ONSECURITY
SERVICE SCHEDULES

SCHEDULE 2 - PLATFORM & SUBSCRIPTION SCHEDULE

Applies where an Order includes Platform access, prepaid or committed testing capacity, customer-facing tooling, continuous asset discovery, configurable runtime, support or another recurring Service.

Definitions:

Cash Balance: an accounting credit on the Customer's Platform account representing prepaid amounts available for eligible Services under clause 2.5; it is not cash held on trust, stored value or electronic money and has no cash redemption value except where the Agreement requires a refund.

Service Balance: the Platform record of prepaid or committed Capacity available to the Customer, denominated in money, hours, Usage Units or another metric specified in the Order or Service Document.

Usage Unit: a contractual unit used to measure or consume Services from a Service Balance; it is not money, stored value or electronic money, is non-transferable except as the Agreement permits and has no cash redemption value.

1. Subscription term and Capacity. The Order will state the Initial Term, Platform or software Fees, billing frequency and any testing hours, Services, Cash Balance, Usage Units, credits or other Capacity purchased.
2. Cash Balance, Service Balance and Usage Units. Under the current model, amounts paid for eligible testing or Services may be credited to the Customer account as a Cash Balance and charges for Services drawn down from that balance. Unless the Order states otherwise, unused Cash Balance remains available for 12 months from the date the relevant amount is credited or purchased; OnSecurity may apply the oldest available balance first; and any unused Cash Balance then expires and is non-refundable. OnSecurity may also record testing hours, Usage Units, credits or other Capacity as part of the Service Balance. The Platform may show the amount of Capacity a Service will consume before the Customer confirms a booking or action.
3. Subscription billing. Unless the Order states otherwise, Platform Fees and subscription Fees are invoiced in advance in accordance with the billing frequency in the Order. Usage, overage, additional testing, drill-down hours, licences, third-party charges or other consumption-based amounts may be invoiced separately when incurred or reserved.
4. Annual allocations and accelerated consumption. Where a multi-year Order allocates committed Capacity to each 12-month period of the term (each a Contract Year), the Customer may consume only the allocation invoiced for the then-current Contract Year without accelerating payment. If the Customer consumes more than that allocation, OnSecurity may invoice the corresponding future committed Capacity immediately and reduce the later scheduled invoice by the same amount so the Customer is not charged twice. OnSecurity may suspend further use above the current-year allocation until that accelerated-use invoice is paid.
5. Overage. Capacity used beyond the total amount committed under the Order is additional usage and may be charged at the overage rate stated in the Order or, if none is stated, the rate displayed in the Platform or OnSecurity's then-current standard rate when the additional usage is confirmed.
6. Renewal. Unless an Order expressly states that a subscription does not renew automatically, it renews after the Initial Term for successive 12-month Renewal Terms. Either party may prevent renewal by giving at least 30 days' notice before the end of the then-current term, or any different notice period stated in the Order. A Customer may give notice at any time during a term for termination to take effect at the end of that term.
7. Capacity expiry and rollover. Cash Balance is subject to the 12-month expiry rule in paragraph 2 unless the Order states otherwise. Other unused Capacity expires at the end of the applicable allocation or term unless the Order expressly permits limited rollover. Any rollover, bonus Capacity or promotional Capacity is subject to the limits and expiry stated in the Order or Platform and does not roll indefinitely.
8. Platform access and Users. The Customer may permit authorised Users to access the Platform within the user, asset or usage limits in the Order.
9. Portal availability and automated Services. OnSecurity will use commercially reasonable endeavours to make the Platform available 24 hours a day, seven days a week, but does not guarantee uninterrupted or error-free availability. Planned or emergency maintenance, security events, internet or communications failures, Customer dependencies, third-party dependencies and Force Majeure Events may affect availability. Automated scanning or monitoring is continuous only where the Order or Service Description expressly says so and may then run 24/7 where enabled, subject to those availability limitations and any Service-specific exclusions. Platform access alone does not create a continuous-monitoring obligation.
10. Maintenance, product evolution and third-party tools. OnSecurity may maintain, patch, upgrade, modify and improve the Platform and may add, remove or replace features in accordance with clause 3 of the Master Terms. OnSecurity may

change internal or third-party tools, products, licences, APIs and AI services underlying a customer-facing Service without separately identifying every tool in an Order, and may flow down necessary licence or usage restrictions under clause 6 of the Master Terms.

11. Support and service commitments. Standard support and operational commitments are those described in the applicable Service Description or Order.

12. Customer configuration and integrations. Where the Customer can configure assets, Targets, tools, integrations, AI agents or third-party systems, the Customer is responsible for its configuration choices and for having rights and permissions required for connected systems and data. OnSecurity is not responsible for failures caused by a Customer-selected or Customer-controlled integration or configuration except to the extent caused by OnSecurity's material breach of the Agreement.

13. Data export, switching and exit. Subject to paragraph 14 where applicable, on expiry or termination OnSecurity will make Customer Data reasonably exportable through available Platform functionality or another reasonable method, subject to the Agreement, applicable retention rules and third-party restrictions. OnSecurity is not required to disclose proprietary software, algorithms, security-sensitive material, internal service data or third-party material beyond what applicable law requires.

14. EU Data Act. To the extent Chapter VI of Regulation (EU) 2023/2854 (Data Act) mandatorily applies to an ordered data processing service supplied to a Customer in the European Union: (a) the Customer may, on no more than two months' notice, request switching to another provider, porting of exportable data and digital assets to on-premises infrastructure, or erasure; (b) OnSecurity will provide the reasonable assistance and service continuity required by applicable law during the switching process, with a standard transitional period not exceeding 30 calendar days. The Customer may extend that period once as permitted by the Data Act. If 30 days is technically unfeasible, OnSecurity will notify the Customer within 14 working days of the switching request, explain why and identify an alternative transitional period not exceeding seven months; (c) OnSecurity will provide a retrieval period of at least 30 calendar days after the transition and will erase exportable data and digital assets after the applicable retrieval period where required by law and the switching process has completed; (d) OnSecurity's Data Portability & Exit Guide and associated online register will identify the categories of exportable data and digital assets, any excluded internal-functioning data protected by Intellectual Property Rights or trade secrets, available switching procedures, formats and interfaces (including relevant APIs), and known restrictions or technical limitations; (e) any switching charge will not exceed the amount permitted by applicable law and no switching charge will be imposed where prohibited. Separately requested assistance going beyond OnSecurity's mandatory switching obligations may be charged if agreed in advance; and (f) OnSecurity will publish and identify in the Agreement the webpage required by Article 28 of the Data Act describing the jurisdictions applicable to relevant ICT infrastructure and the general measures used to protect EU-held non-personal data against conflicting third-country governmental access or transfer. This paragraph applies only to the in-scope data-processing-service component of an Order and does not by itself extend those rights to separate professional services. Standard service fees and any lawful Early Termination Charge remain payable except to the extent mandatory law requires otherwise.