

Betelgeuse Entertainment B.V.

Information Technology & Information Security Policy

Version 2.0 — July 1, 2026

Prepared in accordance with the Curaçao Gaming Authority (CGA) Information Security
Control Requirements for CGA Licensees (B2C and B2B), April 2026

Document Control

Document title	Information Technology & Information Security Policy
Company	Betelgeuse Entertainment B.V. (Limited Liability Company, Curaçao Commercial Register no. 161954)
Registered address	Korporaalweg 10, Curaçao
Version	2.0
Classification	Business Confidential
Effective date	July 1, 2026 (date of issue)
Next review date	July 1, 2027 (or earlier upon material change)
Document owner	IT / Information Security Officer
Approved by	Management
Regulatory basis	CGA Information Security Control Requirements for CGA Licensees (B2C and B2B), April 2026; Landsverordening op de Kansspelen (LOK)

Version Control

Version	Date of Issue	Author(s)	Brief Description of Changes	Approved By
1.0	December 1, 2023	Legal	Initial release	Paweł Piętak
1.1	December 12, 2024	Legal	Annual review – no material changes	Paweł Piętak
1.2	December 7, 2025	Legal	Annual review – no material changes	Paweł Piętak
2.0	July 1, 2026	Paweł Piętak	Full revamp in accordance with the new CGA guidelines	Management

1. Introduction and Purpose

Betelgeuse Entertainment B.V. (“the Company”) is a limited liability company incorporated in Curaçao on September 29, 2022 and registered with the Curaçao Chamber of Commerce & Industry under number 161954, with its registered office at Korporaalweg 10, Curaçao. The Company internationally organizes, markets, promotes, manages, supports and operates remote gaming activities, comprising all types of games, betting, betting exchange, interactive casinos, bingos, lotteries and other interactive games. All players targeted by the Company are located outside of Curaçao.

This Information Technology & Information Security Policy establishes the mandatory rules, controls and responsibilities that protect the confidentiality, integrity and availability of the Company's information assets, gaming systems, player data and financial data. It implements the Information Security Control Requirements for CGA Licensees (B2C and B2B) issued by the Curaçao Gaming Authority (CGA) in April 2026, which are based on the Center for Internet Security (CIS) Controls Implementation Group 1 (IG1) and aligned with ISO/IEC 27001:2022.

Compliance with the CGA requirements constitutes a mandatory condition of licensure under the Landsverordening op de Kansspelen (LOK). This policy is therefore binding on all personnel and relevant third parties. The terms “must” and “shall” in this policy indicate binding obligations.

In line with the CGA cybersecurity maturity roadmap, the Company implements the IG1 baseline as a minimum and plans to progress toward CIS Implementation Group 2 (IG2) maturity within 24 to 36 months.

2. Scope

This policy applies to:

- All employees, officers, directors, contractors, temporary staff and interns of the Company;
- All third-party service providers, B2B platform and game content providers, aggregators, hosting providers and consultants with access to Company systems or data;
- All information systems, applications, networks, cloud environments, endpoints and mobile devices used to support the Company's gaming operations;
- All data processed by or on behalf of the Company, including Critical Gaming Data, player personal data, financial data and regulated records.

The Company operates exclusively online (B2C remote gaming). Controls in the CGA requirements that apply specifically to land-based operations (e.g., gaming floor equipment, slot machines, surveillance of physical gaming areas) are not applicable, and this is documented as part of the Company's compliance records. Where the Company operates on third-party or cloud-hosted platforms, the Company remains fully responsible under the LOK for compliance; controls implemented by providers are verified through contractual assurances, due diligence and ongoing monitoring under the shared responsibility model described in Section 17.

3. Roles and Responsibilities

- **Statutory Director (Xecutive Corporate Management B.V.):** Holds executive responsibility and ultimate accountability for information security. Approves this policy, allocates resources, and oversees compliance with CGA license conditions.
- **IT / Information Security Officer:** Owns this policy; maintains the security control framework; manages asset, vulnerability, logging and incident processes; reports on security posture to the Director; acts as primary contact for CGA security matters.
- **Compliance Officer:** Monitors regulatory obligations (LOK, CGA requirements, AML/CFT, data protection); maintains the register of legal obligations; coordinates CGA reporting, self-assessments and audits.
- **Incident Response Manager (primary and backup):** Coordinates detection, response, escalation and notification of security incidents as set out in Section 18.
- **All personnel:** Must comply with this policy, complete required training, protect credentials and assets entrusted to them, and report suspected security incidents without delay.
- **Third-party providers:** Must comply with contractual security obligations consistent with this policy and support the Company's verification and audit rights.

4. Policy Framework and Compliance Demonstration

The Company must implement all applicable CIS IG1 controls within 12 months of license issuance or publication of the CGA requirements, whichever applies. The Company demonstrates compliance through:

- Annual self-assessment reports using CGA-provided templates;
- Independent third-party security audits (mandatory for online operators);
- Incident reporting in accordance with CGA breach notification requirements (Section 18);
- Cooperation with ongoing CGA compliance monitoring, including reviews, inspections, remote assessments and technical validation.

5. Asset Management (CGA 1.9)

5.1 Hardware Asset Inventory

The Company must maintain a complete and accurate inventory of all enterprise devices that interact with gaming data or systems, including application and infrastructure servers (gaming, financial, player management), networking hardware, end-user computing devices and any IoT devices. For each asset the inventory records the static IP or MAC address, hostname or device identifier, asset owner or responsible business unit, and network approval/access status. A formal inventory review is performed at least twice annually.

5.2 Unauthorized Devices

A documented weekly procedure must be operated to identify and respond to unauthorized devices, using automated discovery tools or manual verification. Mitigation actions include removal from the network, blocking remote access, or quarantine. A log of detections,

actions taken and justified exceptions is maintained. Priority is given to devices that could impact game fairness, manipulate outcomes or introduce data protection risks.

5.3 Software Inventory

The Company must maintain an inventory of all authorized software, including gaming software platforms, operating systems, endpoint and server security tools, and reporting, management and compliance applications. Where applicable, each gaming software entry records title and game variant, version and installation date, purpose and business function, and number of licenses or installations. The software inventory is reviewed and updated bi-annually. Tracking includes RNG software, game engines and other components subject to regulatory oversight supplied by licensed B2B providers.

5.4 Unsupported Software

Vendor support status of all approved software must be validated monthly. Unsupported software is removed, or a documented exception is approved recording the risk acceptance rationale and compensating controls (e.g., network isolation, restricted access). As an online B2C operator using certified Remote Gaming Servers and game content from licensed B2B providers, the Company is not responsible for the B2B provider's game lifecycle management or certification process, but must verify certification status at onboarding and at least annually thereafter, contractually require notification of status changes, and notify the CGA of any lapsed or withdrawn certifications affecting components in use (see Section 17).

6. Data Protection and Classification (CGA 1.10)

6.1 Data Classification

All data must be classified into the following sensitivity categories, each with documented handling procedures covering access restrictions, storage locations and protections, and sharing and transfer protocols:

- **Critical Gaming Data:** game event outcomes, high-value transactions, jackpot triggers, sports data feeds and live odds, game results received from B2B providers or content aggregators, RNG output records, and aggregated content used to determine wager outcomes;
- **Player Personal Data:** identity documents, payment details, behavioral data, KYC records and responsible gaming records;
- **Business Confidential Information:** internal financials, operational strategies, contracts;
- **Public Data:** website content, marketing materials.

The data management process is reviewed annually or upon significant system, regulatory or process change.

6.2 Sensitive Data Inventory

A central, up-to-date inventory must be maintained of all locations where sensitive data is stored, processed or transmitted, including databases and application servers, file systems and shared drives, and cloud storage and backup repositories. Each data store is labelled by

data type and classification. The inventory is updated at least annually or upon significant infrastructure change, with priority given to gaming-critical and player personal data.

6.3 Access to Data

Access to sensitive data is limited on a need-to-know basis using role-based access control (RBAC) and the principle of least privilege. Access settings are reviewed regularly for gaming databases, player account and loyalty systems, financial transaction and bonusing systems, and security and audit systems. Access privileges for operational staff, administrative users and third-party vendors are clearly distinguished.

6.4 Retention and Secure Disposal

Retention schedules must be defined for all data categories in line with regulatory requirements and business needs. Gaming transaction records are retained for a minimum of five (5) years, or longer where required by law or license conditions. Secure disposal at end-of-life uses cryptographic erasure, overwriting/degaussing, or physical destruction of media.

6.5 Encryption of End-User Devices

Full-disk encryption must be applied to all laptops, tablets and mobile devices that store or process regulated data, using industry-standard tooling appropriate to the operating system. Encryption keys are managed securely in accordance with Section 24.

7. Secure Configuration (CGA 1.11)

7.1 Configuration Standards

Documented secure configuration (hardening) standards must be maintained for all technology categories, including physical and virtual servers, security appliances, user endpoints and network infrastructure, based on vendor-recommended templates or recognized baselines such as CIS Benchmarks. Standards are reviewed annually or upon deployment of new technologies, preserving the performance requirements of gaming systems.

7.2 Session Locking

All user systems must lock automatically after inactivity: a maximum of 15 minutes for general systems and 2 minutes for mobile devices, enforced through centralized configuration management.

7.3 Firewalls

Host-based firewalls must be installed and configured on all supported servers and endpoints with default-deny rules and allow-listing policies. All rule changes, including exceptions, are reviewed, approved and documented. Firewall rules must support authorized gaming traffic while preventing exposure of unnecessary services.

7.4 Secure Administration Protocols

All administrative and configuration activities must use secure protocols (SSH, SFTP, HTTPS). Insecure protocols (Telnet, HTTP, FTP) are disabled unless explicitly required and risk-justified. Where possible, configurations are managed via version-controlled scripts and infrastructure-as-code.

7.5 Default Accounts

Default accounts on all systems, applications and devices must be disabled, renamed or removed, and all default passwords changed upon deployment. A list of default accounts is maintained, with documented justification and compensating controls for any retained accounts.

8. Account Management (CGA 1.12)

8.1 Account Inventory

A complete inventory of all accounts must be maintained, covering standard user accounts, privileged administrative accounts and system/service accounts. For each account the full name and department, username, and creation and deactivation dates are recorded. Quarterly reviews confirm all active accounts are valid, assigned to current staff and necessary.

8.2 Password Requirements

All accounts must use strong, unique passwords: a minimum of 8 characters where multi-factor authentication (MFA) is in place, and a minimum of 14 characters where MFA is not available. Shared and default passwords are prohibited. Password managers are used to support unique credential storage.

8.3 Dormant Accounts

Accounts must be disabled after 45 days of non-use, with automated inactivity monitoring where technically feasible. Audit logs are retained and reactivation procedures documented.

8.4 Privileged Accounts

Administrative access is restricted to dedicated privileged accounts, separate from standard business accounts, and used only for elevated functions. Privileged accounts must not be used for web browsing, email or general activities. Strict role separation, audit logging and access control reviews apply to administrative access to gaming software and system configurations.

9. Access Control and Multi-Factor Authentication (CGA 1.13)

9.1 Access Granting

A documented and auditable provisioning process must be operated, using automated provisioning where feasible and requiring written or system-based manager approval for all

access requests. Access assignments are documented against onboarding, role changes and temporary or third-party engagements, and access roles are defined by job function.

9.2 Access Revocation

User access must be revoked immediately upon termination, contract completion or role change. HR-initiated events trigger account disablement with notification to IT. Accounts are disabled rather than deleted to preserve audit trails, and the process is applied consistently across on-premise and cloud systems.

9.3 Multi-Factor Authentication

MFA is mandatory for:

- All internet-facing or externally accessible applications and portals;
- Remote access (VPN, RDP or similar);
- Administrative access to core gaming systems and infrastructure.

Acceptable methods are TOTP authenticator applications, FIDO2/WebAuthn hardware tokens, and biometric identifiers. MFA solutions must not interfere with emergency response procedures or uptime of critical systems.

10. Vulnerability and Patch Management (CGA 1.14)

10.1 Vulnerability Management Program

The Company must maintain a documented, risk-based vulnerability management program covering asset discovery and classification, scanning schedules, risk evaluation criteria and time-bound remediation guidelines. Automated vulnerability scans are performed at least monthly (more frequently for critical systems) across operating systems, network infrastructure, web applications and third-party software. Threat intelligence and vendor advisories — including notifications relevant to gaming platforms and RNG components — inform prioritization. The program is reviewed annually or after major environmental changes.

10.2 Patch Management

Patches for operating systems, software and firmware must be applied at least monthly through an automated, repeatable process. Updates are tested in a staging environment before production deployment where feasible, and patch approvals, results and exceptions are documented. Patch cycles are scheduled to avoid peak operating hours, player impact and regulatory audit periods, in coordination with vendors of critical gaming systems.

11. Logging and Monitoring (CGA 1.15)

11.1 Audit Log Management

A documented audit log management process must define logging requirements per system type and business function, minimum retention periods based on regulatory and business requirements, centralized log collection, periodic reviews for anomalies, and secure archival.

Access to audit logs is restricted to authorized personnel. The process is reviewed annually or upon significant change.

11.2 Log Collection and Integrity

Audit logging is enabled on all enterprise assets and forwarded to centralized, tamper-resistant storage (e.g., a SIEM platform). Log integrity is protected using cryptographic hashing or write-once storage. Critical gaming logs must include:

- Gameplay and betting transactions;
- Jackpot wins and high-value events;
- Player account, deposit and withdrawal movements;
- Administrative access and system configuration changes.

12. Web and Email Protection (CGA 1.16)

Only fully supported, current versions of browsers and email clients may be deployed, with automatic updates enabled and unsupported software removed promptly. DNS filtering must be deployed across all endpoints — on-premises and remote — with threat intelligence feeds maintaining updated blocklists and DNS activity monitored for anomalies. Filtering must not interfere with connectivity to legitimate gaming services or cloud environments.

13. Malware Defence and Removable Media (CGA 1.17)

Up-to-date, centrally managed anti-malware software must be installed on all supported endpoints and servers, configured for automatic signature and engine updates and regular scanning, without degrading gaming system performance. Autorun and autoplay functionality for removable media is disabled on all systems. Removable media usage requires documented authorization, and data from external storage must be scanned or validated before transfer.

14. Backup and Recovery (CGA 1.18)

14.1 Recovery Strategy

A documented data recovery strategy must identify the data and systems requiring backup (with emphasis on critical gaming operations), backup and recovery-testing procedures, recovery point objectives (RPOs) and recovery time objectives (RTOs), and security measures for backup data including access restrictions and encryption. The strategy is reviewed annually or upon major change. Gaming transaction data, configuration files and player activity logs are always included.

14.2 Backup Execution and Protection

Backups of systems handling sensitive or regulated data are automated and performed at minimum weekly; gaming transaction logs and financial data are backed up daily or in real time to meet regulatory retention requirements. Backup data uses offline, off-site or immutable storage where feasible to resist tampering and ransomware, and is protected with the same access controls as production data. Restoration is tested periodically.

15. Network Security (CGA 1.19)

An inventory of network infrastructure (routers, switches, firewalls) must be maintained. Firmware and software version status is reviewed at least monthly, and updates applied based on vendor advisories and risk impact. Only supported versions are used; end-of-life products are not permitted in live environments. Updates are coordinated with gaming system maintenance windows and third-party vendors.

16. Security Awareness and Training (CGA 1.20)

16.1 General Awareness

All personnel receive baseline cybersecurity training at onboarding, repeated at least annually or upon policy or threat changes. Training covers secure system and asset use, regulatory obligations and compliance expectations, and gaming-specific threats including gaming fraud, data privacy and social engineering targeting online operators.

16.2 Role-Based Training

Additional role-based training must be provided covering: social engineering defense (phishing, business email compromise, pretexting); authentication practices (password hygiene, MFA, credential protection); secure data handling (storage, transfer, archival, destruction); prevention of unintentional data exposure; incident recognition and reporting; reporting of missing or failed security updates; and the risks of insecure networks, especially for remote access. Training includes simulated exercises involving gaming-specific threats.

17. Third-Party and B2B Provider Management (CGA 1.21)

17.1 Service Provider Inventory

The Company must maintain a complete and current inventory of all service providers, including gaming software and B2B platform providers, game content aggregators, sports data feed providers, cloud hosting and infrastructure providers, payment processors, and security monitoring services. For each provider, the contract type and scope, internal owner, and classification of data or systems accessed are documented, together with the nature and scope of data exchanged, contractual security and integrity obligations, certification or audit status, and procedures for detecting and responding to feed manipulation, data integrity failures or service disruptions. The inventory is reviewed annually or upon change.

Reliance on third-party platforms, hosting providers, game suppliers or managed services does not transfer regulatory accountability: the Company remains fully responsible under the LOK. For cloud infrastructure, the Company documents which controls are managed by the provider under the shared responsibility model and maintains evidence of provider certifications (e.g., SOC 2, ISO 27001).

17.2 Integrity of Game Content and Data Feeds

Where the Company relies on third parties for game content, sports data feeds or aggregated results that influence wager outcomes:

- **Source authentication:** all feeds are received over authenticated, encrypted channels; API connections use mutual TLS or equivalent;
- **Integrity validation:** cryptographic signatures, hash verification or message authentication codes detect tampering or corruption in transit;
- **Monitoring:** feed availability, latency and data consistency are monitored, with procedures to detect and respond to interruptions, result discrepancies or anomalous patterns;
- **Failover and suspension:** affected wagering markets or game offerings are suspended when feed integrity cannot be assured, and resumed only after integrity is re-established;
- **Contractual assurances:** agreements include security controls, incident notification, data integrity guarantees, and the right to audit or request evidence of compliance.

17.3 B2B Certification Monitoring

For licensed B2B providers, the Company must: verify certification status at onboarding and at minimum annually thereafter; include contractual right-to-audit or right-to-request-evidence provisions; require the B2B provider to notify the Company of certification lapses or scope changes; and operate documented escalation procedures for certification lapses, including suspension of affected game content and notification to the CGA. The Company ceases to offer game content from any B2B provider whose required certifications are no longer valid, until restored.

18. Incident Response and CGA Notification (CGA 1.22)

18.1 Roles

A primary and backup Incident Response Manager must be formally appointed, with defined roles for IT, security, compliance, legal and communications. External incident response services may be used, but internal oversight is maintained. Roles include handling gaming-specific scenarios such as payout manipulation or integrity violations. Assignments are reviewed annually.

18.2 Contact Directory

An up-to-date incident contact directory must be maintained, covering internal stakeholders, the CGA and other regulators, law enforcement, the financial intelligence unit, insurance providers, and vendors responsible for critical infrastructure. The incident response plan specifies notification timelines, required reporting information, and coordination with forensics and legal counsel.

18.3 Reporting Process and Mandatory CGA Notification

A documented incident reporting process defines what constitutes a reportable incident, escalation criteria and reporting channels, and is available to all employees and service providers, supported by reporting templates.

Mandatory CGA notification (LOK Article 5): Betelgeuse Entertainment B.V. shall notify the Curaçao Gaming Authority without undue delay, and in any event within 24 hours, of any security incident that compromises gaming integrity; affects player funds or personal data; or

may impact regulatory reporting, system availability or game fairness. Failure to notify constitutes a breach of license conditions under the LOK.

19. Physical and Environmental Security (CGA 1.23)

Physical access to secure areas (e.g., server rooms and locations housing IT equipment) must be restricted using access cards, biometric scanners or equivalent measures, with entry logs maintained and periodically reviewed. Environmental safeguards include climate controls, smoke detection and UPS systems. Clean desk / clear screen practices are enforced, and equipment used or stored off-premises is secured. As an online-only operator, land-based physical gaming controls (slot machines, payout systems, floor surveillance) do not apply; where infrastructure is hosted in third-party data centers, physical security is verified through provider certifications and contractual assurances.

20. Human Resource Security (CGA 1.24)

Background checks must be conducted for new hires in critical or sensitive roles, with enhanced screening for personnel managing financial systems, player data or gaming system oversight. Employment agreements include confidentiality obligations, and employees acknowledge their security responsibilities at onboarding. Non-compliance with this policy may result in disciplinary action. Upon offboarding, company assets are reclaimed and accounts disabled promptly in accordance with Section 9.2.

21. Legal and Regulatory Compliance (CGA 1.25)

The Company must maintain a register of applicable legal, regulatory and contractual obligations (including the LOK, CGA license conditions, data protection, AML/CFT and KYC requirements), with assigned responsibility for tracking changes. Controls safeguard personal data and intellectual property, and data retention and disposal align with legal requirements. The Company supports CGA reporting requirements and demonstrates compliance during inspections.

22. Business Continuity and Operational Assurance (CGA 1.26)

Information security must be integrated into business continuity and disaster recovery plans, which are tested and reviewed annually or upon significant change. Failover and redundancy are implemented for mission-critical gaming systems, and transaction processing systems, real-time reporting tools and regulatory interfaces have defined fallback procedures. Change management includes risk assessments, and data masking and controlled access are used during audits and testing.

23. Security Governance and Oversight (CGA 1.27)

Executive responsibility for information security oversight rests with the Statutory Director. Independent reviews of policy compliance and control effectiveness are conducted, documented operational procedures are maintained for key activities (backups, user access, audits), and corrective actions are monitored to completion. Policies and standards,

including this policy, are reviewed and approved at least annually. Game audit data and compliance logs are governed with defined ownership and oversight.

24. Cryptographic Controls and Data Masking (CGA 1.28)

Sensitive data must be encrypted at rest and in transit using secure, industry-standard protocols (e.g., TLS 1.2+ in transit, AES-256 at rest). Data masking is applied in development, QA and analytics environments. A key management program covers key generation, storage, use and retirement, and a register of cryptographic controls and approved exceptions is maintained. RNG data, player credentials and jackpot triggers are encrypted and masked appropriately.

25. Performance Considerations, Exceptions and Enforcement

25.1 Performance

Security controls are implemented so as not to adversely affect the performance and availability of gaming platforms, the player experience (game fairness, reliability, uptime), real-time processing of transactions and gameplay outcomes, or timely regulatory reporting and audit functions. Where safeguards introduce latency or overhead, compensating controls or alternate configurations are considered.

25.2 Exceptions

Any exception to this policy requires a documented risk assessment, compensating controls, and written approval by the IT / Information Security Officer and the Statutory Director. Exceptions are recorded in an exception register and reviewed at least annually.

25.3 Enforcement

Violations of this policy may result in disciplinary action up to and including termination of employment or contract, and may expose the Company to regulatory action by the CGA, including warnings, compliance orders, administrative financial penalties, enhanced security obligations, or suspension of license. All personnel must cooperate fully with CGA investigations and remediation timelines.

26. Policy Review and Approval

This policy is reviewed at least annually, and additionally upon significant changes to systems, operations, the threat landscape or regulatory requirements (including future CGA IG2 guidance). Amendments are approved by the Statutory Director.

Approved by	Function	Signature / Date
Executive Corporate Management B.V.	Statutory Director of Betelgeuse Entertainment B.V.	

Appendix A: Mapping to CGA Requirements

The table below maps the sections of this policy to the CGA Information Security Control Requirements for CGA Licensees (B2C and B2B), April 2026, and the underlying CIS IG1 controls and ISO/IEC 27001:2022 Annex A references.

Policy section	CGA Guideline section	CIS IG1 / ISO 27001:2022
5. Asset Management	1.9	CIS 1, 2 / A.5.9
6. Data Protection & Classification	1.10	CIS 3 / A.5.9, A.5.10, A.5.15, A.5.33, A.6.7, A.8.1
7. Secure Configuration	1.11	CIS 4 / A.8.5, A.8.9, A.6.7, A.8.1, A.8.2
8. Account Management	1.12	CIS 5 / A.5.15, A.5.16, A.5.17, A.8.2
9. Access Control & MFA	1.13	CIS 6 / A.5.15, A.5.16, A.5.18, A.6.5, A.6.7, A.8.2
10. Vulnerability & Patch Management	1.14	CIS 7 / A.8.8
11. Logging & Monitoring	1.15	CIS 8 / A.8.15, A.8.6
12. Web & Email Protection	1.16	CIS 9 / A.8.1, A.8.23
13. Malware Defence & Removable Media	1.17	CIS 10 / A.8.1, A.8.7
14. Backup & Recovery	1.18	CIS 11 / A.8.13
15. Network Security	1.19	CIS 12
16. Security Awareness & Training	1.20	CIS 14 / A.6.3
17. Third-Party & B2B Provider Management	1.21	CIS 15 / A.5.19
18. Incident Response & CGA Notification	1.22	CIS 17 / A.5.5, A.5.6, A.5.24, A.6.8
19. Physical & Environmental Security	1.23	A.7.1–A.7.14
20. Human Resource Security	1.24	A.5.11, A.6.1–A.6.6
21. Legal & Regulatory Compliance	1.25	A.5.31–A.5.34
22. Business Continuity	1.26	A.5.29, A.8.14, A.8.32–A.8.34
23. Security Governance & Oversight	1.27	A.5.4, A.5.35–A.5.37
24. Cryptographic Controls & Data Masking	1.28	A.8.11, A.8.24