onecom

PenX Service Terms

1 General

1.1 These Service Terms should be read in conjunction with the General Terms and the applicable Order Form.

2 Interpretation

2.1 Terms defined elsewhere in the Contract shall have the same meaning in these Service Terms. The following definition shall also apply:

Authorised Systems	the specific IP addresses, domains, hostnames, and applications: (a) defined and submitted by the Customer (or Onecom on the Customer's behalf) via the PenX Portal; or (b) where the PenX Portal is unavailable, as listed in a Security Authorisation Document
Deliverables	the reports, findings, and remediation guidance provided as part of the Services
PenX Portal	the online dashboard provided by Onecom or its suppliers to manage the Services, define technical scope, and access reports
Security Authorisation Document	any written or electronic form (other than the PenX Portal) signed by the Customer which defines the initial Authorised Systems and grants authority to perform the Services
Service Definition	the technical description of the PenX service tiers (including Foundation, Pro Security, or Advanced), specifications, and delivery targets, as published on Onecom's website or otherwise communicated to the Customer

2.2 The rules of interpretation set out in the General Terms shall apply to these Service Terms.

3 Authorisation & Scope

3.1 The Customer represents and warrants that it has the legal authority to grant Onecom (and its subcontractors) permission to conduct exploitative security testing against the Authorised Systems. This includes obtaining all necessary permissions from third-party owners or host providers (e.g. cloud or managed service providers).

3.2 The Customer shall provide the technical scope for the Services via the PenX Portal. Where the Customer provides scope via a Security Authorisation Document, those details may be migrated to the PenX Portal.

3.3 The Customer agrees that the entry of any IP address, domain, or application into the PenX Portal by its Authorised Contacts constitutes a formal instruction and authorisation to perform exploitative security testing against those assets.

3.4 The latest configuration of Authorised Systems submitted via the PenX Portal shall be deemed the definitive scope of the Services and shall supersede any previous written document. Onecom shall have no liability for testing assets incorrectly entered or omitted by the Customer.

3.5 The Customer shall indemnify and hold Onecom harmless against any claims, losses, or costs arising from testing conducted against assets where the Customer lacked proper legal authority or third-party consent.

4 Customer Operational Responsibilities

4.1 The Customer is solely responsible for ensuring that the Authorised Systems are technically accessible to the PenX platform, including the "whitelisting" of Onecom's source IP addresses within firewalls and other security controls.

4.2 It is a strict condition precedent to the provision of the Services that the Customer ensures adequate and verified system backups exist for all Authorised Systems prior to and during any testing activity. Onecom shall not be required to verify the existence of such backups and shall have no liability for any loss arising from the Customer's failure to maintain them.

4.3 The Services are provided on the assumption that no material changes are introduced to the Authorised Systems during a testing window. Onecom shall not be responsible for inconsistent results or system instability caused by modifications made by the Customer during the performance of the Services.

4.4 The Customer shall maintain the confidentiality of all PenX Portal credentials and ensure that Users use sufficiently strong passwords.

4.5 The Customer must notify Onecom via the PenX Portal (or in writing) of any specific periods where testing is prohibited.

5 Risk Management & Exclusion of Liability

5.1 The Customer acknowledges that the Services are exploitative by nature and are designed to simulate real-world attack techniques. The Customer understands and accepts that the performance of the Services carries an inherent risk of:

5.1.1 temporary performance degradation or "system noise";

5.1.2 system instability or "Denial of Service" events; and

5.1.3 unintended modification of system behaviour or data.

5.2 Notwithstanding the ‘Liability’ clause of the General Terms, Onecom shall have no liability (whether in contract, tort including negligence, or otherwise) for any adverse impact, system instability, corruption of data, or business interruption arising from the technical performance of the Services on the Authorised Systems.

5.3 Unless expressly stated in the Service Definition, the Services do not include:

5.3.1 remediation of identified vulnerabilities;

5.3.2 continuous or real-time monitoring; or

5.3.3 certification of compliance with any regulatory or legal framework.

5.4 The Customer acknowledges and accepts that:

5.4.1 the Services provide a "point-in-time" assessment based on the Authorised Systems and the specific testing period;

5.4.2 the Deliverables identify potential vulnerabilities but do not constitute an exhaustive list of all security risks. The absence of findings in a security report does not guarantee that the Authorised Systems are secure or free from all vulnerabilities;

5.4.3 the Services are preventative in nature. They do not constitute an incident response or breach response service, and the performance of the Services will not determine whether an active compromise or "backdoor" currently exists within the Customer’s environment; and

5.4.4 the Services are intended to supplement, not replace, a comprehensive information security programme.

5.5 The Customer agrees that the exclusions and limitations in this clause 5 and the ‘Liability’ clause of the General Terms are reasonable given the nature of the Services, and that Onecom has offered the Services at the agreed Charges on the basis of this allocation of risk.

6 Support & Reporting

6.1 Technical queries regarding the performance of a scan or portal access shall be triaged via Onecom's standard support channels and escalated to the PenX specialist team where required via a helpdesk-to-helpdesk model.

6.2 Onecom will provide a security report documenting findings and remediation guidance.

6.3 The Services and Deliverables shall be deemed accepted upon the earlier of:

6.3.1 delivery of the security report; or

6.3.2 the conclusion of the agreed testing window.

6.4 The Customer must notify Onecom in writing of any issues or queries regarding a report within 10 Business Days of delivery, failing which the report shall be deemed final.

6.5 All vulnerability findings and reports generated by the Services constitute Onecom's Confidential Information. Onecom and its suppliers shall use such data solely for the delivery of the Services and shall not disclose it to third parties without the Customer's consent, except as required by Applicable Law.

7 Data Retention & Deletion

7.1 Onecom shall ensure that security reports and associated vulnerability data are available to the Customer via the PenX Portal for the duration of the Contract and for a period of 30 days following the termination or expiry of the Services (the **Retention Period**). This is provided to enable the Customer to conduct historical comparative analysis and to download final Deliverables.

7.2 Upon the expiry of the Retention Period, Onecom and its suppliers shall be entitled to permanently and irretrievably delete all Customer data, findings, and evidence stored within the PenX Portal.

7.3 The Customer is solely responsible for downloading and archiving copies of its reports and findings prior to expiry of the Retention Period. Onecom shall have no liability for any loss of data resulting from the Customer's failure to archive its Deliverables prior to their deletion in accordance with this clause 7.

8 Intellectual Property & AI Protections

8.1 For the purposes of these Service Terms, "Software" includes all AI models, weights, inference engines, automated attack logic, and proprietary vulnerability libraries used to deliver the PenX Services.

8.2 The Customer acknowledges that the AI-driven methodologies and logic used by PenX constitute Confidential Information and Intellectual Property Rights of Onecom (or its suppliers). No rights are granted to the Customer to access the underlying models or logic.

8.3 The Deliverables are provided solely for the Customer's internal security remediation and risk management. The Customer shall not:

8.3.1 use the Deliverables (or any part thereof) as training data for any machine learning model or artificial intelligence system;

8.3.2 use the Services for the purposes of competitive benchmarking or reverse-engineering of the AI's attack logic;

8.3.3 publish, disclose, or distribute the Deliverables to any third party (other than the Customer's professional auditors or regulators) without Onecom's prior written consent; or

8.3.4 use any automated scripts or "scraping", "crawlers," or "spiders" to interrogate the PenX Portal or to harvest data regarding the AI's decision-making logic.

8.4 Any feedback, technical data, or "learning" generated through the Software's interaction with the Authorised Systems shall be owned exclusively by Onecom (or its suppliers). The Customer shall not attempt to create any derivative works based on the logic or outputs of the Services.

9 Acceptable Use & Reputational Risk

9.1 The Customer shall use the Services and the PenX Portal strictly in accordance with Onecom's Acceptable Use Policy. The Customer shall not use the Services to conduct unauthorised testing against third-party systems or for any other unlawful purpose.

9.2 Onecom may terminate or suspend the Services immediately where, in Onecom's reasonable opinion, the continued provision of Services to the Customer would expose Onecom or its suppliers to legal, regulatory, or reputational harm.

9.3 A breach of clause 3.1 (authority), clause 8 (intellectual property & AI protections), or clause 9.1 (acceptable use) shall be deemed a material breach of the Contract.