ONSECURITY
SERVICE SCHEDULES

SCHEDULE 3 - MINIMUM SECURITY STANDARDS

1. Security programme. OnSecurity will maintain an information security management programme appropriate to the nature of the Services and information processed, supported by policies, risk management, assigned responsibilities and periodic review.
2. Access control. OnSecurity will apply least-privilege and role-based access principles to material systems handling Customer Data and will use multi-factor authentication for privileged, cloud and other material internal access where technically supported and appropriate.
3. Personnel security. Personnel with access to Customer Data will be subject to confidentiality obligations and security awareness training appropriate to their role. OnSecurity will apply proportionate screening where appropriate to role and risk.
4. Encryption. OnSecurity will use industry-standard encryption for Customer Data in transit over public networks and at rest in systems designed to store Customer Data, subject to technical limitations inherent in the Service or an expressly agreed exception.
5. Vulnerability and patch management. OnSecurity will maintain risk-based processes for identifying, prioritising and remediating material vulnerabilities in systems used to provide the Services, including periodic independent security testing of relevant environments.
6. Secure development and change. For software developed or materially controlled by OnSecurity, OnSecurity will maintain proportionate development, review, testing and change-management controls designed to reduce security risk.
7. Logging and monitoring. OnSecurity will maintain reasonable security logging and monitoring appropriate to the Services and risk, subject to retention periods established through its security and retention policies.
8. Backup, continuity and recovery. Where the nature of a Service requires persistent storage, OnSecurity will maintain backup and recovery controls reasonably designed to support continuity and restoration. Specific recovery time or recovery point objectives apply only where expressly stated in an Order or Service Document.
9. Incident management. OnSecurity will maintain incident response procedures and will investigate, contain and manage material Security Incidents affecting the Services.
10. Supplier security. OnSecurity will apply reasonable due diligence and contractual controls to material Service Providers, proportionate to the service, access and information involved.
11. Data minimisation and retention. OnSecurity will maintain retention and deletion controls designed to keep Customer Data no longer than reasonably required for the relevant Service, legal obligation, security purpose or agreed business need, as further described in the Processing Overview.
12. Certifications and evidence. Current certifications and security evidence may be made available through the Trust Centre or under appropriate confidentiality. A certification applies only to its certified scope and validity period. The Trust Centre remains informational except to the extent a commitment is expressly set out in this Schedule or an Order.