SERVICE TERMS

VERSION 1.0 · AUGUST 2026

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, specifications, and delivery targets, set out in Schedule 1 (PenX Service Definition), as updated by Onecom from time to time in accordance with clause 10

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:

(a) temporary performance degradation or "system noise";

(b) system instability or "Denial of Service" events; and

(c) 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:

(a) remediation of identified vulnerabilities;

(b) continuous or real-time monitoring; or

(c) certification of compliance with any regulatory or legal framework.

5.4 The Customer acknowledges and accepts that:

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

(b) 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;

(c) 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

(d) 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:

(a) delivery of the security report; or

(b) 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:

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

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

(c) 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

(d) 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.

10. Service Definition Updates

10.1 PenX is an evolving service. Onecom may, at its sole discretion, update or replace the Service Definition (including by adding, amending, or retiring PenX tiers or add-ons) at any time, by publishing the then-current version via the PenX Portal, Onecom's website, or such other location as Onecom may make available for that purpose.

10.2 An update or replacement of the Service Definition under this clause 10 shall take effect immediately upon publication. Onecom is not required to give the Customer prior notice of any such update.

SCHEDULE 1

PenX Service Definition

1. Purpose

This document is the Service Definition for the PenX service. It provides a technical description of the service tiers (Foundation, Pro Security, and Advanced), functionality, and delivery targets.

This Service Definition is for technical descriptive purposes and is incorporated by reference into the Contract via the Onecom PenX Service Terms.

For the avoidance of doubt, this Service Definition is subordinate to the legal terms of the Contract. In the event of any conflict or inconsistency between this document and any other document making up the Contract, the order of precedence set out in the General Terms shall apply, and the Order Form, the Onecom PenX Service Terms, and the General Terms shall each prevail over this Service Definition.

2. Overview of PenX

PenX is a managed security testing service designed to help Customers identify security weaknesses across authorised, internet-facing assets and to provide structured reporting with prioritised remediation recommendations.

PenX is a preventative security testing service; it is not an incident response, breach response, or monitoring service.

3. Scope of Testing

PenX testing is performed only against assets expressly authorised by the Customer via the PenX Portal or a Security Authorisation Document.

3.1 In-Scope (where authorised)

- Publicly routable IP addresses
- Domains and subdomains
- Web applications and URLs
- Other external-facing assets expressly listed in the Customer authorisation

3.2 Out-of-Scope (unless expressly agreed in writing)

- Internal/private networks
- Physical security testing
- Social engineering or phishing simulations
- Denial-of-service or stress testing
- Third-party systems not owned or controlled by the Customer
- Any assets not expressly included in the authorised scope

4. Customer Authorisation

Prior to any testing or scanning activity, the Customer must provide written authorisation confirming:

- Ownership or authority to test the assets
- The authorised testing window(s)
- A complete and accurate asset inventory
- Authorised Customer contacts

Authorisation will be captured via the PenX Portal or Security Authorisation Document. Onecom will not commence testing or scanning until valid authorisation is received.

5. PenX Packages

PenX is delivered in defined tiers. Specific pricing, minimum term, and add-ons are detailed in the Order Form.

5.1 PenX Basic

Intended for: All businesses

Includes:

- Scheduled testing frequency: Monthly
- Automated vulnerability scanning only on authorised scope
- Includes a report of identified vulnerabilities

5.2 Foundation (SMB baseline)

Intended for: Small and medium businesses.

Includes:

- Scheduled testing frequency: Quarterly
- Automated vulnerability scanning
- Penetration testing within the authorised scope
- PenX report including:
  - Executive summary
  - Risk ratings and prioritisation
  - Affected assets and evidence
  - Remediation recommendations
- Customer notifications (pre and post-test)

5.3 Pro Security

Includes:

- Scheduled testing frequency: Monthly
- All Foundation inclusions
- Eligibility for enhanced remediation support (where purchased)

5.4 Advanced (Enterprise Scope)

Includes:

- Scheduled testing frequency: Monthly
- Broader and/or more complex testing scope

The specific inclusions, scope, and limitations of the Advanced package shall be defined exclusively in the applicable Order Form. No services are included unless expressly stated.

5.5 PenX One-off Basic Vulnerability Scan

Intended for: Customers receiving a single, non-recurring scan under an individual Order, rather than a subscription package.

Includes:

- A single, non-recurring automated vulnerability scan (a “Soft vulnerability scan” for the purposes of section 7 below)
- Scope limited to up to 10 customer-nominated, internet-facing IP addresses and/or domains
- Automated scanning only; does not include exploitative penetration testing
- A vulnerability scan report including risk ratings and remediation recommendations, delivered in accordance with the targets in section 8

Excludes (unless separately purchased as an Add-On per section 10):

- Human validation of findings
- Scheduled or recurring testing
- Remediation support or retesting

6. Delivery Process

A typical PenX engagement follows these steps:

1. **Order:** Customer places an Order for PenX
2. **Authorisation:** Customer completes Security Authorisation Document or defines scope in the PenX portal and provides asset inventory
3. **Scheduling:** Testing schedule is agreed
4. **Pre-Test Notification:** Customer is notified of upcoming testing window (typically 7 days prior)
5. **Execution:** Testing is executed within the authorised window
6. **Validation:** Findings are human-validated where applicable
7. **Reporting:** Report is published and the Customer is notified
8. **Post-Test Notification:** Customer is notified of report availability

7. Validation of Findings

Human validation of findings is included for penetration testing activities prior to report release.

Soft vulnerability scans are automated in nature and do not include human validation.

8. Report Delivery Targets

Onecom aims to deliver the PenX report within 3-5 Business Days following completion of the authorised test.

Delivery times may vary depending on scope complexity, asset volume, and validation requirements.

9. Remediation Support and Retesting

9.1 Remediation Support

Where purchased as an add-on, Onecom provides a remote walkthrough of the report to explain findings and remediation options.

9.2 Retesting

Retesting of remediated findings is not included by default. It must be purchased as an add-on and is limited to the specific findings identified in the original report.

10. Add-On Services

The following add-ons may be available where stated in the Order Form:

- Additional IP addresses or assets
- Out-of-hours testing windows
- Report walkthrough or remediation consultation
- Targeted retesting
- One-off penetration testing