

Lanmark Cyber Services Terms of Service

VERSION 1.1



Document Control

Document Reference	Lanmark Cyber Services Terms of Service		
Document Version	1.1		
Document Date	February 2023		
Revision History	Date	Version	Reason
	22/10/23	1-0	Document Published
	10/02/24	1-1	Document Revised

Managed Detection and Response (MDR-as-a-Service).....	4
Security Operations Centre (SOC-as-a-Service)	4
Extended Detection and Response (XDR-as-a-Service).....	4
Scope of Services	5
Managed Detection and Response / SOC Services	5
Microsoft Defender for Endpoint Detection and Response Solution	6
Lanmark Deliverables / Responsibilities	6
Client Responsibilities	6
Service Terms	8
Exclusions	8
Steady State Operations	9
How does Lanmark work as a Managed Security Services Provider (MSSP)?	9
What happens if Lanmark finds a problem before I do?	9
What is Lanmark's expected response time to clients for alerts?.....	9
How does Lanmark determine the Priority Level?.....	9
What if I add or remove servers or other devices within my environment?	10
What type of alerts will I see and what should I do?	10
Vulnerability Assessments	11
Penetration Testing	11
1. Definitions	12
2. Scope of Services	12
3. Term and Termination	13
4. Fees and Payment	13
5. Confidentiality	13
6. Intellectual Property	13
7. Limitation of Liability	14
8. Indemnity.....	14
9. Governing Law	14
10. Miscellaneous.....	14

These Cyber Services Terms of Service (“Cyber Services Terms”) set out the terms and conditions upon which Lanmark Limited (“Supplier” or “Lanmark”) provide Managed Services to the Customer (as identified in the Account Application Form) and are governed by the Master Services Agreement set out at lanmark.com/terms-of-business (“MSA”).

These Cyber Services Terms together with the MSA, the Account Application Form, the applicable Order Form(s), Quote, other applicable Additional Conditions and any other documents agreed between the Parties, constitutes the entire agreement between the Parties in relation to the supply of the Services by the Supplier.

Definitions and interpretation:

1. Except as defined in these Cyber Services Terms, all capitalised terms used in these Cyber Services Terms shall have the meaning given to them in the MSA.
2. The terms set out in these Cyber Services Terms are in addition to and should be read in conjunction with the terms of the MSA.
3. In the event of a conflict, the provisions of these Cyber Services Terms shall take precedence over the MSA.



Managed Detection and Response (MDR-as-a-Service)

Security Operations Centre (SOC-as-a-Service)

Extended Detection and Response (XDR-as-a-Service)

Scope of Services

The primary objective of our Managed SOC and Detection and Response services is to detect intrusions and unauthorised activity and to automate a containment and/or quarantine action quickly. The services are customised for each client and will create a cyber security risk management posture to protect enterprise data, assets, and brand equity for clients and stakeholders. Lanmark will support an advanced security posture of your network environment through the following capabilities:

Service	Service Only	Service and Solution
Security Operations Centre (SOC) <i>Monitoring, Alerting and Response for SIEM solutions and Microsoft 365</i>	Lanmark provides monitoring of the Client's configured and operational SIEM solutions.	Lanmark will implement and monitor Microsoft Sentinel or Rapid7 Insight SIEM solutions
Managed Detection and Response (MDR) <i>Monitoring, Alerting and Response for EDR solutions</i>	Lanmark provides monitoring of the Client's configured and Operational EDR solutions.	Lanmark will implement and monitor Microsoft Defender for Endpoint.
Extended Detection and Response (XDR) Combination of MDR and SOC solutions	Lanmark provides monitoring of the Client's configured and operational SIEM and EDR solutions.	Lanmark will implement and monitor Microsoft Sentinel or Rapid7 Insight SIEM solutions and Microsoft Defender for Endpoint

Managed Detection and Response / SOC Services

The Security Operations Centre (SOC) will provide 24/7/365 monitoring, alerting, and containment of real-time threats for all devices within the client enterprise network using endpoint protection software, log aggregation and identity analysis and active threat hunting tools provided by Lanmark.

- Managed Detection and Response
 - 24/7/365 Monitoring, Alerting and Containment of Real-Time Threats
 - Protection (24x7x365)
 - Monitoring
 - Active Threat Hunting
 - Contain & Quarantine
 - Incident Response Assistance
 - Alert / Inform / Educate
- Vulnerability Monitoring/Reporting
- Vulnerability Management

- Endpoint Detection and Response

Microsoft Defender for Endpoint Detection and Response Solution

The service utilises Microsoft's Defender Protection/Detection Platform tools that provides autonomous endpoint protection, prevention and detection of attacks and visibility into endpoint environments.

Features include:

- Protection against both malware and malware free attacks
- Anti-virus tools
- Machine learning and artificial intelligence to detect known and unknown malware and ransomware
- Behaviour-based indicators of attack (IOAs) to prevent sophisticated files and malware-free attacks
- Automated detection of unidentified zero-day attacks
- Exploit blocking mechanisms to stop the executing and spread of threats via unpatched connections
- Positive and negative approaches
- Identify attacks and stop breaches 24/7/365 with an elite team of Lanmark experts who proactively conduct incident response, hunt, investigate and engage in Red Team exercises
- Industry leading threat intelligence, incident investigation, and response

Lanmark Deliverables / Responsibilities

- Lanmark will manage this onboarding project
- Lanmark will manage and maintain the necessary licenses to support Endpoint protection (EDR) and Threat Hunting
- Lanmark will lead system tuning efforts during onboarding phase and during operational phase after major systems changes/additions
- Lanmark will respond to and mitigate alerts and issues defined in Scope of Services
- Lanmark will contact Client IT Staff for support and remediation of issues beyond what is defined in Scope of Services
- Lanmark will provide monthly threat/activity reports
- Lanmark will host a quarterly review to discuss threat/activity, trends and security issues

Client Responsibilities

As the consumer and network owner, Client will have the following basic responsibilities before, during and after the project:

- Provide a single point of contact to serve as the primary liaison with Lanmark throughout the project and to work with Lanmark to satisfy client responsibilities
- Provide any technical information in support of this engagement

- Procure, install and manage all endpoint software required for this engagement
- Ensure all client enterprise systems, workstations and laptops are up to date, fully patched and properly supported
- Respond to Lanmark notification of alerts and remediate systems as necessary
- Provide details of changes within the environment {i.e., servers, domain controllers, firewalls, workstations etc.)

Service Terms

Client acknowledges that certain Services provided by Lanmark are dependent upon Third Party Software or Third-Party Services that are subject to volume-based pricing (e.g., end user seat licenses, data processing consumption/usage fees, etc.). Therefore, Client acknowledges and agrees that Lanmark's quoted pricing is based upon Client's representations regarding the size and scale of its computing environment. In the event such environment increases in size (e.g., user or processing growth), Lanmark will be required to charge more to account for any capacity related up charges Lanmark receives from its third-party software and services providers.

In furtherance of the foregoing, Lanmark and/or its third-party software and service providers will be auditing the environment for user, system, and data usage growth at least quarterly. Changes to the overall security program, including network architectures, network components (Firewalls, routers, Active Directory Domain Controllers, Routers, etc.), must be discussed with Lanmark prior to implementation to ensure no lapse in overall security posture; these changes must be addressed through custom "level of effort" if they require Lanmark to perform work. Client acknowledges and agrees that cost increases based on increased volume and usage may not be reduced if usage is reduced as Lanmark may be required to purchase long-term licenses for such volume increases.

The following cost increases are estimates and may not be the final surcharges applicable to the relevant types of usage or volume increases (depending on the final selection of Third-Party Software and Third-Party Services used to provide the Lanmark Services).

Exclusions

- The following elements are excluded from the services proposed in this Statement of Work
 - Remediation of issues identified through the activities defined in this Statement of Work
 - NOTE: Remediation is referred to as the act of IT System Administrator-level activity to update or reconfigure systems (patches, upgrades, etc.) related to hardware or software configurations and improvements. This does not apply to remediation of systems identified as being under attack during a breach attempt.
- Development of custom solutions, including scripting, including any modification of client application software
- Any additional hardware/software or configuration thereof not listed in this document
- Development or architectural design beyond what is required to perform the work detailed in the Project Details for this Project
- Ongoing configuration changes once implementation has completed (any services beyond the scope of the engagement will be quoted as a separate project or service)

Steady State Operations

How does Lanmark work as a Managed Security Services Provider (MSSP)?

Lanmark is constantly monitoring your endpoints and network. Lanmark monitors 24 hours/7 days a week. We will identify and prevent most threats before any compromise will take place. We will notify client if any action needs to be taken due to a threat.

What happens if Lanmark finds a problem before I do?

Lanmark will remediate the threat and contact you as needed depending on the severity level of the threat.

What is Lanmark's expected response time to clients for alerts?

For P1 and P2 events, we will Create a Ticket in our ticketing system and immediately attempt to contact you for notification of event or support to manage the event. We will contact you (primary contact) and then provide periodic updates based on the priority of the problem.

Response Times and Availability				
Priority	SOC Action	Response (in hours)	Target Resolution* (in hours)	Update Interval (every in hours)
P1	Create Ticket / Call Customer	0.5 hour	4 hours	1 hour
P2	Create Ticket / Call Customer	1 hour	8 hours	2 hours
P3	Create Ticket	4 hours	16 hours	24 hours
P4	Create Ticket	12 hours	32 hours	48 hours
P5	Create Ticket	32 hours	48 hours	48 hours

*Target Resolution does not guarantee the situation will be resolved.

How does Lanmark determine the Priority Level?

P1: Probable or Actual Cyber event that requires immediate response and client notification.

P2: POSSIBLE Cyber events that require monitoring and customer notification.

P3: Detected security events that pose no immediate threat to confidentiality, integrity or availability of infrastructure.

P4: Activity or system upgrades that are needed but do not pose an immediate threat.

P5: Routine requests for information or systems upgrades.

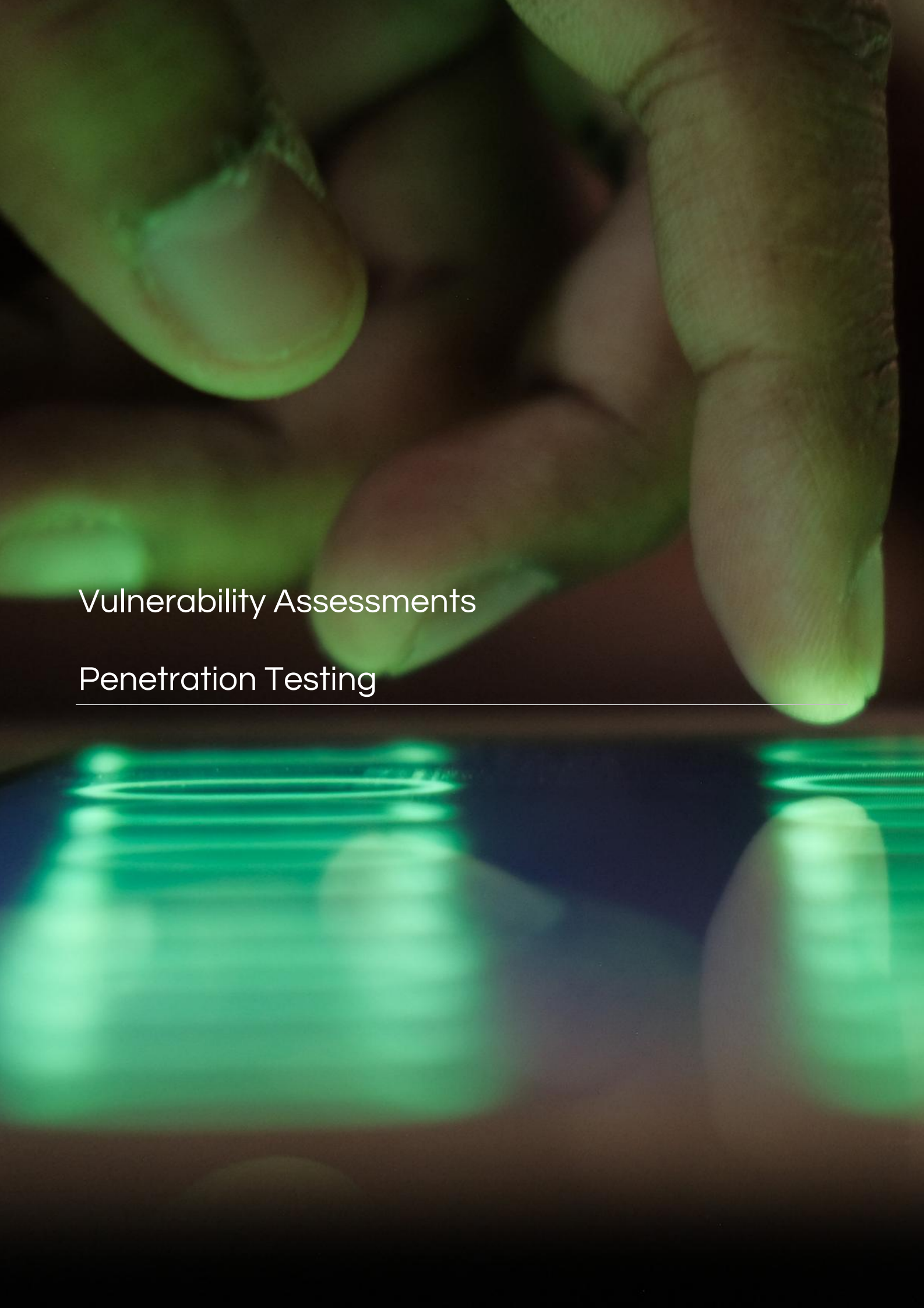
What if I add or remove servers or other devices within my environment?

Your network will change with time, but your security posture should remain high. Adding new servers or workstations should be accompanied by installing endpoint software. Adding firewalls or domain controllers to enhance network operations should be accompanied by ensuring logs for these devices are forwarded to your SIEM product. If you have any questions about how to proceed, please contact your Account Executive or Project Manager to discuss the situation and ensure your security posture remains intact.

What type of alerts will I see and what should I do?

Some of the most common types of alerts are called potentially unwanted programs (PUP). As your MDR Lanmark is monitoring your endpoints and will take action immediately upon detection of malicious software. If you notice malicious or anomalous activity within the network, please do not hesitate to contact us.

- Our endpoint detection response (EDR) may react to a PUP and immediately isolate the software; you may never be alerted to this activity.
- If you see alerts on your systems that warrant concern, please contact Lanmark based on priority. We may be in the early stages of an investigation, but your input will certainly help determine the severity of the situation.

A close-up photograph of a hand with fingers touching a smartphone screen. A red laser grid is overlaid on the screen, creating a grid of red lines. The background is dark, and the lighting is focused on the hand and the screen.

Vulnerability Assessments

Penetration Testing

1. Definitions

1.1. "Service Provider" refers to Lanmark Limited.

1.2. "Client" refers to the individual or entity purchasing the services provided by the Service Provider.

1.3. "Services" refers to the vulnerability assessment and penetration testing services provided by the Service Provider.

1.4. "Agreement" refers to these terms and conditions, including any applicable service agreements or schedules.

1.5. "Confidential Information" means any information disclosed by either party to the other, directly or indirectly, that is designated as confidential or would be reasonably understood to be confidential.

1.6. "Intellectual Property" means any patents, trademarks, trade names, design rights, copyright, database rights, know-how, and any other intellectual property rights.

2. Scope of Services

2.1. The Service Provider agrees to provide vulnerability assessment services and penetration testing services, including but not limited to testing of external IPs, internal IPs, web applications, and social engineering testing, as specified in the service agreement.

2.2. Access to Client Systems: The Client acknowledges

and agrees that the provision of the Services requires the Service Provider to have access to the Client's systems. This may include, but is not limited to, access to external and internal networks, web applications, and other systems as agreed upon in the service agreement. The Client shall ensure that such access is granted in a timely manner and maintained throughout the duration of the Services.

2.3. Whitelisting: The Client agrees to whitelist the Service Provider's scanning systems and IP addresses to ensure that security controls do not block or interfere with the testing process. The Service Provider will provide a list of IP addresses and other necessary details for whitelisting purposes.

2.4. Client Responsibilities:

a) Provide the Service Provider with access to all necessary systems, networks, and information required to perform the Services.

b) Ensure that all necessary permissions and authorisations are obtained to allow the Service Provider to conduct the Services.

c) Ensure that the environment is in a stable state and that adequate backups are in place before testing begins.

d) Inform the Service Provider of any specific security policies or compliance requirements that must be adhered to during the testing process.

e) Provide timely feedback and responses to any queries or requests for information from the Service Provider.

2.5. Service Provider Responsibilities:

a) Perform the Services in a professional and diligent manner, using reasonable skill and care.

b) Ensure that all testing activities are conducted in accordance with the agreed scope and any applicable legal or regulatory requirements.

c) Provide the Client with detailed reports of the findings, including identified vulnerabilities, potential impacts, and recommended remediation actions.

d) Maintain confidentiality of all Client information and data accessed during the provision of the Services.

e) Notify the Client immediately of any significant security issues discovered during the testing process.

2.6. Exclusions: The fees for the Services do not include any remediation work to fix identified issues. Any such remediation work will be subject to a separate agreement and additional fees.

2.7. Use of Third-Party Service Providers: The Service Provider may utilise third-party service providers in the provision of part or all of the Services. The Service Provider will ensure that any third-party service providers comply with the terms and conditions of this Agreement and maintain the confidentiality of any Client information accessed during the provision of the Services.

3. Term and Termination

3.1. This Agreement shall commence on the date of acceptance and shall continue until the completion of the Services or until terminated in accordance with this clause.

3.2. Either party may terminate this Agreement with immediate effect by giving written notice to the other party if the other party:

a) commits a material breach of this Agreement and fails to remedy that breach within 30 days of being notified in writing to do so; or

b) becomes insolvent or unable to pay its debts as they fall due.

3.3. The Client may terminate this Agreement for convenience by giving 30 days' written notice to the Service Provider.

4. Fees and Payment

4.1. The fees for the Services shall be as set out in the service agreement. All fees are exclusive of VAT, which shall be added to the invoice at the applicable rate.

4.2. The minimum fee for vulnerability assessment and penetration testing services is £2400.

4.3. The Client shall pay all invoices within 30 days of the date of the invoice.

4.4. If the Client fails to pay any amount due under this Agreement, the Service Provider may suspend the provision of the Services until such payment is made.

5. Confidentiality

5.1. Each party undertakes that it shall not at any time disclose to any person any Confidential Information except as permitted by this clause.

5.2. Each party may disclose the other party's Confidential Information:

a) to its employees, officers, representatives, or advisers who need to know such information for the purposes of carrying out the party's obligations under this Agreement; and

b) as may be required by law, a court of competent jurisdiction, or any governmental or regulatory authority.

6. Intellectual Property

6.1. All Intellectual Property rights in or arising out of or in connection with the Services shall be owned by the Service Provider.

6.2. The Service Provider grants to the Client a non-exclusive, non-transferable licence to use the deliverables produced by the Service Provider solely for the purpose of receiving and using the Services.

7. Limitation of Liability

7.1. Nothing in this Agreement shall limit or exclude the Service Provider's liability for:

- a) death or personal injury caused by its negligence;
- b) fraud or fraudulent misrepresentation; or
- c) any other liability which cannot be limited or excluded by applicable law.

7.2. Subject to clause 7.1, the Service Provider shall not be liable to the Client, whether in contract, tort (including negligence), breach of statutory duty, or otherwise, for any loss of profits, or any indirect or consequential loss arising under or in connection with this Agreement.

7.3. The Service Provider's total liability to the Client in respect of all other losses arising under or in connection with this Agreement, whether in contract, tort (including negligence), breach of statutory duty, or otherwise, shall not exceed the total fees paid by the Client under this Agreement.

8. Indemnity

8.1. The Client shall indemnify and hold harmless the Service Provider against all liabilities, costs, expenses, damages, and losses (including but not limited to any direct, indirect, or consequential losses, loss of profit, loss of reputation, and all interest, penalties, and legal and other reasonable professional costs and expenses) suffered or incurred by the Service Provider arising out of or in connection with the Client's breach of this Agreement.

9. Governing Law

9.1. This Agreement and any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with it or its subject matter or formation shall be governed by and construed in accordance with the law of England and Wales.

9.2. Each party irrevocably agrees that the courts of England and Wales shall have exclusive jurisdiction to settle any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with this Agreement or its subject matter or formation.

10. Miscellaneous

10.1. Assignment: The Client shall not, without the prior written consent of the Service Provider, assign, transfer, charge, subcontract, or deal in any other manner with all or any of its rights or obligations under this Agreement.

10.2. Entire Agreement: This Agreement constitutes the entire agreement between the parties and supersedes and extinguishes all previous agreements, promises, assurances, warranties, representations, and understandings between them, whether written or oral, relating to its subject matter.

10.3. Amendments: No variation of this Agreement shall be effective unless it is in writing and signed by the parties (or their authorised representatives).

10.4. Waiver: A waiver of any right or remedy under this Agreement or by law is only effective if given in writing and shall not be deemed a waiver of any subsequent breach or default.

10.5. Severance: If any provision or part-provision of this Agreement is or becomes invalid, illegal, or unenforceable, it shall be deemed modified to the minimum extent necessary to make it valid, legal, and enforceable. If such modification is not possible, the relevant provision or part-provision shall be deemed deleted. Any modification to or deletion of a provision or part-provision under this clause shall not affect the validity and enforceability of the rest of this Agreement.

10.6. Notices: Any notice given to a party under or in connection with this Agreement shall be in writing and shall be delivered by hand, sent by pre-paid first-class post or other next working day delivery service, or sent by email to the address specified in the service agreement.

10.7. Third Party Rights: Unless it expressly states otherwise, this Agreement does not give rise to any rights under the Contracts (Rights of Third Parties) Act 1999 to enforce any term of this Agreement.

10.8. Force Majeure: Neither party shall be in breach of this Agreement nor liable for delay in performing, or failure to perform, any of its obligations under this Agreement if such delay or failure results from events, circumstances, or causes beyond its reasonable control.