ONSECURITY
SERVICE SCHEDULES

SCHEDULE 1 - SECURITY TESTING SCHEDULE

Applies where an Order includes penetration testing, vulnerability testing, red teaming, retesting, continuous security testing or another activity involving authorised access to or assessment of a Target.

1. Authority to test. The Customer expressly authorises OnSecurity, its Affiliates, personnel and authorised contractors to access, interact with, scan, probe, assess and test the authorised Targets to the extent reasonably required for the ordered Services. The authority is intended to constitute consent and authorisation for the purposes of the Computer Misuse Act 1990 and analogous laws that would otherwise prohibit the authorised activity.
2. Customer authority and third-party permissions. The Customer warrants that it owns the Targets or has authority from the relevant owner or operator to authorise the Services and has obtained all required consents, provider notifications and permissions from hosting providers, cloud providers, ISPs, software vendors or other affected third parties. For phishing, social engineering, monitoring or physical testing, the Customer is also responsible for any required internal approvals, employee or individual notices, lawful basis and consultation processes. OnSecurity may request reasonable evidence of authority and may refuse or suspend testing where it reasonably doubts that authority.
3. Targets. A Target is authorised only when identified with sufficient specificity through the Order, Platform or another written method accepted by OnSecurity. The Customer is responsible for the accuracy of Target details and must promptly remove or correct a Target it is no longer authorised to test.
4. Standing authorisation and continuous Services. A penetration test or assessment is point-in-time unless the Order or Service Description expressly identifies it as recurring or continuous. An Order may give standing authorisation for recurring, multi-test or continuous testing during the Order term, allowing OnSecurity to perform the authorised activities against enabled Targets without a new contract for each test, subject to applicable Testing Windows, blackout periods, rate limits, exclusions and stop procedures.
5. Testing Windows, Normal Testing Hours and continuous activity. A Testing Window may be set in the Order or later through the Platform, email or another retained written communication by an authorised Customer contact. Positive enablement or approval through the Platform may constitute written authorisation. Unless otherwise agreed, manual penetration testing is performed during Normal Testing Hours of 07:00 to 19:00 UK local time (GMT or BST, as applicable) on a Business Day. Where an Order permits continuous or recurring activity, the Customer is responsible for notifying OnSecurity in advance of critical business periods or blackout periods during which specified testing should not occur. Automated scanning, discovery and other automated activity may operate continuously 24 hours a day, seven days a week, subject to Platform and Service availability and any agreed exclusions or rate limits.
6. High-impact testing. Denial-of-service, availability, stress, destructive, physical or other high-impact testing is excluded unless expressly identified and separately authorised in writing. Where authorised, the parties may agree additional safeguards such as specific windows, rate or bandwidth limits, excluded systems, emergency-stop contacts and required third-party notifications.
7. Testing methods, automation and AI. OnSecurity may select and change reasonable testing tools, techniques and delivery methods, including manual testing, proprietary automation and AI-assisted workflows, provided it remains within the authorised scope and complies with the Agreement.
8. Emergency stop. The Customer may issue an emergency stop instruction using the agreed contact route. OnSecurity will use reasonable efforts to cease affected active testing as soon as practicable after receipt and verification. A stop instruction does not entitle the Customer to a refund for work already performed, reserved resources or non-cancellable third-party costs.
9. Estimates and additional time. Where clause 2.8 of the Master Terms applies to testing estimated by hours or days, the Customer may authorise additional time or ask OnSecurity to stop at the purchased limit. If the Customer asks OnSecurity to stop at the limit, OnSecurity gives no assurance in respect of untested scope and may issue a partial or qualified report.
10. Findings and severity. OnSecurity will assess findings using its then-current methodology, which may include current CVSS methodology together with contextual threat, exploitability, environmental and business-risk factors. A severity rating communicates OnSecurity's professional assessment at the time and is not a guarantee of business impact or future exploitability.
11. Critical findings. During active testing, OnSecurity will use reasonable efforts to notify the Customer promptly through the agreed channel of a finding classified by OnSecurity as Critical where OnSecurity reasonably considers it creates an immediate and material risk of compromise or material operational, financial or reputational harm.

12. Reports, retesting and remediation validation. Any output identified as draft, preliminary or interim may change and must not be relied on as a final Deliverable. A final report or finding may be shared confidentially as permitted by the Master Terms but must not be published, used in marketing or presented as an OnSecurity certification or endorsement without OnSecurity's prior written consent. Where retesting is available, the Customer may request remediation validation against findings from the original authorised scope during the 60-day period after the initial Testing Window unless the Order or Service Description states otherwise. The Order or Service Description will state whether retesting is included or consumes additional Capacity. Retesting is limited to verifying remediation of original-scope findings unless the parties agree expanded scope.
13. Postponement, cancellation and Service Balance. Unless an Order states otherwise, a booked test cannot be cancelled for a cash refund once the Order has been accepted. OnSecurity may permit postponement or rescheduling subject to resource availability. Where unused prepaid testing Fees or Capacity are retained as a Service Balance, they are subject to the expiry, drawdown and other rules stated in the Order or Platform & Subscription Schedule and have no cash redemption value unless the Agreement expressly provides otherwise. The Customer remains liable for committed third-party costs or reserved resources that cannot reasonably be avoided.
14. Testing risk and Customer resilience. The Customer acknowledges that authorised security testing can cause interruption, degradation, account lockout, alerting, data change or other effects. The Customer will ensure appropriate internal stakeholders, SOC teams and affected third parties are informed where required. OnSecurity will use reasonable care to avoid unnecessary impact but does not guarantee testing will be risk-free.
15. Open-source and third-party intelligence. Where an ordered Service includes open-source intelligence, credential-exposure, threat-intelligence or similar searches, OnSecurity may search and present lawfully available or licensed third-party information relating to enabled Targets. OnSecurity does not control the underlying third-party source and cannot amend, suppress or remove information held there. Results may include historic, duplicated, stale or previously known information, including old credentials or passwords, and do not by themselves establish that a credential remains valid or that a current compromise exists.
16. Testing limitations. Findings reflect the authorised scope, conditions, credentials and information available at the time. OnSecurity does not guarantee identification of every vulnerability, including unknown vulnerabilities or those detectable only through different credentials, attack paths, tools, timing or methods.
17. Incorrect or unauthorised Targets

17.1 Unless otherwise expressly agreed, OnSecurity may rely on Target details and authority provided or confirmed by or on behalf of the Customer and is not required independently to verify ownership of, or authority over, a Target or scope.

17.2 If OnSecurity becomes aware, or is notified, that a Target may have been identified incorrectly, is not authorised for testing or that testing has affected a system or third party outside the authorised scope, OnSecurity will as soon as reasonably practicable:

(a) stop the affected testing;

(b) notify the Customer;

(c) take reasonable steps within its control to avoid further impact; and

(d) reasonably cooperate with the Customer to assess what has occurred and, where reasonably practicable and using commercially reasonable endeavours, identify the cause and any appropriate mitigation and remediation.

OnSecurity's cooperation under this paragraph does not transfer responsibility for the incorrect or unauthorised Target to OnSecurity or constitute an admission of liability.