Lanmark Managed Cyber Security Services Terms of Service

VERSION 1.1

Document Control

Document Reference	Lanmark Managed Cyber Security Services Terms of Service		
Document Version	1.1		
Document Date	February 2025		
Revision History	Date	Version	Reason
	02/02/25	1-0	Document Published
	10/02/25	1-1	Document Revised

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

Identity Threat Detection and Response (ITDR-as-a-Service)

Managed SIEM

Lanmark Managed Cyber Security Services Terms of Service

1. Introduction

1.1 Overview

These Lanmark Managed Cyber Security Services Terms of Service ("**Managed Cyber Security Services Terms**") describe the terms and conditions under which Lanmark Limited ("**Lanmark**," "**we**," or "**us**") provides its Managed Cyber Security Services to you (the "**Client**"). These Managed Cyber Security Services Terms apply to Lanmark's use of one or more third-party cyber security service providers (collectively referred to as "**Third-Party Service Provider**") in order to deliver the Managed Cyber Security Services.

These Managed Cyber Security Services Terms are in addition to, and governed by, Lanmark's Master Services Agreement and General Terms of Business located at [**https://www.lanmark.com/terms-of-business**] ("**MSA**").

Definitions and interpretation:

1. Except as defined in these Managed Cyber Security 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 Managed Cyber Security 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 Managed Cyber Security Services Terms shall take precedence over the MSA.

1.2 Related Documents

In addition to these Managed Cyber Security Services Terms and the MSA, the following documents form part of the agreement between the Parties regarding Lanmark's Managed Cyber Security Services:

- **Third-Party Service Provider Terms of Service** (the "**Third-Party TOS**"), which set out the terms and conditions applicable to the Third-Party Service Provider's software, platform, or security services.
- **Third-Party Cyber Security Services – Access and Permission Explanation and Requirements** (the "**Third-Party Access Requirements**") document, which explains the permissions required when deploying the Third-Party Service Provider's services and the associated risks and responsibilities.

Should any conflict arise between these Managed Cyber Security Services Terms, the MSA, or other documents, the order of precedence shall be: (1) these Managed Cyber Security Services Terms; (2) the MSA; (3) any other referenced documents.

1.3 Definitions

Capitalised terms not defined herein shall have the meanings given to them in the MSA or in the Third-Party TOS.

2. Scope of Services

2.1 Managed Cyber Security Services

Lanmark's Managed Cyber Security Services combine multiple capabilities—such as **MDR-as-a-Service** (Managed Detection and Response), **ITDR-as-a-Service** (Identity Threat Detection and Response), and **Managed SIEM**—to deliver continuous, real-time monitoring of your users, network, and endpoints. This unified approach helps ensure early detection of malicious activities, reduces threat dwell time, and enables swift incident response. Below is an overview of each component:

- **MDR-as-a-Service**
    - **Comprehensive Endpoint Security**: Advanced threat detection technologies, expert human analysts, and incident response capabilities safeguard endpoint devices.
    - **Proactive Threat Detection**: Alerts generated by Endpoint Detection and Response ("EDR") tools are automatically prioritised. SOC analysts apply threat intelligence and machine learning to validate and act on potential threats.
    - **Incident Response & Remediation**: When a threat is confirmed, our analysts rapidly contain and remediate the incident, minimising potential disruption.
- **ITDR-as-a-Service**
    - **Real-Time Monitoring of User Activities**: Entra (or relevant directory) events and user behaviour are continuously monitored to identify risky or abnormal sign-ins.
    - **Core Identity Threats Detected**:
        1. Credential Theft
        2. Session Hijacking
        3. Location-Based Anomalies
        4. Privilege Escalation
        5. Malicious Inbox & Forwarding Rules
    - **Immediate Response**: Suspicious identity-based activity triggers alerts to our SOC analysts, who investigate root causes and coordinate corrective measures.
- **Managed SIEM**
    - **Centralised Logging & Correlation**: Network activity, firewall logs, and other security events are centralised in a SIEM solution for real-time analysis.
    - **Intelligent Alerting**: Potential anomalies or breaches generate alerts for SOC analysts.
    - **Swift Investigations**: SOC analysts triage these alerts and take action (or guide the Client's team) to mitigate risk across the Client's environment.
- **24/7 Real-Time Monitoring**
    - **Continuous Visibility & Reduced Dwell Time**: Our SOC coverage minimises the time between initial compromise and detection.

- **Expert Oversight**: Although we use automation and machine learning, skilled security analysts remain actively involved in threat hunting, investigations, and remediation.

2.2 Use of Third-Party Software

Lanmark utilises one or more Third-Party Service Providers to deliver some or all of the Managed Cyber Security Services. The Client acknowledges that each Third-Party Service Provider operates independently, and the Third-Party TOS, as well as the Third-Party Access Requirements document, govern aspects of the Third-Party Service Provider's software, data processing, and responsibilities.

2.3 References to Policies and Documentation

Technical details about how elevated permissions or access rights are granted and used by any Third-Party Service Provider appear in the Third-Party Access Requirements document. The Client is responsible for reviewing that document to understand the specific permissions and associated risks.

---

3. Client Responsibilities

3.1 Collaboration and Timely Information

- The Client shall provide Lanmark with the necessary technical information, system access, and reasonable assistance to enable the successful deployment and ongoing management of the Managed Cyber Security Services.
- The Client must ensure that all relevant IT systems (servers, endpoints, software, cloud services, etc.) are adequately licensed, patched, and maintained.

3.2 Granting of Permissions

- By authorising and installing any Third-Party Service Provider's software or applications within the Client's Microsoft 365, Azure Active Directory environment, or on any systems, the Client agrees to grant Lanmark and the Third-Party Service Provider such permissions as are reasonably required to perform the Managed Cyber Security Services.
- The Client acknowledges that elevated or administrative permissions, while essential for effective threat detection, carry inherent risks if misused or compromised. The Client agrees that it has reviewed and will abide by the Third-Party Access Requirements document.

3.3 Data Backups

- The Client retains responsibility for maintaining complete backups of all systems, applications, and data. Lanmark's Managed Cyber Security Services do not include long-term data backup or archival unless explicitly agreed upon in writing.

---

4. Relationship with Third-Party Service Provider

4.1 Independent Providers

- Each Third-Party Service Provider is an independent vendor integrated by Lanmark to deliver Managed Cyber Security Services.
- Lanmark does not own, manage, or control any Third-Party Service Provider's internal operations, software development, or personnel.

4.2 Third-Party TOS

- The Client acknowledges that each Third-Party Service Provider's TOS applies to that provider's software and cloud services operating in the Client's environment.
- To the extent the Third-Party TOS imposes obligations on the Client (e.g., compliance with relevant laws or acceptable usage terms), the Client agrees to honour those obligations.

4.3 No Warranties by Lanmark for Third-Party Service Provider

- Lanmark makes no additional warranties, representations, or guarantees regarding any Third-Party Service Provider's software or platform beyond what is stated in that provider's TOS.
- Any claims or issues arising specifically from the Third-Party Service Provider's software performance, design, or reliability are governed by the Third-Party TOS.

---

5. Fees and Payment

5.1 Service Fees

- Fees for Managed Cyber Security Services, including licensing or subscription costs charged by the Third-Party Service Provider, will be set out in an Order Form or Quote and are subject to the MSA's payment terms.
- If the number of protected endpoints or users grows, Lanmark may adjust the fees accordingly, in line with the Third-Party Service Provider's pricing policies.

5.2 Price Adjustments

- If a Third-Party Service Provider changes its fees or usage tiers, Lanmark reserves the right to pass on these changes to the Client upon written notice, consistent with the MSA or the applicable Order Form.

---

6. "Hold Harmless" and Indemnification for Third-Party Provider Activities

6.1 Third-Party Access and Risks

The Client understands and accepts that granting administrative or elevated permissions to a Third-Party Service Provider creates a risk that such permissions could be misused, or be compromised through a security breach.

6.2 Hold Harmless Clause

By authorising and installing the Third-Party Service Provider's application(s) or software within your Microsoft 365, Azure Active Directory environment, or other systems, you acknowledge that Lanmark Limited is not responsible for any actions taken by the Third-Party Service Provider or its representatives, whether inadvertent or otherwise, nor for any resulting data loss or disruption. You agree to indemnify and hold

Lanmark harmless against any claims arising out of or related to the Third-Party Service Provider's use or misuse of the granted permissions, unless such claims result solely from Lanmark's gross negligence or wilful misconduct.

6.3 Limitation of Liability

- Except as required by law or otherwise stated in these Managed Cyber Security Services Terms, Lanmark's liability for any security incident, service interruption, or damages arising from or related to the Managed Cyber Security Services, including the Third-Party Service Provider's software, remains subject to the limitations and exclusions in the MSA.

6.4 Client's Additional Indemnification Obligations

- The Client shall defend, indemnify, and hold Lanmark harmless from and against any claims, liabilities, losses, or damages (including reasonable legal fees) arising out of:

    1. The Client's failure to implement or observe recommended security protocols.
    2. The Client's misuse or misconfiguration of any Third-Party Service Provider's software.
    3. Any claims that the Client's data or systems infringe or violate the rights of third parties when transmitted through or stored by the Third-Party Service Provider.

---

7. Disclaimers and Warranty Limitations

7.1 No Guarantee of Comprehensive Security

- Lanmark's Managed Cyber Security Services aim to reduce, not eliminate, security risks. No service can guarantee total protection or detect every possible threat.
- Lanmark disclaims any warranty of uninterrupted or error-free operation of the Managed Cyber Security Services.

7.2 Third-Party Service Provider Software "As Is"

- The Client recognises that each Third-Party Service Provider's software or platform is provided "as is," subject to that provider's own disclaimers as stated in its TOS. Lanmark does not guarantee that the Third-Party Service Provider's software will be free of vulnerabilities or immune from malicious attacks.

7.3 Applicable Law

- All implied warranties and conditions not expressly stated herein are disclaimed to the maximum extent allowed under applicable law.

---

8. Confidentiality and Data Security

8.1 Client Data

- As between the Client and Lanmark, the Client retains ownership of its data. Lanmark will only use such data as necessary to provide the Managed Cyber Security Services and fulfil its obligations under these Managed Cyber Security Services Terms and the MSA.

8.2 Confidential Information

- Each Party shall treat any Confidential Information from the other Party in accordance with the MSA. This applies to any data or logs the Client provides to Lanmark or to any Third-Party Service Provider.

8.3 Data Protection

- Lanmark and any Third-Party Service Provider will implement administrative, physical, and technical safeguards to help protect the confidentiality, integrity, and availability of Client data. Specific measures or certifications (e.g., SOC 2) may be documented in the Third-Party Access Requirements or the Third-Party TOS.

---

9. Term and Termination

9.1 Term

- These Managed Cyber Security Services Terms are effective upon the Client's acceptance (e.g., signature, click-through, or reference in a purchase order) and continue for the duration stated in the Managed Cyber Security Services subscription or agreement.

9.2 Termination Rights

- Either Party may terminate these Managed Cyber Security Services in accordance with the MSA, for example, due to material breach or insolvency.
- Lanmark may suspend or terminate the Managed Cyber Security Services if the relevant Third-Party Service Provider discontinues or materially modifies its services.

9.3 Consequences of Termination

- The Client must promptly remove the Third-Party Service Provider's software from its systems (unless otherwise agreed).
- Lanmark will cease any monitoring or response activities under these Managed Cyber Security Services Terms.
- Any Client data will be returned or deleted according to the data retention and deletion schedule set forth in the MSA or any relevant agreements.

---

10. General Provisions

10.1 Entire Agreement

These Managed Cyber Security Services Terms, together with the MSA, the Third-Party TOS, the Third-Party Access Requirements, and any other referenced documents, constitute the complete and exclusive agreement between Lanmark and the Client for Managed Cyber Security Services. They supersede all prior or contemporaneous agreements or understandings, whether written or oral, regarding the subject matter herein.

10.2 Governing Law and Jurisdiction

These Managed Cyber Security Services Terms are governed by and interpreted under the laws and jurisdiction provisions outlined in the MSA.

10.3 Severability

If any provision of these Managed Cyber Security Services Terms is deemed invalid or unenforceable, the remainder of the provisions shall remain in force.

10.4 No Third-Party Beneficiaries

Nothing in these Managed Cyber Security Services Terms shall be construed to grant rights to, or create obligations in, any party other than Lanmark and the Client.

10.5 Changes to These Terms

Lanmark may update these Managed Cyber Security Services Terms from time to time, subject to any notice requirements outlined in the MSA. Continued use of the Managed Cyber Security Services after updated terms become effective constitutes acceptance of the revised terms.

IN WITNESS WHEREOF, the Parties have caused these Managed Cyber Security Services Terms to be duly executed by their authorised representatives.

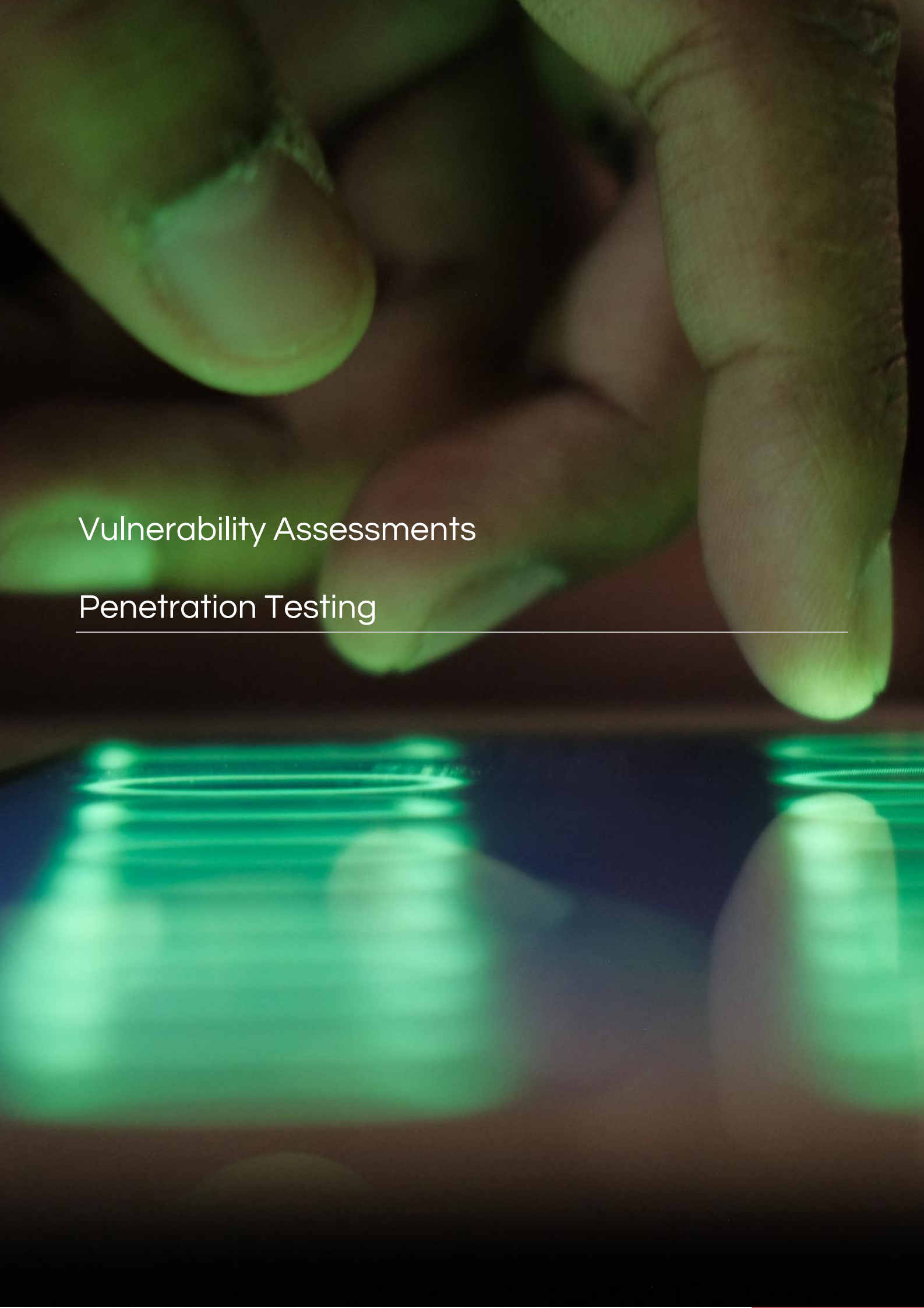
---

11. Further Information

For additional details on the Third-Party Service Provider's data processing, terms of service, and security practices, please refer to:

- **Third-Party Service Provider Terms of Service** (as provided by Lanmark or directly by the Third-Party Service Provider)
- **Third-Party Cyber Security Services – Access and Permission Explanation and Requirements** (also provided by Lanmark)

If you have any questions about these Managed Cyber Security Services Terms, or if you wish to terminate, suspend, or modify your Managed Cyber Security Services, please contact your Lanmark account manager.



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.