Cyber Security Policy

Document owner: Managing Director, Danpol Ltd.
Published: 1 December 2025
Applies to: All employees, contractors, suppliers with access to Danpol information assets, cloud services, or operational technology.

1. Purpose and scope

This policy sets minimum cyber security controls for protecting Danpol data, client information, and operational systems. It aligns with ISO 27001/27701, UK GDPR, NCSC 10 Steps, and Constructionline CAS digital governance clauses.

2. Governance and responsibilities

- **Managing Director:** Provides resources, signs the Information Security Management System (ISMS), and holds ultimate accountability.
- **Information Security Lead:** Maintains the ISMS, monitors threats, reports KPIs, and coordinates incident response.
- **Department leads and project managers:** Ensure local adherence, maintain asset registers, and validate supplier controls.
- **All users:** Follow secure working practices, complete training, and report suspicious activity immediately.

3. Access control

- Role-based access granted via Azure AD, using least privilege and documented approvals.
- Multi-factor authentication enforced on all corporate accounts, VPN, and privileged tooling.
- Accounts reviewed quarterly; dormant accounts disabled after 30 days.
- Shared credentials are prohibited; service accounts use managed secrets.

4. Asset and data protection

- Laptops, tablets, and mobiles managed through MDM with disk encryption, anti-malware, and remote wipe.
- Only approved cloud platforms (Microsoft 365, SharePoint, Autodesk Construction Cloud) may store regulated data.
- Sensitive project files tagged using Microsoft Purview; external sharing requires data loss prevention (DLP) policy exemptions.
- Removable media is blocked by default; exceptions require director approval and encryption.

5. Network and application security

- All internet traffic routes through secure web gateways with threat detection and TLS inspection.
- Firewalls and SD-WAN policies segregate site networks, OT devices, and corporate services.
- Applications follow secure development lifecycle (threat modelling, dependency scanning, penetration testing prior to go-live).
- Vendors hosting Danpol data must provide penetration test evidence annually.

6. Monitoring and incident response

- Managed detection and response (MDR) tooling collects endpoint, network, and cloud logs into a SIEM with 24/7 analyst coverage.
- Alerts triaged within 15 minutes; high-severity incidents escalated to the Gold Incident Team.
- Incident response playbooks cover ransomware, account compromise, data exfiltration, and OT disruption.
- Lessons learned feed into security awareness campaigns and tabletop exercises each quarter.

7. Training and awareness

- Mandatory induction and annual refresher modules cover phishing, password hygiene, data handling, and secure collaboration.
- Quarterly phishing simulations track behavioural improvement; users failing two tests receive targeted coaching.
- Project-specific briefings explain client security clauses, BIM collaboration etiquette, and OT safety protocols.

8. Supplier and third-party controls

- Suppliers must complete cyber questionnaires (aligned to NCSC CAF) and provide evidence of certifications or compensating controls.
- Contracts mandate incident notification within 24 hours, audit rights, and data return/destruction procedures.
- Critical SaaS platforms require backup arrangements and business continuity tests annually.

9. Business continuity and recovery

- Workstations and cloud services backed up daily with immutable storage; recovery objectives documented per system.
- OT environments maintain offline configuration backups and failover procedures.
- Cyber incident plans integrate with the wider Business Continuity and Crisis Management framework.

10. Compliance and review

Security controls are audited internally twice a year and externally at least annually. Policy updates occur alongside ISMS management reviews or when threat landscape changes. Evidence packs, including logs and risk registers, are stored in the Danpol policy vault.

Signed on behalf of Danpol Ltd.:

Daniel Nowakowski

Managing Director

1 December 2025

Digitally signed with authorisation stored in the Danpol policy vault.