assistance within three hours via Supplier's SOC hotline which is available 24x7x365. The emergency request will consist of an initial assessment and triage via phone to discover and confirm the nature and impact of the incident within Customer‘s environment, including the collection and analysis of all relevant information, and to provide advice based on the nature of the incident. Customer will provide all necessary resources and information to ensure the success of the service. If more detailed analysis is required or the incident has been confirmed as a data breach the service will provide additional support to investigate the extent of the incident which may include forensic analysis supported onsite (Digital Forensics) where required at an additional cost as defined in the Services Agreement Standard Terms. Digital Forensics support will be charged, as required, at a day rate of ~£1,500.00 as updated by Suppler from time to time.

A. Customer shall provide and coordinate Supplier's access to the systems to be investigated. Before any system access is granted, Customer shall inform Supplier in writing and in advance of any security and access standards or requirements that may change.

B. During an assessment, the configuration of Customer's network will be kept as stable as possible (i.e., no new systems or configuration changes). If changes are required, Customer shall inform Supplier, and a mutually acceptable testing schedule shall be agreed upon.

C. During the initial notification call, Customer shall provide Supplier with information below to create an incident ticket. Customer shall appoint an authorised contact person for every incident raised. The appointed contact person shall be preregistered with Supplier.

Customer Name

1. Locations affected by the incident
2. Priority of the incident
3. Information on how the incident was identified

Contact Name

4. Contact Phone Number
5. Details of incident

6. Information on when the incident was first identified

Note: Should Customer consider the nature of the incident to preclude the support desk being provided with these details, Customer contact may simply state that the incident is a 'flash priority' at which point Supplier support personnel will request no further details and will immediately initiate the response procedures.

D. It is also the responsibility of Customer to provide details of the priority classification for discussion prior to rollout of the services. Further to this, it is considered Customer's responsibility to make the following information available and the processes followed. Supplier will work closely with Customer (as a separate engagement) to ensure that all responsibilities can be met.

E. Customer shall maintain accurate network diagrams and make these diagrams available to Supplier as required.

F. Customer shall maintain accurate process maps and diagrams, detailing the systems involved with the transmission, storage, or processing of sensitive information.

G. Customer shall provide an updated list (per incident) of personnel with which the aspects of the incident may be openly discussed. All other personnel will simply be directed toward their own management for information.

H. Customer shall provide contact information for senior personnel related to affected departments or systems to be contacted for further information (see previous point).

5. Managed Detection & Response

Supplier will provide a SaaS based security information and event management platform to deliver real-time analysis of potential cybersecurity threats. Supplier's security analysts will analyse Customer logs 24x7x365 to identify security threats and raise events to Customer for investigation. Customer will install, with the support of Supplier, relevant software and virtual hardware to support the delivery of the Service.

A. Definitions

The following additional definitions shall apply to this Service:

"APT" or "Advance Persistent Threat" means a set of stealthy and continuous computer hacking processes.

"Attack" means the inflow of malicious or illegitimate call requests to an infrastructure or web platform for malicious intent. The purpose of this is to gain access or to deliver disruption to the infrastructure.

“Critical” means the classification by Supplier of a Security Event as defined in the Managed Detection & Response Service Level Agreement (MDR SLA) that will receive the highest level of response from Supplier's designated trained security professionals.

“Incident Response Plan” means the overarching framework for both parties’ efficient and professional reactions during a security incident.

“Non-Critical” means a Security Event as defined in the MDR SLA that does not require immediate attention because it is deemed not to be critical.

“Runbook” means a routine compilation of procedures and operations which designated employees will use as a reference.

“Security Event” means 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 Incident” means a situation where an adverse impact has resulted from a Security Event.

“SIEM” means software products and services combining security information management (SIM) and security event management (SEM) that provide real-time analysis of security alerts generated by network hardware and software applications.

“Threat Investigation” means any actions taken by Supplier to validate a Security Event as a real threat and to rule out the possibility of it being a false alert.

“Threat Signatures” means any information provided by Vendors to help identify any threats that could impact Customer’s network or infrastructure.

“Vendors” means third parties who provide Supplier with infrastructure, products, intelligence or expertise to allow us to provide the Services, including but not limited to dedicated hardware appliances, Threat Signatures, and vulnerability scanning services.

“Zero-day” means an attack that exploits a previously unknown vulnerability in a computer application or operating system, one that developers have not had time to address and patch.

B. Supplier Obligations

Supplier will provide the following in accordance with the Order Form, the MDR SLA and Runbooks.

Active monitoring of all systems in scope for Security Event using a threat intelligence SIEM module.

Correlate various logs to identify any Security Events that may carry a potential threat.

Interpretation of logs and audit trail and focus on threats that matter most to Customer.

Incident investigation from triggered alerts and abnormal behaviour in accordance with a well-defined and agreed Runbook.

Customer notification and incident reporting in accordance with the agreed incident response plan.

Provide recommendations for dealing with incidents.

Ongoing management and maintenance of the threat (SIEM) appliances: installation, migration and configuration of the SIEM hardware or software.

All configuration files will be kept and backed-up for a minimum of 30 days with daily restore points covering one week, unless an alternative period is formally requested by Customer and agreed by Supplier.

All logs will be kept and backed-up for a minimum period of 30 days, with immediate access and 1 year in archive.

Incident reports will be generated within 24 hours following any critical Security Event as soon as the investigation has been completed. Upon request, Supplier will provide incident reports for any critical Security Events that have occurred.

Access to an online portal which will contain up-to-date incident reports and change control information.

C. Customer Obligations

Customer agrees to perform the obligations and that Supplier's ability to perform its obligations and its liability are dependent on Customer's compliance with the following:

Customer is required to make appropriate staff available to help Supplier with the following items (if applicable):

1. Runbooks
2. Incident Response Plan
3. Any other documents or procedures required to provide the Services.
4. Any infrastructure or platform used to provide the Services
5. Any other procedures required to provide the Services

In the case of a Security Event occurring, Customer agrees to work in line with agreed Runbooks.

Customer agrees and understands that the effectiveness of the Services depends on the collaboration during the on-boarding phase that will define and assess the processes, escalation points and on-going communication channels.

Customer must inform Supplier of any changes that could affect any individual Runbook or the Incident Response Plan. This also includes the escalation procedures, availability and contact details of personnel, reliability, performance and any other security or compliance related requirements.

D. Supplier MDR SLA

Supplier will work in line with the agreed Runbooks.

Supplier will monitor all key components used in the delivery of the Services 24x7x365.

In the event of any issues arising, Supplier will work to identify and resolve any threats or issues as quickly as possible.

Supplier will provide technical staff 24x7x365 to support the Services provided and to assist Customer with any issues that may arise. A 24-hour telephone number will be available for Customers. Email support will also be provided but should not be used for emergencies.

If a Critical event occurs, Supplier will perform an initial Threat Investigation and then notify Customer within 30 minutes of the Security Event if it has been deemed by Supplier to have become a Critical event.

If a Security Event occurs of a Non-Critical nature, Supplier will take actions in line with the agreed Runbook.

If a Security Event occurs Supplier will first carry out a Threat Investigation and will then respond to Customer within the timeframes listed in the table below.

For any Security Event which Supplier deems to be Critical prior to the Threat Investigation being completed, Supplier will contact and regularly update Customer.

The Security Event severity is typically set via the stage at which the event comes in the attack kill chain. The further along this process the more severe the event.

SEVERITY LEVEL	EXAMPLE	COMMUNICATION METHOD	RESPONSE TIME
Critical	Command and Control communication established / outbound	Phone, portal and email	30 minutes

	connection to known bad actor address		
High	Brute-force activity against externally facing systems with legitimate accounts	Phone, portal and email	30 minutes
Medium	Infrastructure or system version Information disclosure	Portal and email	-
Low	Administrator account lockout	Portal and email	-
Informatio nal	Reconnaissa nce such as Port Scanning	Portal only	-

E. EXCLUSIONS

Supplier will not be liable under the following conditions:

1. Where scheduled maintenance was being carried out;

2. Where there has been any act or omission of Customer (or its Representatives) in breach of the Services Agreement;

3. For any security breaches caused by any Customer changes of which Supplier was not made aware;

4. For any security breaches where Supplier takes an action requested by Customer which has not been agreed or tested as part of creating the relevant Runbook;

5. Where Threat Signatures were not available by the Vendors to allow Supplier to identify a threat including but not limited to Zero-day Attacks and APTs.

6. Outsourced Data Protection Officer (DPO)

A managed service where Customer can purchase a number of days (smallest amount is 0.5 days) per month for DPO services. Where Customer does not use the total amount of time in any given month, that time may be carried over to the subsequent month (but not longer).

Supplier will provide virtual consultation to Customer, information, advice and other related services, in accordance with the DPO Service Levels below, to ensure that Customer processes the personal data of its staff, customers, service providers or any other individuals (also referred to as data subjects) in compliance with Applicable Data Protection Laws and best practice.

A. Supplier Obligations

Supplier will:

Act as the Data Protection Officer (DPO) for Customer in accordance with Applicable Data Protection Laws;

Facilitate Customer compliance with the UK/EU GDPR and other applicable data protection legislation by ensuring effective systems and controls are in place to enable Customer to comply with their legal obligations;

Act as Customer's intermediary between relevant stakeholders, including supervisory authorities, data subjects, and business units;

Report notifiable data breaches identified and notified to Supplier by Customer to the Information Commissioner's Office (ICO) and any relevant supervisory authority at the end of any statutorily required notice period where the requisite notice has not been sent earlier either by Customer or Supplier at Customer's instruction; and

Inform and advise Customer's senior management (where appointed to do so) in accordance with Supplier's position as DPO of Customer.

B. Customer Obligations

Customer will ensure compliance with all Applicable Data Protection Laws and in particular Customer will:

Report all notifiable and potential data breaches to Customer assigned DPO dposupport@targetdefense.com as soon as Customer becomes aware of the breach;

Submit details of data breach(es) to Supplier for reporting to the ICO and any relevant supervisory authority without undue delay; and

Where Customer fails to comply with reporting obligations above, Supplier shall not be liable and Customer will indemnify Supplier for any penalties imposed by the ICO, any relevant supervisory authority or any third-party claims, because of failure and or delay in reporting notifiable breaches.

C. DPO Service Levels

Priority levels will be addressed in line with the following Service Levels.

Type	Response Time
Critical	within 1 Hour
Urgent	within 4 Hours
Non-urgent	by the end of the Next Business Day

All Service Levels apply only from 9:00am to 5:30pm GMT Monday to Friday excluding UK bank holidays ("Working Hours"). All DPO Service requests must originate with an email sent to the allocated DPO and copied to dposupport@targetdefense.com and the subject line must contain the priority in accordance with the following:

1. "Critical" a scenario which will have serious immediate impact on the protection of personal data

2. "Urgent" for advice on GDPR/data protection topics that are subject to time constraints

3. "Non-urgent"for advice and guidance on GDPR/data protection issues and longer term projects that do affect Customer's operations.

7. Penetration Testing

Supplier will perform penetration testing that evaluates Customer systems to validate and exploit known vulnerabilities by assessing critical external and/or internal assets and/or APIs and/or web applications and /or mobile applications and/or cloud

infrastructure and/or wireless infrastructure using experienced penetration testers to determine if Customer's organisation is susceptible to attacks. Supplier will provide a report in both online and downloadable versions within 5 working days of completion of a test.

A. Definitions:

"Late Availability Test" where Customer contacts Supplier to conduct Penetration Tests with five working days or less notice.

"Red Team Penetration Test" means the onsite presence of Supplier who will test the System as described in a scope Annex made by Supplier to Customer.

"Test Start Time" means the provisional or definitive date and time listed in the Order Form (or otherwise later expressly agreed by the parties in writing) that determines when the Services will commence.

B. Customer Obligations:

To submit, by upload into the penetration testing dashboard, any necessary further scope details at least five working days prior to the start of the Penetration Tests for efficient scheduling of necessary resources and time.

Where Customer fails to submit the necessary scope details, Supplier shall reschedule the Penetration Test and Customer shall be liable for any charges.

Customer and Supplier will agree dates promptly after the Commencement Date or as set forth in the Order Form for Supplier to deliver the Services within 12 months of the execution of the Order Form and, where Customer fails to agree dates for the Services through no fault of the Supplier, Customer will forfeit their right to the Services for the relevant 12-month period and, for the avoidance of doubt, no refund or waiver of Fees or related costs, all owed upon execution of the Order Form, will be issued by Supplier.

Where Customer requests a Late Availability Test and fails to timely provide Supplier with the necessary information to commence the Penetration Test, Supplier shall not be obliged to carry out the relevant Services and Customer will not be entitled to any refunds or waiver of Fees or related costs.

Customer acknowledges that the Service will be provided remotely unless explicitly requested and agreed otherwise. If onsite access is required to facilitate testing, Supplier will provide the option of customer present equipment (CPE) to facilitate remote testing from Supplier's secure remote location. In person tests may be provided upon request by Customer or Supplier, subject to approval by Supplier.

Customer acknowledges that a Penetration Test is a snapshot in time and that it is limited to the actions set out on the Order Form (which actions may be agreed in an incorporated scope Annex document).

Customer shall comply with any rules imposed by any third party whose content or services are accessed via the Services.

Customer shall inform Supplier forthwith if any of the Services are subject to interference or malfunction.

Customer, prior to Penetration Tests, must proactively and appropriately backup all critical data from its Systems that will form part of the Penetration Tests.

Where Customer engages Supplier to provide a Red Team Penetration Test, Customer further represents and warrants to Supplier that Customer: a) has the necessary authority to instruct Supplier to provide the Red Team Penetration Test; and b) shall sign a letter of authority (duly signed by an authorised member of the executive board or equivalent) in the eventuality that Supplier requires it.

8. Virtual Chief Information Security Officer (VCISO)

Supplier will provide a remote managed service that includes an experienced Information Security Consultant to build and implement information security strategy for Customers. The service may require an initial health check to establish the current security posture of Customer's organisation and enable Supplier's Consultant to build a strategy. This Service can also provide support to manage existing security frameworks such as Cyber Essentials and ISO 27001. On-site visits may be arranged, where agreed, with Customer in exceptional circumstances.

A. Supplier Obligations

Supplier will provide regular updates to Customer where reasonably requested;

Supplier will provide regular (at least monthly, at Supplier's discretion) updates on the progress of the implementation of the agreed security strategy;

Supplier will only amend any agreed strategy with the written agreement of Customer; and

Supplier will work with third party suppliers of Customer where reasonably requested (e.g., outsourced IT providers).

B. Customer Obligations

Customer will notify Supplier's designated VCISO of changes to Customer's business including, interpreted broadly:

1. Structural/organisation changes e.g., acquisitions, sales;
2. Critical role and responsibility changes;
3. Key Customer supplier changes that may impact on information security;

4. New Customer supplier onboarding that may impact information security;
5. New software/solutions/hardware/cloud services that are planned; and
6. Key personnel changes.

Customer will notify the VCISO of any security incidents or data breaches of which it becomes aware.

Customer will notify VCISO of any Customer regulatory, legislative and/or contractual requirements.

Customer will, when raising a request for assistance from its VCISO, ensure that vciso@targetdefense.com is copied on all messages.