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 via the platform for Customer to define its digital assets profile, assisting in identifying its attack surface and aligning relevant threat intelligence feeds. Customer will add assets to ensure the correct threat intelligence feeds align to Customer's environment.

b) Breach Detection
Supplier will provide a breach detection solution to protect Customer's organisation and staff from data breaches. The platform detects leaks of data in the dark web, private hacker forums, and criminal marketplaces, and provides alerts of what has been detected.

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

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

- Windows: FileScan, ContentControl, UserControl, Application Blacklisting, DataProtection, TrafficScan, AntiPhishing Firewall, BehavioralScan, MailServers (Exchange-only servers), DeviceControl, AntiExploit
- Mac: FileScan, Update Server, and ContentControl 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) Endpoint Protection Pro
Supplier will provide Endpoint Protection Pro software and the platform to manage the endpoints. Supplier will also provide staff to manage, tune and support the platform. The following features are included:

- Windows: FileScan, ContentControl, UserControl, Application Blacklisting, DataProtection, TrafficScan, AntiPhishing Firewall, BehavioralScan, MailServers (Exchange-only servers), DeviceControl, AntiExploit, Patch Management, Volume Encryption, EDR Sensor
- Mac: FileScan, Update Server, and ContentControl with TrafficScan + AntiPhishing, EDR Sensor
- Linux: FileScan, Update Server, and EDR Sensor

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.

f) Microsoft 365 Secure Score Monitoring

Microsoft Secure Score is a measurement of an organisation's security posture, with a higher number indicating more recommended actions taken. The platform will automatically assess the Customer's Secure Score and provide alerts to help remediate any issues. The platform ensures Customer's environment is continually secured by regularly checking for misconfiguration.

This service helps organisations to:

- Report on the current state of the organisation's security posture.
- Improve security posture by providing discoverability, visibility, guidance, and control.
- Compare with benchmarks and establish key performance indicators (KPIs).

g) Microsoft 365 Identity Monitoring

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

h) Panic Button

Supplier will provide a 24x7x365 emergency help button which allows Customer to raise potential security incidents with Supplier's 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. Panic Button is subject to acceptable use policies.

i) Phishing Simulator

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

j) Security Information and Event Management (SIEM)

Supplier will provide 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 from Supplier, the relevant software and virtual hardware to support delivery of the service.

k) Threat Dashboard

Supplier will provide a single interface within the platform that displays threats across all the services provided. Threats are automatically populated by each feature, including live threat intelligence tailored to Customer. The platform provides functionality to manage threats, assign them to specific individuals for remediation, and categorise them by risk level. Customer will take action to remediate threats, accept risks, or acknowledge false positives as identified.

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 commonly used by attackers, including sub-domain detection, port scanning of top 20 ports, network information gathering, SSL validation, site popularity risk assessment, 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 domains as the scope for these checks.

m) Online Training & Exams

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

n) Vulnerability Scanning

Supplier will provide functionality within the platform to allow Customer to run automated vulnerability scans of common ports, with the option to customise scope to Customer's requirements, to assess systems or applications for known security flaws and weaknesses. Supplier will provide alerts that can be managed, allocated, assigned and marked as accepted risks, along with actionable remediation advice. This service will allow Customer to identify assets prone to attack. Customer will define the scope of scans and take measures to patch or remediate threats as advised.

o) Endpoint Agent

Supplier will provide a lightweight software agent to be installed on Customer's end-user devices. The agent will collect information regarding the host device's operating system and installed applications, enabling detailed visibility of asset profiles. The service also includes functionality to isolate the host device from connected networks, facilitating rapid response to suspected compromises or security breaches. The agent operates continuously, ensuring that device information is regularly updated, and isolation capabilities can be triggered as needed.

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, Applicable Data Protection Laws, other data protection laws and data protection in general. . 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 data protection 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 Gap Analysis (including but not limited to 27001, 9001, 27701, 22301)

Supplier will provide an experienced ISO consultant to undertake a Gap Analysis against, as appropriate, the version of the ISO 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 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 Implementation (including but not limited to 27001, 9001, 27701, 22301)

Supplier will provide an experienced ISO lead implementer to deliver an ISO 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 Internal Audit (including but not limited to 27001, 9001, 27701, 22301)

Supplier will provide an experienced ISO 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 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 Applicable Data Protection Law and other data protection awareness. These can be delivered through an online portal with built in reporting, allowing the Customer to track that staff have watched the videos. Other delivery methods include on-site training and virtual training using video conferencing tools. Bespoke training courses covering specific information security, cyber security or data protection 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. <u>Cyber Essentials</u>

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 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:

Supplier in addition will provide:

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

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. Details of the insurance cover can be requested from the insurer.

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 benefit to Customer other than as set forth herein.

a. 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 the above reminders do not result in a Customer reply with an offered date or a submission, Customer will be invoiced either at the point where their account expires (6 months after the questionnaire account being added) or when their contract ends, whichever is sooner.

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.

b. 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'.

The following charges will apply to any Customer short-term cancellation and rescheduling:

cancellation or rescheduling requested between 7 and 14 days before the scheduled start date for delivery of any Services: 50% of the scheduled Service Fees of the cancelled or rescheduled Service(s); or
for cancellation or rescheduling requested within 7 days before the scheduled start date for delivery of any Services: 100% of the scheduled Service Fees of the cancelled or rescheduled Service(s).

Customer agrees to allow Supplier to conduct a discovery exercise as part of the Cyber Essentials Plus test. This may be, but not limited to:

- Establishing enrolled devices via Customer's MDM system.
- Establishing connected devices via Customer's managed firewall.
- Establishing connected devices via Customer's managed Antivirus.
- Establishing devices connected to Customer's Network by performing a network scan against the Customer's corporate network using a network scanning tool such as Nmap.
- Establishing number of users against a provided list of devices through a review of Customer's managed Email service.

Supplier reserves the right to conduct the discover exercise multiple times to ensure that the information is valid and true.
Supplier reserves the right to conduct more than one of the above listed bullet point exercises to ensure accuracy.
If a discovery exercise is not possible, or if the result of the exercise shows major inconsistencies between the provided device list and the answers to Customer's Cyber Essentials Basic Self-Assessment, the Cyber Essentials Plus test will be marked as a Fail and will not be able to progress or eligible for a refund.
Supplier must hold all data relating to the Cyber Essentials Plus test for the term of Customer's Cyber Essentials Plus certificate (i.e., 12 months).

4. <u>Incident Response</u>

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

i. Locations affected by the incident
ii. Priority of the incident
iii. Information on how the incident was identified

Contact Name

iv. Contact Phone Number
v. Details of incident
vi. 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. 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@bulletproof.co.uk** 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.

Priority	Acknowledgement	Response	Resolution
Critical	1 hour	1 hour	1 day
Urgent	4 hours	4 hours	2 days
Standard	1 day	3 days	5 days
Scheduled	1 day	Mutual Agreement	Mutual Agreement

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@bulletproof.co.uk** and the subject line must contain the priority in accordance with the following:

i. Critical:
e.g., Serious incident (mass data breaches or live data threat such as ongoing data theft for instance) where immediate support to contain or reduce the impact is warranted
1 hour, issue to be raised by emailing consultants and DPO mailbox (add critical to subject heading and add "high importance flag" added) and phoning it in

ii. Urgent:
e.g., incident/ breach which has essentially stopped, other topics with high time pressures and financial or reputational risks for the business

4 hours to 1 day, issue to be raised by emailing consultants and copying in DPO mailbox (add urgent to subject line and "high importance flag" added)

iii. Standard Priority:
e.g., advice and guidance on matters with shorter timescales (regulatory response, DSARs, etc.,)
next 1-3 business days (to be agreed based on circumstances), issue to be raised by emailing consultants and copying in DPO mailbox or agreed over Teams or other conversation with the actual timeline agreed in initial reply

iv. Scheduled:
Anything else, development, DPIA process, project support…
Timescales to be agreed on a case-by-case basis, typically around 1 week but longer for larger items with higher complexity and amenable lead times, raised by emailing consultants, DPO mailbox, or other conversation

6. Penetration Testing (Standard and Simulated Attack)

a. Standard 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 and/or physical security controls/sites and/or hardware and/or exposed online content (OSINT) and/or staff security awareness (Social Engineering/phishing) 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 five (5) working days of completion of a test.

a.1 Definitions

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

"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.

"Open-Source Intelligence (OSINT)" – the collection and analysis of publicly available information to verify what information can be extracted about an organisation or individual before any hypothetical attack would take place.

"Social Engineering (Phishing/Vishing)" – the conduct of controlled phishing campaigns to allow an organisation to test its resilience, such exercises being customisable to target specific departments, remote workers, executive level staff or everyone across the business, allowing Customer to determine whether more training or stricter policies are required.

a.2 Customer Obligations

To submit, by upload into the SaaS platform (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 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.

For hardware/device assessments, Customer is required to provide the hardware in scope at least two (2) weeks before the start date of the assessment to allow adequate time for Supplier to confirm connectivity. The following are also required where possible:

- Any cables, interfaces or power supplies that would be required for normal hardware operation
- Where the tester would be allowed to open the device up, any hardware security/anti-tamper devices should be disabled (for example if testing card payment terminals, these automatically become unusable/self-wipe if opened)
- Product and API documentation if applicable
- Schematics (depending on scope of the engagement)
- Firmware images (depending on scope of the engagement)

b. Simulated Attack Penetration Testing (Red, Purple and Black Teams)
Supplier will perform a special form of penetration testing -- a simulated cyber-attack that will aim to achieve specific goals set by Customer and evaluate customer systems to validate and exploit known vulnerabilities in critical systems and/or physical onsite locations using experienced penetration testers to determine if Customer's organisation is susceptible to real-world attack vectors. Supplier will provide a report in both online and downloadable versions within 5 working days of completion of a test.

b.1 Definitions
In addition to the Penetration Testing definitions in 7.A.1 above, the following apply:
"Red Team" - A red team engagement is an objective driven assessment that uses tactics, techniques, and procedures (TTPs) to emulate real-world threats. This engagement is comprised of various activities (chained or not) to assess the possibility of accessing particular systems/data or physical locations (Black Team assessments). Such activities aim to attack people, processes, and technology to reach pre-defined goals as opposed to solely measuring their defensive effectiveness. The methodology of a Red Team is bespoke and is created during the scoping phase depending on the goals and attack paths Customer wants to explore during the assessment. These attack paths predominantly focus on Physical Locations, Staff and Infrastructure & Technology as each possess their own threat profiles.
"Purple Team" – A purple team engagement is a Red Team engagement with a higher level of collaboration and feedback between the offensive and defensive teams. Ultimately, this tends to provide a higher level of coverage within the assessment's time period as the collaboration can help guide the offensive team to focus on specific areas of weakness or to tailor attacks against software and systems in use. This also gives the opportunity for defensive teams to tune their detection, response and containment capabilities.
"Black Team" - This is a Physical Security assessment that utilises a bespoke scope to satisfy Customer's specific aims and goals. The assessments highlight the strengths and weaknesses of the physical security controls in place and provide in-depth recommendations on how each reviewed site could improve their overall physical security posture. Often, the security of IT infrastructure and data that is only available "internally" is prioritised less in the ongoing hardening and issue remediation campaigns within an organisation. This can lead to security gaps as the only limitation from accessing these resources may be the fact that an attacker needs to be physically inside the premises. These exercises help show the viability of an external attacker gaining this level of access and highlights the subsequent risk landscape if this situation was to arise in the real world.

b.2 Additional Customer Obligations
All engagement options require trusted parties to attend an enhanced scoping and planning workshop prior to the start of the engagement. This must be completed a minimum of two (2) weeks prior to the start of any complex red team engagement (Black Team, Purple Team, Red Team). This workshop is mandatory to ensure the safe and correct delivery of the engagement, failure to complete this workshop will affect project start dates.
Customer must ensure that the required technical and trusted contacts are available throughout the engagement. Emergency and out of hours contact processes will be put in place and both Customer and Supplier must adhere to these.
Customer acknowledges that the Service will be provided remotely unless explicitly requested and agreed otherwise, dependent on the rules of engagement. If onsite access is required to facilitate testing, a minimum of two emergency contacts must be provided and available for contact throughout any on-site phases. Further to this, a letter of authorisation is required for Customer/operatives to verify their identity and authority to be onsite if questioned by Customer. Customer is responsible for ensuring that this authorisation letter and the emergency contacts possess sufficient authority to

authorise Supplier and provide a suitable level of indemnity from any situations that may involve law enforcement escalations or internal security.
Where onsite presence is required, Customer is required to highlight any environmental factors, restricted areas, equipment or security controls that may impact the safety of Supplier.
Customer will adhere to any rules of engagement, processes and any additional obligations agreed upon in the scoping and planning workshop. These will be clearly defined and provided to Customer in writing following the workshop and prior to the start of the engagement, any changes to this document must be agreed on by both parties.
Customer may be required to ensure operational secrecy is maintained within the organisation. Any failure in this process may impact the results and outcomes of the engagement, Supplier will ensure any concerns around operational secrecy and its impact are raised in writing to the trusted parties prior to adding caveats and amendments to report findings.
Customer must provide all information required during scoping and planning sessions and ensure this information is accurate to the best of their knowledge, attempts to deliberately hinder or manipulate the engagement will be documented and included in the final report.
Where Customer engages Supplier to provide a Simulated Attack engagement, Customer further represents and warrants to Supplier that Customer: a) has the necessary authority to instruct Supplier to provide the Red Team engagement; 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.

Simulated Attack Cancellation charges:
In addition to the charges set forth in the Services Agreement Standard Terms for services related to non-Supplier delay, cancellation and rescheduling charges, for costs related directly to the administration, system, personnel, facilities, third party and/or other allocated resources associated with scheduled Services, the following charges will apply to any Customer short-term cancellation and rescheduling:

a. cancellation or rescheduling requested between 30 and 20 days before the scheduled start date for delivery of any Services: 20% of the scheduled Service Fees of the cancelled or rescheduled Service(s); or
b. for cancellation or rescheduling requested between 19 and 15 days before the scheduled start date for delivery of any Services: 40% of the scheduled Service Fees of the cancelled or rescheduled Service(s) ; or
c. for cancellation or rescheduling requested within 14 days before the scheduled start date for delivery of any Services: 100% of the scheduled Service Fees of the cancelled or rescheduled Service(s).

b.3 Additional Supplier Obligations
Supplier will make commercially reasonable efforts to ensure testing activities are carried out professionally and minimise risk to Customer's operations. Simulated Attack activities will be logged and any actions that cannot be reverted by the Supplier during clean-up phases will be included in the report as "Clean Up Actions" with clear instructions to enable Customer to remove all traces of Simulated Attack activity at the conclusion of the project.
Supplier will notify Customer and cease testing should evidence of real ongoing threat activity be discovered during the engagement.
Supplier will ensure all communication channels used during the engagement are encrypted at all points and any operational data including log sources are backed up and securely encrypted within controlled networks.
All Red Team actions by all team members during the engagement are recorded. Operations Logs can be made available to Customer at any point during the engagement on request. At a minimum the following data is provided for all activities; time, date, source, target and action.
Where onsite presence is required, the Health & Safety of the operatives is the responsibility of Supplier during the assessment. Due to this, the safety of the operatives and the risks from each activity will be continuously reviewed by the Team Leader of each assessment. If it is found that the security controls in place or conditions of a site in scope may present a risk to the operatives, the team may decide that it is unsafe to proceed. Examples of this would include unsafe areas under construction, the use of armed guards, electric fences or guard dogs. In such an event, the operatives will raise these concerns in writing to Customer.
For onsite Black Team assessments, a number of key points will be adhered to for every assessment:

- No use of violence, threat of violence or threatening behavior will be used on any engagement
- Unless otherwise specified, no action will be performed that has a high likelihood of damaging Customer site or its assets. This includes acts such as lock picking or pushing open weak magnetic door locks
- The impersonation of a Police officer, Fire Officer or Health & Safety Inspector is not permitted
- No unlawful activity is permitted
- A full record of each visit will be maintained

7. 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 Cyber Security Assessment 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:

a. Structural/organisation changes e.g., acquisitions, sales;
b. Critical role and responsibility changes;
c. Key Customer supplier changes that may impact on information security;
d. New Customer supplier onboarding that may impact information security;
e. New software/solutions/hardware/cloud services that are planned; and
f. 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@bulletproof.co.uk** is copied on all messages.