ONSECURITY CUSTOMER AGREEMENT

Supplier	OnSecurity Technology Limited
Company number	14184026
Registered office	1 Victoria Street, Bristol, England, BS1 6AA

1. The Agreement, acceptance and contract hierarchy

1.1 The agreement between OnSecurity and the Customer (Agreement) comprises, as applicable: (a) these Master Terms; (b) each Order accepted by OnSecurity; (c) each applicable Service Schedule; (d) each Service Document expressly incorporated by the Master Terms, a Service Schedule or an Order; and (e) any separate Data Processing Addendum expressly agreed to apply.

1.2 These Master Terms may be accepted through the Platform or another electronic or signed process. Acceptance of an Order also confirms the then-current Master Terms and incorporated documents presented or linked with it.

1.3 Each Order forms a separate contract under these Master Terms. Ending one Order does not automatically end another Order or the Agreement.

1.4 The Customer confirms that anyone who accepts the Agreement, places or changes an Order, administers its account or gives testing authority on its behalf is authorised to do so. OnSecurity may rely on a User or other person reasonably appearing to have that authority unless notified otherwise in advance.

1.5 OnSecurity may retain, and rely on as evidence of acceptance and authority, reliable electronic records of contract formation, including the accepting User, date and time, Order, Agreement version and linked documents.

1.6 If documents forming the Agreement conflict, the following order of precedence applies: (a) the Order, for the commercial and service-specific matters it records; (b) the applicable Service Schedule; (c) these Master Terms; and (d) incorporated Service Documents. An Order varies a legal provision of these Master Terms only if it expressly identifies the provision being varied.

1.7 Customer purchase orders, procurement or onboarding terms, policies and other Customer terms do not amend the Agreement unless OnSecurity expressly agrees in writing.

1.8 The Trust Centre, Privacy Notices, marketing materials, proposals, questionnaires and other pre-contract information are for information, assurance or due diligence only and do not create contractual warranties, Service Levels or obligations unless expressly incorporated into the Agreement.

2. Orders and provision of Services

2.1 **Request for Quote.** Information submitted in a request for quote, whether through the Platform quoting journey or an offline, bespoke or other agreed process, is preliminary and is not an Order or commitment by OnSecurity.

2.2 **Quote.** OnSecurity may review, clarify or adjust submitted information before issuing a Quote through the Platform, by email, in an order form or statement of work, or by another written method accepted by OnSecurity.

2.3 **Order acceptance.** The Customer may accept a Quote through the Platform, electronic signature, an offline signed document or another method identified by OnSecurity. The accepted Quote, together with the applicable Agreement documents, becomes the Order. Unless stated otherwise, a Quote may be accepted only during its stated validity period.

2.4 **Scope and operational details.** User numbers, Targets, Testing Windows and other operational details may be updated where the Service permits. An operational update does not change committed Fees or materially expand contracted scope unless agreed by the parties. An administrative edit by OnSecurity does not itself authorise testing of a new or materially changed Target.

2.5 **Cash Balance, Service Balance and Capacity.** Amounts paid for eligible Services may be credited to the Customer's account as a Cash Balance and drawn down as Services are used. Cash Balance, Service Balance, Usage Units and other Capacity are measured, used, expire and roll over as set out in the Platform & Subscription Schedule and the Order.

2.6 OnSecurity is not required to provide a Service until the Order is accepted and relevant Customer prerequisites are satisfied. Once accepted, an Order cannot be cancelled, reduced or rescheduled except as the Agreement or Order permits or OnSecurity agrees.

2.7 Unless an Order expressly states otherwise, time is not of the essence and dates, hours, effort, completion times and resource requirements are estimates and are not fixed prices, guaranteed dates or Service Levels. Fees for time-based Services are charged on actual time used, up to any limit in the Order.

2.8 If OnSecurity reasonably expects an estimate to be exceeded, it may notify the Customer and seek approval for additional scope, time or Fees. OnSecurity may pause affected work while awaiting a decision, and work already performed and committed third-party or resource costs remain payable.

2.9 A Customer-requested change is binding only when OnSecurity accepts it through the Platform, an updated Quote or Order, change confirmation or another written record. OnSecurity may adjust scope, dates, Capacity and Fees to reflect the change.

2.10 If the Customer asks OnSecurity to begin urgent work before an Order or change is documented, OnSecurity may do so in good faith and the Customer will pay the notified Fees or rates or, if none were notified, OnSecurity's then-current standard rates.

2.11 OnSecurity may provide Services through Affiliates, personnel, contractors, licensors, cloud providers and other Service Providers. OnSecurity remains responsible for its contractual obligations except where the Agreement identifies a third-party product or service as supplied on direct or pass-through terms.

2.12 If a Service or material third-party dependency is discontinued, materially changed or unavailable, OnSecurity may replace it with substantially equivalent or better functionality or delivery arrangements, and will give the Customer reasonable notice of a replacement that materially affects the Service where practicable, which may be given under clause 18.4(c). If no reasonable replacement is available, OnSecurity may discontinue the affected Service under clause 16.6, with a refund of prepaid Fees for the unused period under that clause as the Customer's sole remedy.

3. Changes to the Agreement and Services

3.1 OnSecurity may change the Agreement (including Service Schedules, Service Descriptions and Service Documents) and the Services where reasonably necessary for operational, legal, regulatory, security, technical or commercial reasons, including changes to technology, delivery methods or Service Providers. A change cannot alter Fees already committed under an accepted fixed-price or fixed-term Order; clause 7 governs Fees.

3.2 OnSecurity will make a change by publishing it at Legal & Trust Centre or another notified location, and may offer alerts for changes. The change takes effect on the date stated in the publication which is a notice under clause 18.4(c). The Customer should check the Legal & Trust Centre regularly and keep its account and contact details up to date.

3.3 If a change materially and adversely reduces the core functionality of an active Service, the Customer may object within 30 days of publication. The parties will work together reasonably to address the impact. If there is no reasonable solution, the Customer may terminate only the affected Service from the change's effective date, without an Early Termination Charge. This right does not apply where the change: (a) is required by law or a competent authority; (b) is reasonably necessary to address a material security risk; or (c) results from a third-party withdrawal or change, and OnSecurity provides a materially equivalent alternative where reasonably practicable.

4. OnSecurity commitments

4.1 OnSecurity will provide the Services with reasonable care and skill, consistent with standards generally expected of providers of similar services, and in material accordance with the applicable Order and Service Schedule.

4.2 OnSecurity will maintain the licences, permissions and authorisations required to perform its obligations and comply with laws applicable to it as supplier of the Services.

4.3 OnSecurity may improve, automate, reconfigure or otherwise change its tools, techniques, methods, personnel and Service Providers, provided it continues to comply with the Agreement.

4.4 Platform availability, testing hours, automated scanning, retesting and other service-specific commitments are set out in the applicable Service Schedule, Service Description or Order.

4.5 If the Customer believes there has been a material failure to comply with clause 4.1, it must notify OnSecurity in writing, with reasonable detail, within 60 days of delivery. The Customer must give OnSecurity the access and information it reasonably needs, and a reasonable opportunity to correct or re-perform the affected Service or Deliverable, which OnSecurity will use reasonable endeavours to do. If OnSecurity does not do so, it will refund the Fees paid for that Service or Deliverable. Subject to clause 14.3, this is the Customer's sole remedy for the failure. If OnSecurity does not correct, re-perform or refund as this clause requires, clause 16.4 applies.

4.6 OnSecurity may give reasonable directions about use of the Services where necessary for security, safety, service quality, other customers or OnSecurity's systems. The Customer will comply with those directions.

5. Customer obligations and dependencies

5.1 The Customer will promptly give OnSecurity, free of charge, the accurate and complete information, Customer Materials, access and cooperation (including decisions and approvals) that OnSecurity reasonably needs to provide the Services.

5.2 The Customer is responsible for:

(a) the lawfulness, accuracy and integrity of Customer Data, Customer Materials, instructions and Targets;

(b) obtaining all consents, licences and approvals (including from third parties) that the Services require; and

(c) complying with laws that apply to its business, systems and use of the Services.

The Security Testing Schedule sets out additional authority requirements for security testing.

5.3 The Customer will maintain appropriate backups, continuity and recovery arrangements, and the systems, networks and third-party services it needs to receive the Services. It is responsible for restoring its own systems and data.

5.4 The Customer is responsible for its Users' acts and omissions as if they were its own, and for User permissions and account administration. It will keep credentials secure (including using multi-factor authentication where OnSecurity requires it) and promptly remove access that is no longer needed.

5.5 The Customer will promptly notify OnSecurity of any actual or suspected unauthorised access, compromise or security incident affecting the Services, or any other circumstance likely to materially affect their delivery.

5.6 If the Customer, a User or anyone else for whom the Customer is responsible delays, prevents or increases the cost of OnSecurity's performance, then to the extent affected:

(a) OnSecurity is relieved of the corresponding obligation or Service Level;

(b) affected dates are reasonably extended; and

(c) OnSecurity may recover its reasonable additional costs, including wasted effort and remobilisation.

5.7 The Customer must not use the Services:

(a) unlawfully or in breach of third-party rights;

(b) to interfere with OnSecurity or any other customer; or

(c) contrary to OnSecurity's reasonable security or usage instructions.

6. Platform, software and third-party products

6.1 Where an Order includes Platform, software or hosted-service access, OnSecurity grants the Customer a non-exclusive, non-transferable right during the Order term for authorised Users to access and use it for the Customer's internal business purposes, subject to any user, asset, Capacity or usage limits in the Order.

6.2 The Customer must not: (a) reverse engineer, decompile or attempt to derive source code from the Platform; (b) use the Platform or Service Documents to build a competing service; (c) resell, sublicense or commercially exploit the Platform for third parties; (d) bypass technical restrictions; (e) introduce malicious code; or (f) interfere with the security, integrity or operation of the Services.

6.3 Services may use third-party products, licences, APIs, software, content or data sources. The Customer will comply with applicable third-party terms notified by OnSecurity or accepted by the Customer. A third-party product, integration or service separately selected or contracted by the Customer remains the Customer's responsibility unless the Order expressly says otherwise.

6.4 Trial Services. A free, proof-of-concept, preview, beta or trial Service (a "Trial Service") is provided "as is", may be changed, suspended or withdrawn at any time, and carries no Service Level unless the Order says otherwise. The Customer selects its Targets and must use a Trial Service only against non-production Targets. By enabling a Target, the Customer confirms that it is non-production and backed up. OnSecurity does not verify this, and the Customer bears the risk of testing any Target that is not. Subject to clause 14.3, OnSecurity gives no warranty, condition or representation for a Trial Service, is not liable for loss arising from testing a Target that was not non-production, and otherwise limits its total liability for a Trial Service to £100, which applies instead of clause 14.6.

7. Fees, invoicing and payment

7.1 Unless stated otherwise, Fees exclude VAT and other applicable sales taxes, which the Customer will pay at the prevailing rate against a valid VAT invoice where applicable.

7.2 Payment timing and billing structure are as stated in the Order. If the Order is silent, invoices are due within 30 days of the invoice date. OnSecurity may invoice Services separately. A purchase order is an administrative requirement only and does not delay payment.

7.3 OnSecurity may change its standard prices for future Orders at any time, and may revise recurring or subscription Fees for a Renewal Term by notice or publication before that Renewal Term.

7.4 The Customer must notify OnSecurity promptly of any good-faith invoice dispute, with reasonable details. The Customer must pay undisputed amounts and may not withhold unrelated Fees. OnSecurity will not suspend a Service for a genuinely disputed amount. Unresolved disputes are escalated under clause 18.10.

7.5 The Customer will pay Fees in full without set-off, counterclaim or deduction, and without withholding unless the law requires it. Where withholding is required and the Customer is outside the UK, the Customer will pay the additional amount needed so that OnSecurity receives what it would otherwise have received.

7.6 On overdue undisputed amounts, OnSecurity may charge interest, fixed compensation and reasonable recovery costs as permitted by the Late Payment of Commercial Debts (Interest) Act 1998.

7.7 If an undisputed amount remains overdue five Business Days after notice requiring payment, OnSecurity may suspend the affected Services or account access until payment is made, and may recover the reasonable third-party, reconnection, remobilisation and administrative costs of restoring them. Suspension does not waive payment obligations or extend a committed term.

7.8 Unless this Agreement, an Order or a Service Schedule states otherwise, prepaid Fees, committed subscription charges and unused Capacity are non-refundable.

8. Intellectual property and Deliverables

8.1 Each party retains ownership of Intellectual Property Rights it owned, licensed or developed independently of the Agreement. The Customer retains ownership of Customer Data, Customer Materials, Customer systems and Customer branding.

8.2 OnSecurity, its Affiliates, Service Providers and licensors retain all Intellectual Property Rights in the Services, Platform, software, Service Documents, methodologies, tools, templates, know-how, processes, models, automation and generic materials, including developments and improvements created in providing the Services.

8.3 Subject to payment of the applicable Fees, OnSecurity grants the Customer a perpetual, non-exclusive, worldwide, royalty-free licence to use Customer-specific Deliverables for its internal business purposes and for assessing, improving and reporting on its security. The Customer may share a complete and unmodified report or finding confidentially with its Affiliates, advisers, auditors, regulators, insurers, relevant service providers and bona fide customers or prospects where reasonably required. No third-party recipient acquires a duty of care, warranty or reliance right against OnSecurity unless OnSecurity expressly agrees in writing.

8.4 The Customer grants OnSecurity, its Affiliates and Service Providers a non-exclusive, worldwide, royalty-free licence for the relevant Service term to host, copy, access, adapt and otherwise use Customer Materials as reasonably necessary to provide, secure, support and improve the Services and exercise OnSecurity's rights under the Agreement.

8.5 Where a Service or Deliverable includes third-party Intellectual Property Rights, the Customer's rights are subject to applicable third-party licence restrictions notified by OnSecurity, and OnSecurity grants no greater rights than it is permitted to grant.

8.6 OnSecurity may use general skills, experience, ideas and know-how retained in the unaided memory of its personnel; aggregated or de-identified information that does not identify the Customer or an individual; and feedback or suggestions voluntarily provided by the Customer, to analyse, secure, benchmark, improve and develop the Services. This does not permit disclosure of Customer Confidential Information.

8.7 The Customer agrees that OnSecurity may use its name and logo to identify it as a customer, including in customer lists and on OnSecurity's website. OnSecurity will follow any reasonable brand guidelines the Customer provides, and will stop new uses within a reasonable time of the Customer's written request. OnSecurity will obtain the Customer's prior written consent before publishing a case study, press release or other material that names the Customer or describes its use of the Services

8.8 If a third party claims that the Customer's authorised use of an OnSecurity-owned Platform component or Deliverable infringes its Intellectual Property Rights in the UK or EEA, OnSecurity will defend the claim and indemnify the Customer against damages finally awarded or settlement amounts approved by OnSecurity. This does not apply where the claim is caused by Customer Materials or specifications, Customer or third-party modification, use outside the Agreement or after requested cessation, combination with items not supplied or approved by OnSecurity where the claim would otherwise have been avoided, or third-party components supplied on pass-through terms.

8.9 If a claim under clause 8.8 is made or reasonably likely, OnSecurity may procure continued use, modify or replace the affected item with materially equivalent functionality, or terminate the affected Service and refund prepaid Fees for its unused period. Clauses 8.8 and 8.9 are the Customer's exclusive remedies for third-party Intellectual Property Rights infringement.

9. Confidentiality

9.1 Each party will keep the other party's Confidential Information confidential, use it only to perform or receive the Services or exercise rights under the Agreement, and disclose it only to personnel, Affiliates, advisers and Service Providers who need to know it and are subject to appropriate confidentiality obligations.

9.2 Confidential Information does not include information that the receiving party can demonstrate: (a) is or becomes public other than through breach; (b) was lawfully known to it without restriction before disclosure; (c) is lawfully received from a third party without confidentiality restriction; or (d) is independently developed without use of the disclosing party's Confidential Information.

9.3 A party may disclose Confidential Information where required by law, court or regulator, provided it gives advance notice to the other where legally permitted and reasonably assists the other party to protect such information.

9.4 The obligations in this clause continue for five years after the relevant disclosure or termination, whichever is later, except that trade secrets, credentials and security-sensitive information remain protected for so long as they remain confidential by nature.

9.5 Each party acknowledges that damages may be an inadequate remedy for misuse of Confidential Information and that injunctive, specific performance or other equitable relief may be available.

10. Data protection and privacy

10.1 Roles and processing details. Each party will comply with the Data Protection Laws that apply to it. OnSecurity acts as processor when it processes Customer Personal Data on the Customer's behalf. It acts as an independent controller where it determines the purposes and means of processing, including business contact, account, billing and service-security data, as described in the applicable Privacy Notice. The Processing Overview, together with the Order and Service Description, sets out the subject matter, duration, nature and purpose of the processing, the types of personal data, the categories of data subjects, locations and retention. It forms part of the Customer's documented instructions. Processing under this clause 10 includes Customer Personal Data

that the Customer or its Users load onto the Platform or otherwise give to OnSecurity, and Customer Personal Data that OnSecurity accesses or observes in delivering the Services, including during security testing.

10.2 Processor obligations. Where OnSecurity acts as processor, it will:

(a) process Customer Personal Data only on the Customer's documented instructions (including the terms of this Agreement, Orders, licences, authorised use of the Platform and other written instructions consistent with the Services), unless law requires otherwise, in which case it will inform the Customer of that requirement before processing unless the law prohibits this;

(b) inform the Customer if it reasonably considers that an instruction infringes Data Protection Laws, unless prohibited from doing so;

(c) ensure that personnel authorised to process Customer Personal Data are bound by appropriate confidentiality obligations; and

(d) implement appropriate technical and organisational measures, including the Minimum Security Standards and the TOMs identified in the Processing Overview.

OnSecurity may update those measures under clause 3, but will not materially reduce the overall level of protection during an active committed Order, except where reasonably required by law, regulation or security risk, or by a dependency outside its reasonable control.

10.3 Assistance and Personal Data Breaches. Taking account of the nature of the processing and the information available to it, OnSecurity will:

(a) provide reasonable assistance with data-subject requests and with the Customer's obligations on security, data protection impact assessments and prior consultation;

(b) notify the Customer without undue delay after becoming aware of a Personal Data Breach affecting Customer Personal Data; and

(c) provide the information reasonably available to it to help the Customer meet its notification obligations.

Assistance within standard Service functionality is included. OnSecurity may charge for other assistance at its then-current rates, unless the assistance is needed because of OnSecurity's material breach of this clause.

10.4 Sub-processors. The Customer gives OnSecurity general written authorisation to appoint and replace Sub-processors. OnSecurity will keep its current Sub-processor list in the Processing Overview. Before an addition or replacement Sub-processor processes Customer Personal Data, OnSecurity will actively notify the Customer through the Platform, the Customer's nominated contact or another electronic mechanism identified there. The Customer is responsible for monitoring those notices and keeping its contact details current.

10.5 Sub-processor objections and terms.

(a) The Customer may object within 10 Business Days of that notice being deemed received under clause 18.4(c), but only on reasonable, specific and documented grounds relating to an actual or likely breach of Data Protection Laws. If it does not object in time, the change is deemed accepted.

(b) After a valid objection, OnSecurity may use an alternative Sub-processor, modify the processing, add reasonable safeguards or propose another commercially reasonable solution. It is not required to materially alter the Services or incur disproportionate cost.

(c) If no reasonable solution is available within a further 10 Business Days, the Customer may terminate only the affected Service (or the affected Order if it cannot reasonably be separated) without an Early Termination Charge, and OnSecurity will refund prepaid Fees for the unused terminated period.

(d) OnSecurity will bind each Sub-processor to data protection obligations equivalent to those in this clause 10, to the extent Data Protection Laws require, and remains liable to the Customer for their performance to that extent.

10.6 International transfers. OnSecurity will ensure that any restricted transfer of Customer Personal Data takes place under an applicable adequacy decision, the EU Standard Contractual Clauses, the UK International Data Transfer Agreement or Addendum, or another lawful transfer mechanism. The Customer authorises transfers to the Sub-processors identified in the Processing Overview on that basis.

10.7 Return, deletion and retention. At the end of the relevant Services, OnSecurity will, at the Customer's choice notified within 30 days, return or delete Customer Personal Data in accordance with the Processing Overview, subject to available Service functionality. If the Customer does not choose in time, OnSecurity will delete Customer Personal Data in accordance with its legal requirements and its retention, archive and security processes and procedures, as described in the Processing Overview. OnSecurity may keep Customer Personal Data to the extent applicable law requires. Backup copies may remain until overwritten in the ordinary backup cycle, provided they stay protected and are restored only for recovery, security or legal purposes.

10.8 Records and audit. OnSecurity will make available the information reasonably necessary to demonstrate compliance with this clause 10, and will allow for and contribute to audits by the Customer or an auditor it mandates, subject to confidentiality.

(a) The parties will ordinarily use the Trust Centre, certifications, independent audit reports, questionnaires and remote evidence before any on-site audit.

(b) The Customer may request no more than one audit in any 12 months, unless a regulator requires otherwise or there has been a material Personal Data Breach or reasonable evidence of material non-compliance.

(c) Audits are subject to reasonable notice, must respect confidentiality and security, and must minimise disruption.

OnSecurity may charge reasonable rates for Customer-requested assistance, unless the audit identifies a material breach by OnSecurity.

10.9 Customer responsibilities:

(a) The Customer is responsible for the lawfulness of Customer Personal Data, for providing required privacy information and having a lawful basis, and for ensuring its instructions comply with Data Protection Laws.

(b) The Customer will provide only the personal data the Services reasonably require.

(c) The Customer will not knowingly provide personal data of its own customers, end users or other third parties (including special category and criminal-offence data) unless it is necessary for the Services and expressly agreed, or reasonably inherent in an authorised Target.

10.10 Security testing and incidental access. The Customer acknowledges that OnSecurity may access, view or copy Customer Personal Data held in or reachable through a Target as an inherent result of testing, or in demonstrating a vulnerability. That access is processing on the Customer's instructions. OnSecurity will:

(a) use that data only as reasonably necessary to identify, evidence and report vulnerabilities and the method of access;

(b) limit what it captures and retains as evidence, and minimise or redact personal data in reports where reasonably practicable; and

(c) not, unless agreed otherwise, extract data in bulk or use it for any other purpose.

The Customer authorises OnSecurity to report the fact, method and type of data exposed as a finding. Access authorised by this clause is not a Personal Data Breach by OnSecurity, but this does not limit OnSecurity's obligations under clause 10.3 for its own security incidents.

11. Security and incidents

11.1 OnSecurity will comply with the Minimum Security Standards and will manage Security Incidents in accordance with them. The Customer will give reasonable cooperation where a security event in its environment may materially affect the Services. Personal Data Breaches are handled under clause 10.

12. AI and automation

12.1 OnSecurity may use automation and artificial intelligence (AI) in or to support the Services. AI use: (a) does not expand any authorised Target or Testing Window; (b) remains subject to OnSecurity's confidentiality, data protection, security and reasonable-care obligations; and (c) involving Customer Personal Data is subject to clauses 10.4 to 10.6. Where the Customer can configure, instruct, approve or enable AI functionality, it is responsible for that configuration and for any decision or action it takes in reliance on outputs, unless OnSecurity expressly accepts responsibility. Additional AI-specific terms apply only where an Order or Service Schedule expressly incorporates them.

13. Warranties and Service limitations

13.1 Each party warrants that it has authority to enter into the Agreement. The Customer also warrants that it enters into the Agreement in the course of business and not as a consumer.

13.2 Subject to clause 14.3, and except for the express commitments in the Agreement, all other conditions, warranties and terms implied by statute, common law or otherwise (including fitness for a particular purpose) are excluded to the extent the law allows.

13.3 OnSecurity is not responsible for a failure, delay or loss to the extent it is caused by: (a) the Customer's instructions, delay, breach or inaccurate information; (b) Customer systems, networks, configurations or third-party services that the Customer selects or controls; (c) unauthorised modification, or use contrary to the Agreement or OnSecurity's reasonable instructions; or (d) communications networks or internet infrastructure outside the reasonable control of OnSecurity and its Service Providers.

13.4 Security testing, scanning, threat-intelligence and related Services provide assurance based on the agreed scope, timing, credentials, tools, methods and information available when performed and do not guarantee that every vulnerability, threat, compromise or future security issue will be identified or prevented.

13.5 OnSecurity does not warrant that the Platform or Services will be uninterrupted or error-free or that outputs, findings or recommendations will meet every Customer requirement. Recommendations are guidance requiring Customer judgement, and the Customer remains responsible for remediation decisions and operation of its environment.

14. Liability and indemnities

In this clause 14, "liability" means liability arising under or in connection with the Agreement (including any collateral contract), whether in contract, tort (including negligence), breach of statutory duty, misrepresentation, restitution or otherwise.

14.1 **Customer indemnity.** The Customer will indemnify OnSecurity, its Affiliates, personnel and relevant Service Providers against third-party claims, and resulting losses, liabilities, damages, costs and reasonable legal expenses, arising from: (a) OnSecurity testing or assessing a Target which the Customer did not own or have authority to permit OnSecurity to test; or (b) OnSecurity's authorised use of Customer Materials or Customer Data infringing a third party's Intellectual Property Rights or other rights.

14.2 **Indemnity procedure.** A party seeking the benefit of an indemnity under the Agreement will notify the indemnifying party promptly after becoming aware of the claim, provide reasonable cooperation at the indemnifying party's cost and allow it control of the defence and settlement, provided no settlement admits liability for, or imposes a material non-monetary obligation on, the indemnified party without consent. Delay in notice relieves the indemnifying party only to the extent materially prejudiced.

14.3 **Liability that cannot be limited.** Nothing in the Agreement excludes or limits either party's liability for death or personal injury caused by negligence, fraud or fraudulent misrepresentation, or any other liability that cannot lawfully be excluded or limited.

14.4 **Indirect loss.** Subject to clause 14.3, neither party is liable for indirect, special, incidental or consequential loss or damage.

14.5 **Excluded losses.** Subject to clause 14.3, 5.6 and 7.7, neither party is liable for the following, whether direct or indirect: (a) loss of profit, revenue, business, contracts, opportunity or anticipated savings; (b) loss of goodwill or reputation; (c) loss or corruption of data; (d) business interruption; or (e) wasted expenditure or management time.

14.6 **Liability cap.** Subject to clauses 14.3 and 14.7, each party's total liability under or in connection with an Order, for all claims arising from any one incident or series of connected incidents will not exceed the lower of £500,000 and the Fees paid or payable by the Customer for the 12 months before the event giving rise to the claim (or, if the event occurs in the first 12 months of the Agreement, for those first 12 months). Despite the previous sentence but subject to clauses 14.3 and 14.7, each party's total aggregate liability under or in connection with the Agreement will not exceed £500,000.

14.7 **Customer exceptions.** Nothing in the Agreement limits or excludes the Customer's liability for: (a) Fees, cancellation or Early Termination Charges payable under the Agreement; (b) an indemnity given by the Customer under the Agreement; (c) unauthorised or unlawful testing, Targets or instructions; (d) deliberate infringement or misuse of OnSecurity Intellectual Property Rights; or (e) deliberate breach of confidentiality or unlawful misuse of security credentials.

14.8 **Data Processing Liability.** In this clause 14.8, "Article 82" means Article 82 of the UK GDPR or the EU GDPR, as applicable, and "losses" means compensation paid to data subjects, fines and penalties to the extent lawfully recoverable, and reasonable costs (including legal and legally required notification costs), in each case directly caused by the relevant breach. Subject to clauses 14.3 and 14.6, to each party's duty to mitigate (including by using available appeal processes), and except to the extent a party proves it is not in any way responsible for the event giving rise to the damage (Article 82(3)): (a) each party will indemnify the other for losses arising directly from its own breach of Data Protection Laws; (b) OnSecurity's indemnity for losses the Customer pays to a third party because OnSecurity acted outside or contrary to the Customer's lawful instructions is limited to OnSecurity's part of responsibility for the damage; and (c) where both parties are responsible for the same damage, each is liable only for its own part, and a party that has paid more than that part may recover the excess from the other (Article 82(4) and (5)). This clause allocates liability between the parties only and does not limit data subjects' rights. Amounts recoverable under it are not excluded by clause 14.4 or 14.5.

15. Suspension

15.1 OnSecurity may suspend all or part of a Service, account, User or testing activity, to the extent and for as long as reasonably necessary:

(a) to protect the security, integrity or availability of the Services, the Platform, or any Target or third-party system;

(b) to respond to suspected misuse (including breach of clause 5.7), unauthorised access or unlawful activity;

(c) where the Customer is in material breach of the Agreement;

(d) where OnSecurity reasonably doubts the Customer's authority to authorise testing of a Target, or a Target appears to be incorrect or unauthorised;

(e) where testing is having, or is likely to have, an adverse effect on a Target or third party beyond what the Customer authorised;

(f) to comply with law, regulation or a binding requirement of a competent authority;

(g) to address an urgent issue with a Service Provider on which a Service depends; or

(h) for non-payment of an undisputed amount under clause 7.7, or as a Service Schedule permits.

15.2 Where reasonably practicable and lawful, OnSecurity will notify the Customer before or promptly after suspending, and will restore the affected Service promptly once the reason for suspension is resolved. OnSecurity is not liable for a suspension made in good faith and in accordance with this clause.

16. Term, renewal and termination

16.1 These Master Terms begin when accepted by the Customer and continue until terminated under the Agreement. Each Order begins and continues for the term stated in that Order or applicable Service Schedule.

16.2 A one-off Service ends when completed unless the Order states otherwise. Subscription and recurring Services are subject to the renewal rules in the Order and Platform & Subscription Schedule.

16.3 The Customer may not terminate a committed Order for convenience during its Initial Term or Renewal Term. A non-renewal notice takes effect only at the end of the then-current term. If OnSecurity agrees an early convenience termination, the Customer will pay any Early Termination Charge stated in the Order or, if none is stated, the unpaid committed Fees for the remainder of the term.

16.4 Either party may terminate an affected Order by written notice if the other party commits a material breach of the Agreement and: (a) where the breach is capable of remedy, fails to remedy it within 30 days after receiving written notice requiring it to do so; or (b) where the breach is not capable of remedy, immediately on written notice.

16.5 Either party may terminate the Agreement or an affected Order immediately if the other enters administration, liquidation or an analogous insolvency process, ceases substantially all business or is unable to pay its debts as they fall due, except for a solvent restructuring.

16.6 OnSecurity may terminate an affected Service by notice (or the affected Order, if the Service cannot reasonably be separated) where:

(a) continuing it becomes unlawful or is prohibited by a competent authority;

(b) continuing it is no longer reasonably possible because a Service Provider or technology is discontinued and no reasonable replacement is available under clause 2.12; or

(c) an unresolved valid objection under clause 10.5 prevents the affected processing.

OnSecurity will give at least 30 days' notice of termination under this clause, or shorter notice where the cause requires it. Unless the cause is the Customer's breach, OnSecurity will refund prepaid Fees (including unused Capacity) for the unused affected period, and no Early Termination Charge applies.

16.7 Either party may terminate an affected Order by written notice if a Force Majeure Event prevents or materially affects the performance of all or a substantial part of the Services under that Order for more than 30 continuous Business Days. On termination under this clause, OnSecurity will refund prepaid Fees for the unperformed part of the Services, and no Early Termination Charge applies.

16.8 Either party may terminate these Master Terms on 30 days' notice where no committed Order remains in force. Termination of the Master Terms does not end an Order before its committed term expires.

16.9 On expiry or termination, accrued rights and payment obligations are unaffected. The Customer's right to access the terminated Service ends, subject to any agreed data export or retrieval period, and OnSecurity may retain information only as permitted by the Agreement or law. If the Customer terminates an Order under clause 16.4, OnSecurity will refund prepaid Fees for the Services not performed under it.

16.10 Provisions intended by their nature to survive expiry or termination continue, including confidentiality, intellectual property, payment, data protection where processing continues, liability, governing law and accrued rights.

17. Compliance

17.1 Each party will comply with applicable anti-bribery, anti-corruption, sanctions, export-control and similar laws in connection with the Agreement. The Customer will not require OnSecurity to provide any Service, access, technology or technical data where doing so would cause OnSecurity or a Service Provider to breach those laws.

17.2 OnSecurity may refuse, suspend or modify a Service as reasonably required to comply with law, sanctions, export controls, a regulator or accreditation requirement and, where reasonably practicable, will explain the impact to the Customer.

17.3 The Customer is responsible for legal and regulatory requirements specific to its sector or use of the Services unless the Agreement or Order expressly allocates the requirement to OnSecurity.

18. General

18.1 **Force Majeure.** Neither party is liable for delay, failure or non-performance caused by an event beyond its reasonable control, including utility or communications failure, third-party cyber attack, governmental action, war or terrorism, natural disaster, epidemic or pandemic, industrial action other than its own workforce, or critical supplier failure despite reasonable mitigation. A Force Majeure Event does not excuse the Customer's obligation to pay Fees due under the Agreement.

18.2 **Assignment.** The Customer may not assign or transfer the Agreement without OnSecurity's prior written consent, not to be unreasonably withheld or delayed. OnSecurity may assign or transfer it to an Affiliate or in connection with a merger, reorganisation, financing or sale of all or substantially all of the relevant business or assets, on written notice.

18.3 **Subcontracting.** Clause 2.11 applies to subcontracting. Sub-processing is governed by clause 10.

18.4 **Notices.**

(a) Formal notices of breach, termination, dispute, non-payment or assignment must be in writing and sent either by email to the legal or contract notice address in the Order or the Customer's account or the last contact notified, or by pre-paid first-class post to the recipient's registered or principal office.

(b) An email is deemed received when sent, if sent before 17:00 on a Business Day and no delivery failure message is received, and otherwise at 09:00 on the next Business Day. A posted notice is deemed received at 09:00 on the second Business Day after posting.

(c) Operational, Service, change and Sub-processor notices may be given through the Platform, OnSecurity's website or another electronic mechanism specified in the Agreement. Such a notice is deemed received when it is published, or sent to the Customer's account contact, through that mechanism.

18.5 **Entire agreement and non-reliance.** The Agreement is the entire agreement between the parties on its subject matter and supersedes all prior proposals, discussions and representations. Each party acknowledges that, in entering into the Agreement, it has not relied on any statement, representation or warranty that is not set out in the Agreement, and that it will have no remedy in respect of any such statement, representation or warranty. Nothing in this clause limits or excludes liability for fraud or fraudulent misrepresentation.

18.6 **No waiver.** Delay or failure to exercise a right is not a waiver. A waiver applies only to the specific circumstance for which it is given.

18.7 **Severance.** If a provision is invalid or unenforceable, it will where possible be modified to the minimum extent necessary to make it valid and enforceable, and the remainder of the Agreement continues in force.

18.8 **Relationship.** The parties are independent contractors. Nothing creates a partnership, joint venture, employment, fiduciary or agency relationship, and neither party may bind the other except as expressly stated.

18.9 **Third-party rights.** Except for persons entitled to the benefit of an indemnity under the Agreement, no person who is not a party may enforce the Agreement under the Contracts (Rights of Third Parties) Act 1999. The parties may vary or terminate the Agreement without any third party's consent.

18.10 **Dispute resolution.**

(a) If a dispute cannot be resolved promptly through the usual operational contacts, either party may give a dispute notice under clause 18.4(a). The relevant managers will try to resolve it within 10 Business Days of that notice. If it remains unresolved, senior managers or executives will try to resolve it within a further 10 Business Days.

(b) Neither party may start court proceedings until that process has been completed, except: (i) for urgent interim or protective relief; (ii) to preserve a limitation period; (iii) to recover an undisputed debt; or (iv) where the other party refuses or fails to participate in the process.

(c) If the Customer starts proceedings in breach of this clause, it will reimburse OnSecurity's reasonable legal and professional costs caused by that breach, to the extent not otherwise recovered. This is subject to the court's jurisdiction as to costs.

(d) The parties may agree mediation or another form of ADR.

18.11 **Governing law and jurisdiction.** The Agreement and any non-contractual obligations arising from it are governed by the laws of England and Wales. The courts of England and Wales have exclusive jurisdiction, except that either party may seek urgent interim or protective relief in any court of competent jurisdiction.

19. Definitions and interpretation

19.1 **Definitions.** In the Agreement, the following terms have the meanings set out below.

Affiliate: an entity which controls, is controlled by or is under common control with a party.

Business Day: a day other than Saturday, Sunday or a public holiday in England when banks in London are open for business.

Capacity: prepaid or committed testing hours, Usage Units, credits, monetary balance or another service-usage metric identified in an Order or Service Document.

Confidential Information: information disclosed or made available in connection with the Agreement which is marked confidential or which a reasonable person would understand to be confidential, including security information, credentials, findings, business information, know-how, designs, technology including technical specifications and configurations, pricing, trade secrets, Customer Data and non-public technical information.

Customer: means any legal entity (or entities as the case may be) that has entered into and signed any Order or the Agreement, or which receives Services from OnSecurity under the terms of the Agreement, or the legal entity which is listed in an Order.

Customer Data: data, content or information submitted, made available, collected from an authorised Target, (subject to clause 8.3) generated for or by the Customer or otherwise processed in connection with the Services, excluding OnSecurity's service telemetry, methods, tools and de-identified information.

Customer Materials: Customer Data, systems, software, documentation, specifications, brands and other materials supplied, made accessible or authorised by or on behalf of the Customer for the Services.

Customer Personal Data: Personal Data processed by OnSecurity as processor on behalf of the Customer in providing the Services.

Data Protection Laws: privacy and data-protection laws applicable to the relevant processing, including the UK GDPR, Data Protection Act 2018, applicable provisions of the Data (Use and Access) Act 2025, the EU GDPR where applicable, and implementing or replacement legislation. “UK GDPR” has the meaning given in the Data Protection Act 2018. “EU GDPR” means Regulation (EU) 2016/679 of the European Parliament and of the Council, as amended from time to time.

Deliverable: a report, finding, document or other customer-specific output expressly identified as a deliverable in an Order or Service Description.

Early Termination Charge: a charge payable for agreed or permitted termination of a committed Order before the end of its current term, as stated in the Order or clause 16.3.

Fees: charges payable under an Order, including subscription, Platform, testing, usage, professional-service, licence, product, overage, cancellation or other agreed charges.

Force Majeure Event: an event beyond a party's reasonable control within clause 18.1.

Initial Term: the initial committed term of an Order stated in that Order or applicable Service Schedule.

Intellectual Property Rights: patents, copyright, database and design rights, trade marks, domain names, rights in software, confidential information, know-how, trade secrets and any other intellectual property rights and all similar or equivalent rights or forms of protection, whether registered or unregistered, including applications, renewals and extensions, anywhere in the world.

Master Terms: these terms and conditions.

Minimum Security Standards: OnSecurity's then-current minimum contractual security standards identified in the Online Contract Information table and incorporated into the Agreement.

Order: an accepted Quote, online or offline order form, statement of work, proposal or other ordering record accepted under clause 2 which identifies the Services, applicable term and Fees.

Personal Data: has the meaning given in applicable Data Protection Laws.

Personal Data Breach: a personal data breach within applicable Data Protection Laws affecting Customer Personal Data.

Platform: OnSecurity's customer-facing software platform and associated interfaces made available as part of the Services.

Privacy Notice: a notice explaining OnSecurity's processing as controller, including the Website Privacy Notice and Platform Privacy Notice.

Processing Overview: OnSecurity's then-current Data Privacy & Processing Overview, available through the online Legal & Trust Centre.

Quote: a written quotation or commercial offer issued by or on behalf of OnSecurity which may become an Order when accepted under clause 2.

Renewal Term: a renewal period applying after an Initial Term in accordance with the Order or applicable Service Schedule.

Security Incident: a material actual or reasonably suspected event compromising the confidentiality, integrity or availability of Customer Data or a contracted Service, excluding routine unsuccessful attempts that do not materially affect the Service or data.

Services: the services, Platform access and Deliverables that OnSecurity agrees to provide under an Order, as described in the applicable Service Description and Service Schedule.

Service Description: a document or webpage describing the functionality, scope or operation of a Service.

Service Document: a Service Description, support policy, acceptable-use requirement, Processing Overview, Minimum Security Standards, data portability or exit guide, or other OnSecurity document expressly incorporated into the Agreement.

Service Level: a measurable service commitment expressly identified as a service level in an Order or Service Document.

Service Provider: an Affiliate, subcontractor, cloud provider, licensor, supplier or other third party used by OnSecurity in connection with the Services.

Service Schedule: service-specific contractual terms identified in an Order or stated to apply to a category of Services.

Sub-processor: a Service Provider engaged by OnSecurity to process Customer Personal Data on behalf of the Customer.

Target: a system, application, network, domain, account, device, environment, physical asset or other subject identified or enabled by the Customer for security testing or assessment.

Testing Window: a period during which intrusive or active testing is authorised, as recorded in an Order, the Platform or another retained written communication.

User: an individual authorised by the Customer to access or administer the Platform or Services.

19.2 In the Agreement: headings do not affect interpretation; the singular includes the plural and vice versa; a person includes an individual and any incorporated or unincorporated body; "including" and similar words are illustrative; "written" includes email and reliable electronic records; references to legislation include amendments, re-enactments and subordinate legislation; and references to a document include that document as validly updated under the Agreement.

Online Contract Information

Master Terms and Schedules	https://onsecurity.io/legalandtrustcentre
Data Privacy & Processing Overview	https://onsecurity.io/privacy-policy/
Minimum Security Standards / TOMs	https://onsecurity.io/legalandtrustcentre
Sub-processor updates	https://onsecurity.io/legalandtrustcentre