Schedule 5 — Security Schedule

ATSC Global Limited · the minimum technical and organisational measures for every ATSC Service

Field	Detail
Document reference	ATSC-SCH5-SEC
Version	1.0, November 2026
Effective date	[DATE OF PUBLICATION]
Status	Contractual minimum. The Supplier may improve these measures at any time and may change them only where the overall level of protection is not reduced (Agreement clause 6.1).
Relationship to the DPA	This Schedule is Annex II of the Standard Contractual Clauses and expands Annexure 3 of the Data Processing Agreement.

1. Governance

1.1 The Supplier maintains a documented information security programme, approved by its board, including an information security policy, an acceptable use policy for personnel, a risk assessment methodology and a risk register reviewed at least annually. The current internal policy set is the IT Security Policy Manual, the Data Protection Policy and the Records Management Policy.

1.2 The Supplier designates a named individual responsible for information security, with sufficient authority and resources, who reports to the board at least twice a year.

1.3 Certifications held: the Supplier does not currently hold a third-party information security certification, and will notify Customers if it obtains one. Microsoft Azure, the hosting Sub-processor, holds ISO/IEC 27001 and SOC 2 Type II certifications for its infrastructure. Those certifications cover Microsoft's infrastructure only, not the Supplier's own operations, and the Supplier shall provide Microsoft's reports on request where Microsoft permits.

2. Personnel

2.1 Personnel with access to Customer Data are subject to written confidentiality obligations, background screening where lawful in their jurisdiction, security and data protection awareness training at onboarding and at least annually, and a disciplinary process for security breaches.

2.2 Access rights are removed within one (1) Business Day of a person leaving or changing role.

3. Access control

3.1 Unique named accounts; role-based access with least privilege by default; multi-factor authentication for all administrative, privileged and remote access to production systems; privileged access granted on a time-limited basis where technically feasible; quarterly review of privileged access; automatic session timeout; no shared administrative accounts.

3.2 The Services support single sign-on via SAML 2.0 or OpenID Connect for Enterprise tier Customers, where the product annexure for the Service states that it is supported, and allow Customer Administrators to enforce multi-factor authentication for their Authorised Users.

4. Encryption and key management

4.1 Customer Data is encrypted in transit using TLS 1.2 or higher with modern cipher suites, and at rest using AES-256 or equivalent, including in databases, file storage and backups.

4.2 Encryption keys are managed through a hardware-backed or cloud provider key management service, with access restricted to named personnel and logged. Customer-managed encryption keys are not currently offered.

5. Infrastructure and network security

5.1 Production environments are logically segregated from development and test environments and from each other; network access is restricted by firewalls and security groups on a deny-by-default basis; administrative interfaces are not exposed to the public internet.

5.2 Systems are built from hardened baselines; security patches are applied within fourteen (14) days of release for critical vulnerabilities and thirty (30) days for high-severity vulnerabilities, or an equivalent mitigation is applied.

5.3 Production systems are monitored by centralised logging and intrusion detection, with alerting to on-call personnel.

6. Application security

6.1 The Supplier follows a documented secure development lifecycle, including threat modelling for significant changes, peer code review, automated static analysis and dependency vulnerability scanning in the build pipeline, protection of secrets outside source code, and separation of duties for deployment to production.

6.2 The Supplier maintains a software bill of materials for each Service and monitors Third Party Components and open-source dependencies for disclosed vulnerabilities.

6.3 Live Customer Data is not used in non-production environments, other than in pseudonymised or anonymised form.

7. Testing and vulnerability management

7.1 The Supplier commissions an independent penetration test of each production Service at least annually and after significant architectural change, remediates findings according to severity, and makes an executive summary available to Customers on request under confidentiality.

7.2 The Supplier operates a vulnerability disclosure policy at atsc.global/legal/security through which researchers may report vulnerabilities, and shall not take legal action against good-faith reporters who comply with it.

7.3 The Customer may conduct its own penetration testing of its tenant only with the Supplier's prior written agreement on scope and timing.

8. Incident management

8.1 The Supplier maintains a documented incident response plan, tested at least annually, defining roles, escalation, evidence preservation, communication and post-incident review.

8.2 The Supplier shall notify the Customer of a security incident affecting Customer Data within forty-eight (48) hours of becoming aware of it, in accordance with clause 6.2 of the Agreement and the Data Processing Agreement, and shall cooperate with the Customer's own obligations to notify authorities, including under Article 33 GDPR and, where the Customer is an essential or important entity, under the national rules implementing Directive (EU) 2022/2555 (NIS2).

9. Resilience, backup and continuity

9.1 Customer Data is backed up automatically, with encrypted backup copies held separately from production in the Hosting Region. Restores are tested at the frequency stated in the SLA.

9.2 The Supplier maintains business continuity and disaster recovery plans designed to meet the recovery point and recovery time objectives in the SLA, tested at least annually.

10. Supplier and Sub-processor management

10.1 Before engaging a Sub-processor or a supplier with access to Customer Data, the Supplier assesses its security and data protection controls, binds it by written terms no less protective than this Schedule, and reviews it at least annually.

10.2 Where the Customer is subject to NIS2 or DORA, the Supplier shall provide reasonable information about its own security measures and supply chain to support the Customer's supplier risk assessment.

11. AI-specific measures

11.1 For Services containing an AI System, the Supplier additionally: separates each Customer's Inputs, Outputs, retrieval indexes and fine-tuning data from other customers'; applies controls against prompt injection and data exfiltration through tool use; requires affirmative user confirmation before an AI agent performs any action that writes, modifies or deletes data in a connected system, unless the Customer configures otherwise; logs AI tool calls for audit; and evaluates Models for security and safety before release. Further terms are in the AI Addendum.

12. Physical security

12.1 Customer Data is hosted only in data centres operated by Sub-processors holding recognised certifications, with controlled physical access, environmental controls, fire suppression and redundant power. The Supplier's own offices do not host production Customer Data.

13. Shared responsibility

Area	Supplier	Customer
Hosting infrastructure and platform	Secure, patch and monitor	—

Area	Supplier	Customer
Application security of the Service	Secure development, testing, patching	Configure settings in line with the Documentation
User access	Provide MFA, SSO and role controls	Manage users, enforce MFA, remove leavers promptly
Customer Data	Encrypt, back up, segregate	Decide what is uploaded; lawful basis; classification
Customer integrations and API keys	Provide secure interfaces	Secure its own systems and credentials
End-user devices and networks	—	Secure them
On-premise deployments	Secure software and timely Updates	Infrastructure, network, physical security, applying Updates

14. Assurance

14.1 The Supplier shall, on request and not more than once a year, complete a reasonable security questionnaire from the Customer, and shall provide its current certifications, penetration test summaries and policies under confidentiality. Audit rights in respect of Personal Data are set out in the Data Processing Agreement.

End of Schedule 5.