Information Security Policy

ProvisionIQ Ltd — Protecting Information, Systems, and People

Document	Information Security Policy (ISP)
Company	ProvisionIQ Ltd
Policy Owner	Chief Technology Officer (CTO) / Data Protection Officer (DPO)
Version	2.0
Effective Date	July 2026
Next Review	July 2027
Applies to	All employees, contractors, consultants, partners, and any party with access to ProvisionIQ systems, data, or premises
Compliance basis	ISO 27001:2022 · Cyber Essentials Plus · UK GDPR / DPA 2018 · NCSC Cyber Security Principles
Replaces	Version 1.0 (May 2026)

Statement of Intent

ProvisionIQ Ltd processes special category personal data about children with SEND, including EHCPs, ISPs, health records, safeguarding flags, and multi-agency referrals, some of the most sensitive data in the UK education system. We treat information security not as a compliance exercise but as a fundamental obligation to the schools, pupils, families, and professionals who trust us with their data. This Information Security Policy sets out our commitment to protecting the confidentiality, integrity, and availability of all information assets. Compliance with this policy is mandatory. Breach may result in disciplinary action, termination of contract, or referral to relevant authorities.

Version	Date	Summary
1.0	May 2026	Initial policy — ISMS launch at platform go-live
2.0	July 2026	Added: AI/ML security controls; MIS integration security; IR severity framework; parent portal pen test scope; SIEM enhancement; supply chain AI controls

1. Purpose, Scope, and Objectives

1.1 Purpose

This policy establishes ProvisionIQ's framework for managing information security risks. It defines the rules, responsibilities, and controls that protect ProvisionIQ's information assets — including pupil SEND data, EHCPs, safeguarding records, multi-agency collaboration data, MIS-integrated data, parent portal data, platform source code, commercial information, and staff data — from unauthorised access, disclosure, alteration, or destruction.

1.2 Scope

This policy applies to:

- All ProvisionIQ employees, directors, and shareholders
- All contractors, consultants, and agency workers engaged by ProvisionIQ
- All third-party suppliers, sub-processors, MIS integration partners, and AI service providers with access to ProvisionIQ systems or data
- All information assets owned or managed by ProvisionIQ, including cloud infrastructure, source code, databases, backups, MIS integration pipelines, and physical devices
- All ProvisionIQ software systems, APIs, integrations, and AI/ML components

1.3 Objectives

- Protect the confidentiality, integrity, and availability (CIA) of all information assets, with heightened controls for special category child data
- Meet and maintain Cyber Essentials Plus certification and ISO 27001:2022 accreditation
- Comply with UK GDPR, DPA 2018, PECR, and all applicable legislation including the Children and Families Act 2014
- Prevent, detect, and respond to security incidents promptly and effectively
- Govern all AI/ML features that touch pupil data with rigorous controls proportionate to the sensitivity of that data
- Secure all MIS integration points and third-party data pipelines
- Maintain the trust of schools, pupils, families, and local authorities who rely on our platform
- Continuously improve our Information Security Management System (ISMS)

2. Governance and Accountability

2.1 ISMS Governance Structure

Role	Information Security Responsibilities
Board of Directors	Approves this policy and the ISMS; ensures adequate resources for information security; reviews security

	performance quarterly; accountable for security at the highest level
Chief Technology Officer (CTO)	Policy owner; chairs the Security Committee; responsible for technical security controls; approves security architecture; manages security incidents above P2 severity; approves AI and MIS integration security assessments
Data Protection Officer (DPO)	Advises on GDPR/DPA compliance; conducts DPIAs for all new features handling special category data; manages data subject rights; liaises with ICO; reviews this policy annually; maintains AI Register
Security Lead / Head of Engineering	Day-to-day management of technical security controls; vulnerability management; penetration testing coordination; SIEM oversight; MIS integration security; AI model security
All Employees and Contractors	Comply with this policy and all security procedures; complete mandatory security training; report suspected incidents and vulnerabilities immediately; protect devices, credentials, and data in their care
Customers (Schools/LAs as Data Controllers)	Responsible for their own use of the platform; must configure access controls appropriately; must report suspected data breaches involving their data to ProvisionIQ immediately

2.2 Risk Management

ProvisionIQ maintains a formal Information Security Risk Register, reviewed quarterly by the Security Committee and annually as part of the ISO 27001 ISMS review. Risks are assessed using a likelihood/impact matrix (1–5 scale) and assigned owners. Risks above the defined risk appetite threshold require formal treatment plans approved by the CTO. The register includes a dedicated section for AI/ML risks and MIS integration risks, reviewed at every Security Committee meeting.

2.3 Security Objectives and KPIs

Objective	KPI	Target
Maintain ISO 27001 certification	Annual surveillance audit passed with no major non-conformities	100% — zero major NCs
Maintain Cyber Essentials Plus	Annual renewal passed	100% pass
Patch critical vulnerabilities	Time from disclosure to remediation	< 24 hours critical; < 72 hours high
Security training completion	% of staff completing annual training	100% by end of January each year

Incident detection	Mean time to detect (MTTD) significant incidents	< 4 hours during business hours
Incident response	Mean time to respond (MTTR) to P1 incidents	< 1 hour from detection
Third-party security reviews	% of sub-processors and AI providers reviewed annually	100%
AI feature audit	All AI features in AI Register with current security assessment	100% coverage; quarterly review
MIS integration review	Security assessment of all active MIS integrations	Annually and after any MIS API change

3. Information Classification

All information assets must be classified according to the scheme below. The classification determines the security controls that must be applied.

Classification	Definition	Examples / Handling
RESTRICTED	Highly sensitive; could cause serious harm or legal liability if disclosed	Pupil SEND/health/safeguarding records; EHCPs; ISPs; multi-agency referral records; MIS-sourced pupil data; AI model outputs referencing individual pupils; source code; encryption keys; investor data; DPO investigation records. Access strictly controlled; encrypted at rest and in transit; no external sharing without explicit authorisation; audit logging mandatory
CONFIDENTIAL	Sensitive; could cause commercial harm or reputational damage if disclosed	Customer contracts; pricing; staff salaries; internal security reports; vulnerability disclosures; board minutes; AI model configurations. Need-to-know access; encrypted in transit; not shared outside organisation without NDA
INTERNAL	For internal use; low harm if disclosed but not intended for public view	Internal procedures, policies, meeting notes, general staff communications, non-sensitive product roadmap. Standard access controls; not to be posted publicly
PUBLIC	Intended for public distribution	Marketing materials, published policies, product documentation, job postings. No additional restrictions; standard integrity checks apply

Default Classification

Any information that has not been explicitly classified should be treated as CONFIDENTIAL until the owner assigns a classification. All pupil personal data — including any data received via MIS integration or processed by AI features — is automatically classified as RESTRICTED regardless of other labelling. AI-generated outputs referencing individual pupils are RESTRICTED even if the underlying prompt did not contain personal data. Information owners are responsible for classifying new assets within 5 business days of creation.

4. Access Control

4.1 Principles

- Least Privilege: users are granted the minimum access rights necessary to perform their role. No blanket administrator rights without justification.
- Need to Know: access to RESTRICTED data requires documented business justification.
- Separation of Duties: critical functions (e.g. production deployments, key management, AI model configuration changes) require two authorised persons.
- Just-In-Time Access: privileged access to production systems is granted on a time-limited, per-task basis where technically feasible.

4.2 User Account Management

Control	Requirement
Account creation	All user accounts (staff and platform users) created via formal request; approved by the relevant manager or school administrator; logged in the access register
Authentication	All platform authentication via Keycloak OIDC with PKCE flow. No legacy username/password-only flows for RESTRICTED data access.
Password policy	Minimum 12 characters; must include uppercase, lowercase, digit, and special character; checked against known-breached password lists (HaveIBeenPwned API); not reused across systems
Multi-factor authentication (MFA)	Mandatory for all internal ProvisionIQ systems and all administrator accounts; mandatory for all platform users accessing RESTRICTED data; enforced for production infrastructure access
Session management	Inactive sessions timeout after 30 minutes for RESTRICTED data access; 60 minutes for CONFIDENTIAL; automatic re-authentication required
Privileged access	All privileged/admin access logged; reviewed monthly; production database access requires dual authorisation and is time-limited

Account review	All accounts reviewed quarterly; dormant accounts (no login for 60+ days) suspended pending review; departed employee accounts disabled within 2 hours of confirmed departure
Account termination	On departure: accounts disabled within 2 hours; passwords reset; API keys revoked; Keycloak sessions invalidated; hardware returned; MIS integration credentials rotated; completion logged

4.3 Remote Working and BYOD

- All remote access to ProvisionIQ systems must be over an encrypted VPN or zero-trust network access (ZTNA) solution.
- Remote workers must use ProvisionIQ-issued devices (or devices that meet the Device Security Standard) for accessing RESTRICTED or CONFIDENTIAL data.
- Personal devices (BYOD) are not permitted to access RESTRICTED data unless enrolled in Mobile Device Management (MDM) and compliant with the Device Security Standard.
- Public Wi-Fi must not be used without VPN protection for any ProvisionIQ system access.
- All devices must have full-disk encryption enabled and automatic lock after 5 minutes of inactivity.

5. Cryptography and Encryption

Context	Standard / Requirement
Data at rest (databases, file storage, S3 evidence store)	AES-256 encryption applied to all production data stores including S3-backed evidence and observation file storage. Key management via dedicated KMS; keys stored separately from data and rotated at least annually.
Data in transit (web/API)	TLS 1.3 minimum. Older TLS versions (1.0, 1.1, 1.2) disabled on all public endpoints. HSTS enforced with minimum 1-year max-age. Certificate pinning on mobile clients.
Data in transit (internal/MIS integration)	TLS 1.2 minimum for inter-service communication; mTLS enforced for sensitive microservice communication. All MIS integration API calls authenticated and encrypted end-to-end. MIS credentials stored in secrets management; never logged.
Backups	AES-256 encrypted at point of backup creation. Encryption keys stored separately from backup data in an isolated vault.
Code signing	All production deployments require a signed artefact from the CI/CD pipeline. Signing keys held in hardware security module (HSM).
Keycloak / OIDC	All tokens short-lived (access tokens: 5 minutes; refresh tokens: 24 hours). PKCE enforced on all public clients. Token storage in memory only — never localStorage.

Secrets management	API keys, database credentials, MIS integration tokens, and secrets stored in a dedicated secrets management tool. Never stored in source code, environment files, or version control.
Password hashing	User passwords hashed using bcrypt (cost ≥ 12) or Argon2id. Salted per-account. Never stored in plaintext or reversibly encrypted.
Prohibited practices	Strictly prohibited: MD5 or SHA-1 for security purposes; DES, 3DES, RC4; self-signed certificates in production; private keys in version control; hardcoded cryptographic keys in source code.

6. Physical and Environmental Security

6.1 Cloud Infrastructure

ProvisionIQ's production infrastructure is hosted entirely in UK-based cloud data centres. All S3-backed evidence storage, database backups, and primary data stores are UK-resident. Physical security of data centre facilities is governed by our cloud provider's ISO 27001 and ISO 27017 certifications, reviewed annually. Evidence of certification is retained on file.

6.2 Office and Remote Working Environments

- Clear desk policy: RESTRICTED and CONFIDENTIAL materials must be secured when workstations are unattended.
- Screens must be locked when stepping away from a workstation.
- Physical documents containing personal data must be stored in locked cabinets and shredded (cross-cut) when no longer required.
- Visitors to ProvisionIQ premises must be signed in, accompanied at all times, and must not be given access to screens displaying RESTRICTED data.
- Whiteboards and printed materials containing RESTRICTED or CONFIDENTIAL information must be cleared after meetings.

6.3 Device Security

Control	Requirement
Full disk encryption	Mandatory on all ProvisionIQ-issued and BYOD devices accessing RESTRICTED data (BitLocker/FileVault/LUKS)
Antivirus/EDR	Mandatory endpoint detection and response (EDR) on all managed devices; definitions updated automatically
OS updates	Critical security patches applied within 24 hours; all other OS updates within 14 days
Screen lock	Automatic lock after 5 minutes inactivity; PIN/password/biometric required to unlock

Secure disposal	Devices wiped to NIST 800-88 standard before disposal, repurposing, or return. Certificate of destruction obtained for physical destruction.
Lost/stolen devices	Must be reported to Security Lead within 1 hour; remote wipe initiated within 2 hours

7. Network and System Security

7.1 Network Controls

- All production environments are segmented from development, staging, and corporate networks. Cross-segment communication requires explicit firewall rules with documented justification.
- Web Application Firewall (WAF) deployed in front of all customer-facing services. Rules reviewed monthly and updated within 24 hours of new threat intelligence.
- DDoS mitigation service active on all public endpoints.
- All inbound connections default-deny. Only required ports and protocols explicitly whitelisted.
- Intrusion detection / intrusion prevention system (IDS/IPS) deployed. Alerts reviewed in real time during business hours; out-of-hours via on-call rotation.
- All network traffic between production services logged. Logs retained for 7 years. Immutable and tamper-evident.
- The Parent Portal is treated as a consumer-facing high-risk surface and subject to additional WAF rules, rate limiting, and anomaly detection appropriate to a public-internet authentication endpoint handling children's data.

7.2 MIS Integration Security

ProvisionIQ's API-first architecture integrates directly with school Management Information Systems (MIS). MIS integrations represent a privileged data channel carrying personally identifiable pupil data. The following controls are mandatory for all MIS integrations:

Control	Requirement
Credential management	MIS API credentials (tokens, keys, OAuth secrets) stored exclusively in the secrets management system. Never hardcoded, logged, or stored in environment files or version control.
Least-privilege scoping	MIS API tokens scoped to the minimum data fields required. Read-only where the integration does not require write-back. Scopes documented and reviewed annually.
Encryption in transit	All MIS API calls made over TLS 1.2 minimum; TLS 1.3 where supported by the MIS provider. Certificate validation enforced; self-signed certificates not accepted.

Data minimisation at ingestion	MIS data is filtered at the point of ingestion. Only fields required for SEND provision management are retained on the ProvisionIQ platform. Raw MIS payloads are not stored.
Credential rotation	MIS integration credentials rotated at least every 6 months and immediately on any suspected compromise or staff departure with access to the credential.
Integration monitoring	All MIS integration calls logged with timestamp, data volume, and response code. Anomalies (unexpected data volumes, error spikes, off-hours activity) trigger alerts to the Security Lead.
Third-party MIS provider assessment	MIS provider security posture reviewed as part of the Tier 1/2 supplier assessment process. API security documentation reviewed before integration goes live.

7.3 Vulnerability Management

Activity	Frequency / Target
Automated vulnerability scanning (infrastructure)	Daily scans of all production infrastructure. Critical findings reviewed within 4 hours.
Automated dependency scanning (code)	Every code commit and pull request. Blocking: critical CVEs prevent merge. Non-blocking: high CVEs remediated within 72 hours.
Penetration testing (external)	Annual, by CREST-accredited third-party firm. Full scope: web application (including Parent Portal), API, MIS integration endpoints, infrastructure, social engineering, AI feature attack surface. Additional test following any significant architectural change.
Penetration testing (internal)	6-monthly internal red team exercise. Bug bounty programme in place post-launch.
Patch management	Critical: within 24 hours; High: within 72 hours; Medium: within 30 days; Low: next scheduled maintenance window.

7.4 Security Monitoring and SIEM

ProvisionIQ maintains centralised security monitoring covering all production systems. Log sources include: application logs; web server access logs; authentication events (Keycloak audit log); database query logs; MIS integration pipeline logs; AI feature invocation logs; S3 access logs; infrastructure metrics; and WAF/IDS alerts. All logs are shipped to a centralised SIEM system in real time. Alerts are triaged by the on-call engineer and escalated per the Incident Response Policy. AI feature invocations that access RESTRICTED pupil data generate a dedicated log entry reviewed weekly by the Security Lead.

8. Artificial Intelligence and Machine Learning Security

ProvisionIQ incorporates AI-assisted features including provision planning support and automated compliance reporting. Because these features may process or reference RESTRICTED pupil data, they are subject to controls that go beyond standard software security requirements.

8.1 AI Register

The DPO maintains an AI Register documenting every AI feature in production and development. Each entry records: feature name and description; data inputs (including whether RESTRICTED data is used); model provider and hosting location; anonymisation or pseudonymisation applied; legal basis for processing; DPIA reference; date of last security review; and responsible owner. The AI Register is reviewed quarterly by the Security Committee and annually as part of the ISO 27001 ISMS review.

8.2 Controls for AI Features Accessing Pupil Data

Control	Requirement
No identifiable data to third-party models	Identifiable pupil personal data must not be sent to any third-party AI model provider (including large language model APIs) without: (a) full anonymisation or pseudonymisation verified by the DPO, (b) explicit written consent from the Data Controller (school/LA), and (c) a signed Data Processing Agreement with the AI provider.
AI provider due diligence	All AI service providers assessed as Tier 1 suppliers under §9. UK or equivalent data residency required for any processing of RESTRICTED data. Training data use prohibited without explicit consent.
Prompt injection defence	All AI features that accept user-supplied input must implement prompt injection mitigations. User input sanitised before inclusion in model prompts. System prompts protected and not user-accessible.
Output validation	AI-generated outputs referencing individual pupils must be reviewed and approved by a qualified professional before being saved to a pupil record. AI-generated content is clearly labelled in the platform UI as AI-assisted.
AI-specific audit logging	Every invocation of an AI feature that accesses or references RESTRICTED data is logged with: timestamp; user ID; feature name; data categories accessed; and whether the output was accepted, modified, or rejected by the user.
Model deprecation	When an AI feature or underlying model is deprecated, all associated pupil data used in prompts or cached outputs is securely deleted. Deprecation is treated as a data deletion event and logged.
No training on pupil data	ProvisionIQ does not use identifiable pupil data to train, fine-tune, or evaluate any AI model without explicit written consent from the Data Controller and Board approval.

8.3 Automated Decision-Making

ProvisionIQ AI features are advisory only. No AI feature makes or records an automated decision that produces legal or similarly significant effects for any individual pupil. All AI-generated suggestions are presented to a qualified human professional for review, and the human decision is the recorded outcome. This is enforced at the product level and verified in each DPIA.

9. Secure Software Development

9.1 Secure Development Lifecycle

ProvisionIQ follows a security-integrated Software Development Lifecycle (SDL) aligned with OWASP principles. Security requirements are defined at the design stage, not retrofitted.

SDL Phase	Security Activity	Responsible
Requirements	Threat modelling; security user stories; DPIA trigger assessment; AI Register entry for any new AI feature	CTO + DPO
Design	Architecture security review; data flow diagrams; trust boundary analysis; MIS integration security design	CTO
Development	Secure coding standards (OWASP Top 10); peer code review; secrets scanning; prompt injection review for AI features	All developers
Testing	SAST; DAST; dependency scanning; unit tests for security controls; AI feature output validation testing	CTO
Deployment	Signed artefacts; immutable infrastructure; change approval; automated rollback capability	CTO
Operations	Continuous monitoring; penetration testing; vulnerability management; AI Register review; MIS integration audit	CTO
Decommission	Secure data deletion; AI prompt cache deletion; certificate revocation; access removal; documentation	CTO

9.2 Key Secure Coding Requirements

- All input validated and sanitised; parameterised queries mandatory (no raw SQL construction).
- Output encoding applied to prevent XSS; Content Security Policy (CSP) headers enforced.
- Authentication and session management follows OWASP Authentication Cheat Sheet; Keycloak OIDC/PKCE enforced.
- All sensitive actions protected by CSRF tokens.
- Error messages must not reveal stack traces, internal paths, or sensitive system information to end users.
- Logging must not record passwords, API keys, session tokens, personal data, or AI prompts containing personal data in plaintext.

- Third-party libraries reviewed for known vulnerabilities before adoption; licence compatibility confirmed.
- AI prompt templates reviewed by the Security Lead before deployment to production.

10. Third-Party and Supply Chain Security

10.1 Supplier Security Assessment

Supplier Tier	Assessment Requirements
Tier 1 — Critical (access to RESTRICTED data, core infrastructure, MIS integration, AI model providers)	Full security questionnaire; evidence of ISO 27001 or Cyber Essentials Plus (or equivalent); Data Processing Agreement (DPA) executed; UK or approved data residency confirmed; annual review; right-to-audit clause; penetration testing evidence requested annually; AI providers: training data prohibition clause required
Tier 2 — Important (access to CONFIDENTIAL data or internal systems)	Security questionnaire; evidence of security accreditation or equivalent controls; DPA if processing personal data; annual review
Tier 3 — Standard (no access to personal data, low-risk tools)	Basic due diligence; supplier security policy reviewed; annual check for changes

10.2 Sub-Processor Management

ProvisionIQ maintains a current list of all sub-processors at provisioniq.co.uk/sub-processors. Before adding a new sub-processor that processes customer personal data, ProvisionIQ will notify all affected Data Controllers (schools/LAs) with at least 14 days' notice. Data Controllers may object to a new sub-processor, in which case ProvisionIQ will work with them to find an alternative or allow termination without penalty.

10.3 Contractual Security Requirements

All contracts with Tier 1 and Tier 2 suppliers must include:

- Data Processing Agreement (where personal data is processed)
- Obligation to maintain equivalent security standards to ProvisionIQ
- Incident notification requirement: supplier must notify ProvisionIQ within 24 hours of any suspected breach
- Right to audit or inspect supplier security controls on reasonable notice
- Secure deletion of ProvisionIQ data within 30 days of contract termination
- Prohibition on sub-contracting to fourth parties without ProvisionIQ's prior written consent
- For AI providers: explicit prohibition on using ProvisionIQ or customer data to train any AI model

11. Incident Response

11.1 Incident Severity Classification

Severity	Definition	Initial Response	Escalation
P1 — Critical	Confirmed breach or loss of RESTRICTED pupil data; full platform outage; active ransomware; confirmed unauthorised access to production	Immediate: Security Lead + CTO + DPO paged within 15 minutes	CEO and Board notified within 1 hour; ICO notification assessed within 2 hours; schools notified within 4 hours if data at risk
P2 — High	Suspected breach; significant vulnerability confirmed in production; partial outage affecting multiple schools; MIS integration compromise	Security Lead + CTO notified within 30 minutes; bridge call opened within 1 hour	DPO engaged; ICO notification assessed; schools informed if risk identified
P3 — Medium	Single-school service degradation; suspected (unconfirmed) security event; policy violation identified; AI feature producing unexpected outputs with personal data	Security Lead notified within 2 hours; investigation commenced same business day	Escalate to P2 if personal data confirmed at risk
P4 — Low	Minor policy violation; low-impact anomaly; unsuccessful attack attempt	Security Lead notified within 1 business day; logged in incident register	No external notification unless risk identified

11.2 ICO Notification Procedure

ProvisionIQ has a legal obligation to notify the ICO of personal data breaches that are likely to result in a risk to the rights and freedoms of individuals, within 72 hours of becoming aware of the breach. The following procedure applies:

- The DPO assesses the breach within 2 hours of a P1 or P2 incident being declared, using the ICO's breach assessment criteria.
- If notification is required, the DPO submits the ICO report within 72 hours. A draft notification is prepared within 4 hours of the decision to notify.
- Affected Data Controllers (schools/LAs) are notified without undue delay and in all cases before the ICO is notified, unless doing so would prejudice the investigation.
- If a full notification cannot be made within 72 hours, the ICO is notified with the information available and a reason for the delay.
- All decisions (to notify or not to notify) are documented in the Breach Register with reasoning.
- The DPO maintains a template ICO notification and a Breach Register. Both are reviewed at least annually.

12. Human Resources Security

12.1 Pre-Employment

Check	Requirement
Identity verification	Verified against government-issued photo ID before start
Right to Work	Verified per UK Home Office guidance before start
References	Two professional references checked before start
Criminal record check	Enhanced DBS with Children's Barred List check for all staff with regular access to pupil personal data; standard DBS for all others with system access
Credential verification	Qualifications and certifications relevant to the role verified

12.2 Security Awareness Training

Training	Frequency / Target
Information security induction	All new employees and contractors before system access is granted
Annual security awareness training	All employees and contractors; covers phishing, social engineering, GDPR, password hygiene, incident reporting, clean desk, BYOD, AI security, MIS integration handling. Completion tracked; mandatory.
Phishing simulation	Quarterly simulated phishing campaigns; individuals who fail receive targeted remedial training
Developer secure coding training	Annual; covers OWASP Top 10, prompt injection, AI security, MIS API security; mandatory for all engineering staff
Incident response tabletop exercise	Annual; all relevant staff; tests this policy and the Incident Response Policy including AI and MIS incident scenarios

12.3 Disciplinary and Offboarding

Violations of this policy are treated as disciplinary matters. Depending on severity, violations may result in: formal warning; suspension of system access pending investigation; dismissal; or referral to law enforcement or regulatory authorities.

On departure of any employee or contractor: all accounts disabled within 2 hours of confirmed last working day; Keycloak sessions invalidated; MIS integration credentials rotated; AI Register updated to reassign ownership; all ProvisionIQ devices returned and wiped; all physical access credentials revoked; knowledge transfer and security checklist completed by the manager.

13. Asset Management

ProvisionIQ maintains a formal Asset Register covering all information assets including hardware, software, data assets, MIS integration configurations, and AI model components. The register is reviewed quarterly by the Security Lead.

13.1 Hardware Assets

- All ProvisionIQ-issued devices registered in the Asset Register before issue and tagged with a ProvisionIQ asset ID.
- Mobile devices enrolled in MDM within 24 hours of issue.
- Hardware inventory reconciled monthly; discrepancies investigated within 5 business days.

13.2 Software and AI Assets

- All production software dependencies recorded in the Software Bill of Materials (SBOM), maintained in version control.
- All AI models, APIs, and AI feature components listed in the AI Register with version, provider, and security assessment date.
- Open-source software reviewed for licence compatibility and security before use.
- Unlicensed or unauthorised software is prohibited on all ProvisionIQ systems.

13.3 Data Assets

- All data assets documented in the Record of Processing Activities (RoPA) maintained by the DPO.
- Data flows between systems — including MIS integration pipelines and AI feature data flows — documented and reviewed when any new integration is introduced.
- Shadow IT (unauthorised use of cloud services or applications for ProvisionIQ data) is prohibited.
- No pupil data to be used in any personal AI tool, consumer chatbot, or unauthorised AI service by any member of staff.

14. Business Continuity and Disaster Recovery

14.1 Recovery Objectives

Objective	Target
Recovery Time Objective (RTO)	4 hours for full platform restoration following a major incident (P1)
Recovery Point Objective (RPO)	1 hour maximum data loss (backed by hourly incremental backups)
Uptime SLA	99.5% per calendar month (excluding scheduled maintenance)
Scheduled maintenance window	Maximum 4 hours/month; at least 48 hours' notice; outside business hours where possible

14.2 Backup Strategy

Backup Type	Schedule and Retention
Incremental backup	Hourly; retained 7 days
Daily full backup	00:00 UTC; retained 30 days
Weekly backup	Sunday 02:00 UTC; retained 13 weeks
Monthly snapshot	First Sunday of month; retained 12 months
Offsite / geo-redundant copy	All backups replicated to secondary UK facility within 1 hour of creation

Backups are AES-256 encrypted, stored in a separate UK facility, and access-controlled independently of production systems. Backup restoration is tested quarterly. A full disaster recovery drill is conducted annually.

14.3 Business Continuity Planning

ProvisionIQ maintains a Business Continuity Plan (BCP) covering: key person dependency; supplier failure scenarios including MIS provider failure and AI provider outage; data centre failure; cyberattack scenarios including ransomware; and pandemic/mass absence scenarios. The BCP is reviewed annually and following any significant incident.

15. Compliance and Audit

15.1 Regulatory and Standards Compliance

Standard / Regulation	How ProvisionIQ Maintains Compliance
Cyber Essentials Plus	Annual renewal; external technical assessment by accredited assessor; covers all five controls (firewalls, secure configuration, access control, malware protection, patch management)
UK GDPR / DPA 2018	DPO appointed; RoPA maintained; DPIAs conducted for all high-risk processing including every new AI feature; data subject rights procedures in place; ICO breach notification procedure tested
Children and Families Act 2014 / SEND Code of Practice	Platform features align with statutory SEND framework; data handling respects the heightened sensitivity of EHCP and ISP records
PECR	Cookie consent mechanism implemented; marketing consent records maintained; electronic marketing only to opted-in recipients

NCSC Cyber Security Principles	10 Steps to Cyber Security aligned; Board engagement; risk management; network security; malware prevention; monitoring; home/mobile working; user privilege management; incident management; user education

15.2 Internal Audit

An internal security audit is conducted annually, reviewing compliance with this policy and associated procedures. The audit covers a sample of access logs, change records, training records, supplier assessments, AI Register entries, MIS integration logs, and incident records. Findings are reported to the CTO and Board. All high-severity findings must have a remediation plan within 30 days.

15.3 External Audit and Penetration Testing

An independent CREST-accredited security firm conducts an annual penetration test. The scope explicitly includes: web application testing (including the Parent Portal and all authenticated user journeys); API security testing; MIS integration endpoint testing; AI feature attack surface (prompt injection, data exfiltration via AI); infrastructure testing; and social engineering. Critical and high findings must be remediated before the report is marked closed. Summary findings are available to customers on request.

16. Policy Review and Exceptions

16.1 Policy Review

This policy is reviewed at least annually by the CTO and DPO, and following any of: a significant security incident; a material change to ProvisionIQ's technology, operating model, or AI capabilities; a change to relevant law or regulatory guidance; or an ISO 27001 surveillance audit finding.

16.2 Exception Process

Where a business requirement makes strict compliance with a specific control impractical, an exception may be requested via the CTO. All exceptions must be: documented in writing with business justification; time-limited (maximum 90 days, renewable); accompanied by compensating controls; approved by the CTO; and recorded in the Exception Register. No exception may be granted for controls relating to RESTRICTED pupil data or AI governance without DPO co-approval. Exceptions are reviewed monthly by the Security Committee.

Related Policies

This policy is the top-level information security document and is supported by: Incident Response Policy · Data Protection and Privacy Policy · Acceptable Use Policy · Recruitment and DBS Policy · AI Governance Policy · Data Retention Policy · Business Continuity Plan. Where a sub-policy conflicts with this policy, this policy takes precedence.

Version History

Version	Date	Author	Changes
1.0	May 2026	CTO	Initial policy — ISMS launch at platform go-live
2.0	July 2026	CTO / DPO	Added: AI/ML security controls (§8); MIS integration security (§7.2); incident severity framework with ICO notification procedure (§11); parent portal and AI surface in pen test scope; Keycloak/OIDC/PKCE controls; S3 evidence store encryption; AI Register requirement; shadow IT / consumer AI prohibition; offboarding expanded for MIS credentials and AI Register

Board Approval

This Information Security Policy has been reviewed and approved by the Board of Directors of ProvisionIQ Ltd. It takes effect from July 2026 and supersedes Version 1.0 (May 2026). The Board commits the resources, oversight, and culture necessary to achieve and maintain the security objectives set out in this policy.

Signed on behalf of the Board:  Date: 07/06/2026

Name and Title: Dan Howard- CEO