GROUP POLICY

Group Information Security Policy (GISP)

WEBSITE
Published June 2026

DIPLOMA PLC
VALUE-ADD SOLUTIONS

Contents

Document Control

Policy owner:	Group Integration Director
Published / effective from:	June 2026
Review frequency:	Annual
Next review date:	June 2027
Version:	4.0

1 Purpose

This policy sets out the framework for protecting the confidentiality, integrity, and availability of information assets across Diploma PLC ("Diploma") and its businesses. It provides a consistent and defensible approach to information security, helps manage cyber risks, and supports a culture of security awareness and resilience across the Group.

In plain terms, this policy explains how we protect information at Diploma. It applies to anyone working with our data or systems, including third parties. Every business must take steps to keep information secure - this includes having the right controls in place, following shared standards, and being ready to deal with cyber incidents. The goal is to reduce risk, protect the business, and support a strong security culture across the Group.

2 Scope

This policy applies to all employees, contractors, consultants, and third-party vendors who have access to Diploma's information assets, regardless of location or role. It applies across all Diploma businesses and covers all forms of information assets, including but not limited to:

- Electronic data and systems
- Physical records
- Intellectual property
- Customer, supplier and third-party information
- Operational and financial data
- Communications platforms and tools

3 Policy Statement

Diploma is committed to maintaining a strong and defensible information security posture by implementing risk-based measures to protect the Group's information assets. These measures are designed to ensure confidentiality, integrity, and availability, comply with relevant regulations, and support the Group's strategic objectives.

Diploma aims to build cyber resilience by enabling all businesses to respond to and recover from cyber incidents. This is achieved through:

- Compliance with applicable laws, regulations, and standards.
- Clear roles and responsibilities for information security.
- Promoting a culture of security awareness, including regular training for staff.
- Implementing and maintaining appropriate controls.
- Ongoing monitoring and improvement.
- Incident response, business continuity, and disaster recovery planning.

4 Requirements

4.1 Reference Framework

Framework Adoption

The National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) is the mandated framework for assessing and managing information security risks across the Group. All businesses must leverage the NIST CSF as the foundation for their local information security approach.

Where appropriate — for example, to meet specific regulatory, customer, or operational requirements — businesses may also leverage ISO27001. ISO27001 and NIST CSF are not mutually exclusive and share considerable overlap. Any implementation of ISO27001 should be designed to complement, not replace, the Group's core use of NIST CSF. Where there is a clear benefit, businesses may adopt selected practices from other recognised frameworks, provided these align with Group objectives and do not conflict with the requirements of NIST CSF.

Periodic Reviews

Each business must complete an annual self-assessment against the NIST CSF to evaluate its alignment and maturity. A standard assessment template will be provided and reviewed by the Group Integration Director. In addition to the annual self-assessment, Diploma will carry out formal, independent reviews on a three-year rolling cycle. These reviews aim to ensure consistent application of the NIST CSF across the Group and to identify opportunities for continuous improvement.

4.2 Business Representatives

Each business must appoint a Business Information Security Representative (BISR) and, where feasible, a Technical Information Security Representative (TISR). These individuals are responsible for overseeing implementation of local security measures, supporting policy compliance, and serving as liaisons to the Group Integration Director. If no dedicated resources are available, the BISR will assume primary responsibility for security operations and incident response at the local level.

4.3 Local Policies and Procedures

Formal Documentation

Each business must develop and maintain local policies and procedures that support the implementation of this Group Information Security Policy (GISP), tailored to its specific business and operational needs. These documents must be reviewed and updated at least annually.

Security Awareness & Training

Each business must ensure that staff complete security-awareness training on joining and at least annually thereafter, appropriate to their role. Training should cover the business's key cyber risks - including phishing and social engineering - and how to report a suspected incident. Completion should be recorded and made available on request.

Emerging Technologies

Diploma encourages the adoption of innovative technologies - such as Generative AI and process automation - where they deliver clear business benefits. Before implementation, businesses must conduct a risk assessment to evaluate potential impacts and define appropriate mitigation measures. Supporting documentation and user guidance must be created and shared with relevant staff.

4.4 Information Classification and Handling

All information must be classified based on its sensitivity and business impact, using at least the following categories: Confidential, Internal, and Public.

Businesses must apply appropriate handling, storage, access, and disposal rules based on classification. Retention periods should reflect legal, regulatory, and operational requirements. Where possible, content associated with decommissioned user accounts should be reviewed, securely archived, or deleted based on its classification and business need.

4.5 Information Asset Protection

Each business must assess its information assets for risk and protect them using appropriate organisational and technical controls, aligned with the Group's reference framework. A layered security approach must be applied to support the principle of defence in depth.

The Group Cyber Control Framework (GCCF) supports this framework by defining a baseline set of cyber security controls required across the Group. It establishes minimum expectations for securing systems, data, and services, and is aligned with the NIST CSF to ensure consistent application of core security principles. It also serves as the foundation for local implementation, continuous improvement, and defensible risk management.

4.6 Access Control and Authentication

Each business must implement authentication and access controls in line with the principle of least privilege and need to know basis. Strong authentication (such as multi-factor authentication) must be used where appropriate, particularly on systems that can be accessed from the public internet.

4.7 Monitoring and Logging

Monitoring and logging must be implemented to track systems and access activity, supporting threat detection, incident response, compliance, and forensic investigations. All monitoring must meet local policy and regulatory requirements.

4.8 Incident Management

Each business must be able to detect, respond to, and recover from cyber security incidents in a timely and consistent manner in alignment with the Group Incident Response Plan (GIRP). Businesses must:

- Maintain a Local Incident Response Plan (LIRP) aligned with the GIRP, including clear roles and escalation paths.
- Ensure the LIRP is reviewed annually.
- Integrate the LIRP with Local Business Continuity Plans (LBCP) and Local Disaster Recovery Plans (LDRP) to support coordinated recovery.

4.9 Third-Party and Vendor Security

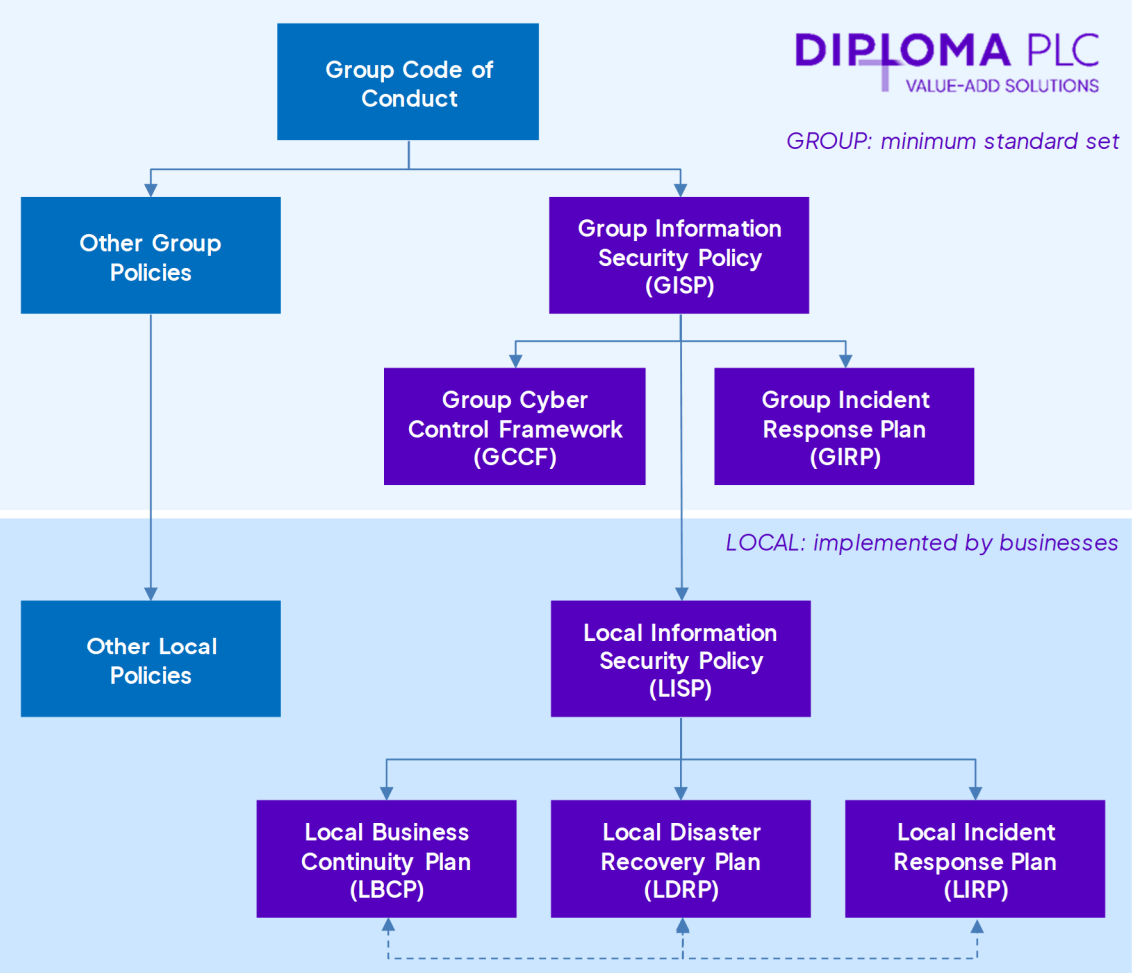
Third-party providers with access to Diploma systems or data must be subject to appropriate due diligence, contractual terms, and security controls. Each business must assess and manage third-party risk in line with the reference framework and the GCCF. Further expectations and practical tools are set out in the GCCF.

4.10 Acquisitions

Newly acquired businesses come within the scope of this policy from the date of completion. As part of post-acquisition onboarding, each acquired business must, within the timeframe agreed with the Group Integration Director:

- Adopt this Group Information Security Policy (GISP) and the supporting Group Cyber Control Framework (GCCF);
- Implement the Key Cyber Controls (KCC) baseline as a priority, with any gaps identified, risk-assessed and placed on a remediation plan; and
- Establish a Local Incident Response Plan (LIRP) aligned to the Group Incident Response Plan (GIRP).
- Onboarding progress, control gaps and remediation timelines are monitored by the Group Integration Director and reported through the Group's governance forums.

5 Related Policies



A collection of Group-wide policies can be found on our website and Learning Management System:

- Group Information Security Policy (GISP)
- Group Cyber Control Framework (GCCF)
- Group Incident Response Plan (GIRP)

6 Compliance & Non-Compliance

Businesses must comply with applicable local and international laws on information security, data protection, and cyber security.

The Group Chief Financial Officer is the executive sponsor for information security and cyber security. The Group Integration Director oversees implementation of this policy and monitors the Group's overall cyber security posture. Periodic updates will be provided to the Board.

Any breach of this policy may result in disciplinary action, up to and including dismissal, in accordance with Diploma's Disciplinary Procedure. Contractual relationships may also be reviewed or terminated where appropriate.

7 Contacts

If you have any queries, please contact the Group Integration Director:

Carolyne.Dick@diplomaplc.com

8 Definitions

Acronym	Definition	Description
BCP	Business Continuity Plan	A structured approach to continuing business functions upon an incident.
LBCP	Local Business Continuity Plan	A local document establishing how essential business functions will continue during and after a disruptive incident. Activated if business operations are affected based on defined criteria.
BISR	Business Information Security Representative	A designated person responsible for overseeing security compliance at the business unit level.
-	Defence in Depth Principle	A cyber security principle that states multiple layers of measures should be implemented to defend assets, so if one layer fails, others can compensate.
DRP	Disaster Recovery Plan	A structured approach to restore normal operation after an incident.
LDRP	Local Disaster Recovery Plan	A local document outlining how IT systems and data will be restored to a "good known state" following an incident. Supports technical recovery post-cyberattack.
GIRP	Group Incident Response Plan	A Diploma document describing the approach to managing cyber incidents.
GCCF	Group Cyber Control Framework	Document which defines a baseline set of security controls required across the Group. Aligned with NIST CSF, it supports consistent protection of systems and data and enables local implementation and continuous improvement.
IRP	Incident Response Plan	A structured approach to address cyber security incidents.
LIRP	Local Incident Response Plan	A local document maintained by each business detailing how to prepare, detect, respond to, escalate, and recover from cyber incidents. Must align with the GIRP.
ISO27001	ISO/IEC 27001 International Organisation for Standardization / International Electrotechnical Commission 27001	An international standard that specifies the requirements for establishing, implementing, maintaining, and continually improving an information security management system (ISMS).
-	Least Privilege Principle	A cyber security principle that states users or systems must only have the minimum authorisation rights necessary to perform their required tasks.
-	Need to Know Basis	A cyber security principle that states access to information or systems is only for those individuals whose job function requires them.
NIST CSF	National Institute of Standards and Technology Cybersecurity Framework	A structured set of guidelines for managing cyber security.
TISR	Technical Information Security Representative	A technical lead responsible for implementing security measures and responding to incidents.