GROUP POLICY

Group Information Security Policy (GISP)



WEBSITE
Published October 2026

DIPLOMA PLC
VALUE-ADD SOLUTIONS

Contents

1 Purpose 2
2 Scope 2
3 Policy Statement 2
4 Requirements 3
4.1 Reference Framework 3
4.2 Business Representatives 3
4.3 Local Policies and Procedures 4
4.4 Information Classification and Handling 4
4.5 Information Asset Protection 5
4.6 Access Control and Authentication 5
4.7 Monitoring and Logging 5
4.8 Incident Management 5
4.9 Third-Party and Vendor Security 6
4.10 Acquisitions 6
5 Group Cyber Security Framework 7
6 Compliance & Non-Compliance 8
7 Contacts 8

Definitions 9

Document Control

Policy owner:	Group Integration Director / Cyber Security Lead
Published / effective from:	October 2026
Review frequency:	Annual
Next review date:	October 2027
Version:	6.0

1 Purpose

This Group Information Security Policy (GISP) establishes the Group's information security requirements and governance expectations and provides the overarching approach for managing information and cyber security risk across the Group.

The Group Cyber Control Framework (GCCF) supports this Policy by defining the cyber security controls through which these requirements are implemented, monitored and assessed across Group businesses. The GCCF uses a tiered control model comprising Key, Enhanced and Comprehensive controls, with the Key Cyber Controls (KCC) forming the minimum baseline required across all Group businesses.

The tiered approach enables additional controls to be applied where appropriate, taking account of the size, complexity, technology environment and risk profile of individual businesses.

2 Scope

This Policy applies to all employees, contractors, consultants, and third-party providers 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 protecting the Group's information assets through the implementation of the Group's minimum cyber security baseline, together with additional risk-based measures where appropriate. 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 the Group's minimum cyber security baseline and additional controls appropriate to the business's risk profile.
- 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. The GCCF is aligned to NIST CSF and translates the Group's cyber security requirements into defined, tiered controls for implementation across Group businesses.

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. 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 compliance with this Policy and the GCCF, and serving as the primary local liaison with the Group Cyber Security Team.

The BISR and TISR also support the business's cyber incident preparedness and response arrangements in accordance with the Group Incident Response Plan (GIRP) and the business's Local Incident Response Plan (LIRP). The TISR will typically fulfil the role of Incident Response Leader and lead Bronze Command (the local operational response level during a cyber incident, as defined in the GIRP) during a cyber security incident, or the BISR where no dedicated technical resource is available.

4.3 Local Policies and Procedures

Formal Documentation

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

Security Awareness & Training

Security awareness training and phishing simulation form part of the KCC minimum baseline and are required across all Group businesses.

Each business is responsible for providing appropriate information security awareness training to its employees and for conducting regular phishing simulations. These activities must be maintained in line with the requirements of the GCCF.

Businesses are responsible for monitoring completion and participation and for taking appropriate action where gaps are identified.

Emerging Technologies

Diploma encourages the adoption of innovative technologies 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.

Use of AI

Given the pace at which AI capability is being added to everyday business tools, each business must maintain a documented position on its use, either as a standalone policy or within existing local policies. As a minimum this should address which tools are approved for business use, what information may and may not be entered into them, who approves new tools, and how output is reviewed before it is relied on.

Approval of a product is not approval of AI functionality subsequently added to it, whether as a new feature or as part of an upgrade. Where a tool is capable of taking action rather than only producing content, additional controls will be needed and the business should satisfy itself these are proportionate to the access the tool is given.

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 NIST CSF. A layered security approach must be applied to support the principle of defence in depth.

The Group Cyber Control Framework (GCCF) supports this Policy by defining the cyber security controls through which the Group's information security requirements are implemented. The GCCF is aligned with the NIST Cybersecurity Framework (NIST CSF) and uses a tiered control model comprising Key Cyber Controls (KCC), Enhanced and Comprehensive controls.

The KCC form the minimum cyber security baseline required across all Group businesses, irrespective of size or risk profile.

Enhanced and Comprehensive controls provide additional layers of protection and are applied where appropriate, taking account of the size, complexity, technology environment and cyber risk profile of the business.

Together, these control tiers provide a proportionate framework that establishes a consistent minimum level of cyber security across the Group while providing additional controls for businesses with greater scale, complexity or cyber risk exposure.

4.6 Access Control and Authentication

Each business must implement authentication and access controls in line with the principles of least privilege and need to know basis. Authentication and access controls must meet the applicable requirements of the GCCF, including the use of multi-factor authentication (MFA) where required by the GCCF.

4.7 Monitoring and Logging

Monitoring and logging must be implemented in accordance with the applicable requirements of the GCCF to support threat detection, incident response, compliance and forensic investigations.

Each business is responsible for ensuring appropriate monitoring and logging is maintained within its environment and complies with applicable local legal and regulatory requirements.

4.8 Incident Management

Each business must maintain appropriate arrangements to identify, respond to and recover from information security incidents in accordance with the GIRP and its own LIRP.

The LIRP must define clear local roles, responsibilities, escalation and communication arrangements for managing a cyber security incident and must be maintained so that responsibilities remain clear if key individuals are unavailable.

The LIRP must be integrated with the business's:

- Local Disaster Recovery Plan (LDRP), which defines how IT systems and data will be restored following an incident; and
- Local Business Continuity Plan (LBCP), which defines how essential business operations will continue during and following disruption.

The LIRP, LDRP and LBCP must be maintained, reviewed and updated to remain appropriate to the business and its operating environment. Disaster recovery testing must be undertaken in accordance with the applicable requirements of the GCCF to provide assurance that critical services can be restored within agreed recovery objectives.

Information security incidents must be reported and escalated in accordance with the GIRP to ensure appropriate local and Group level oversight and response.

4.9 Third-Party and Vendor Security

Each business is responsible for managing the information and cyber security risks associated with third-party providers that access, process, store or manage the business's systems, services or information.

Appropriate security requirements must be considered when engaging and managing third parties, taking account of the nature of the service and the information or systems involved. Third-party cyber security due diligence and assurance activities must be performed in accordance with the applicable requirements of the GCCF.

Businesses remain responsible for understanding and appropriately managing cyber security risks arising from their use of third-party providers.

4.10 Acquisitions

Newly acquired businesses come within the scope of this Policy from the date of completion and are onboarded into the Group's information and cyber security framework as part of the post-acquisition integration process.

As part of post-acquisition onboarding, each acquired business must:

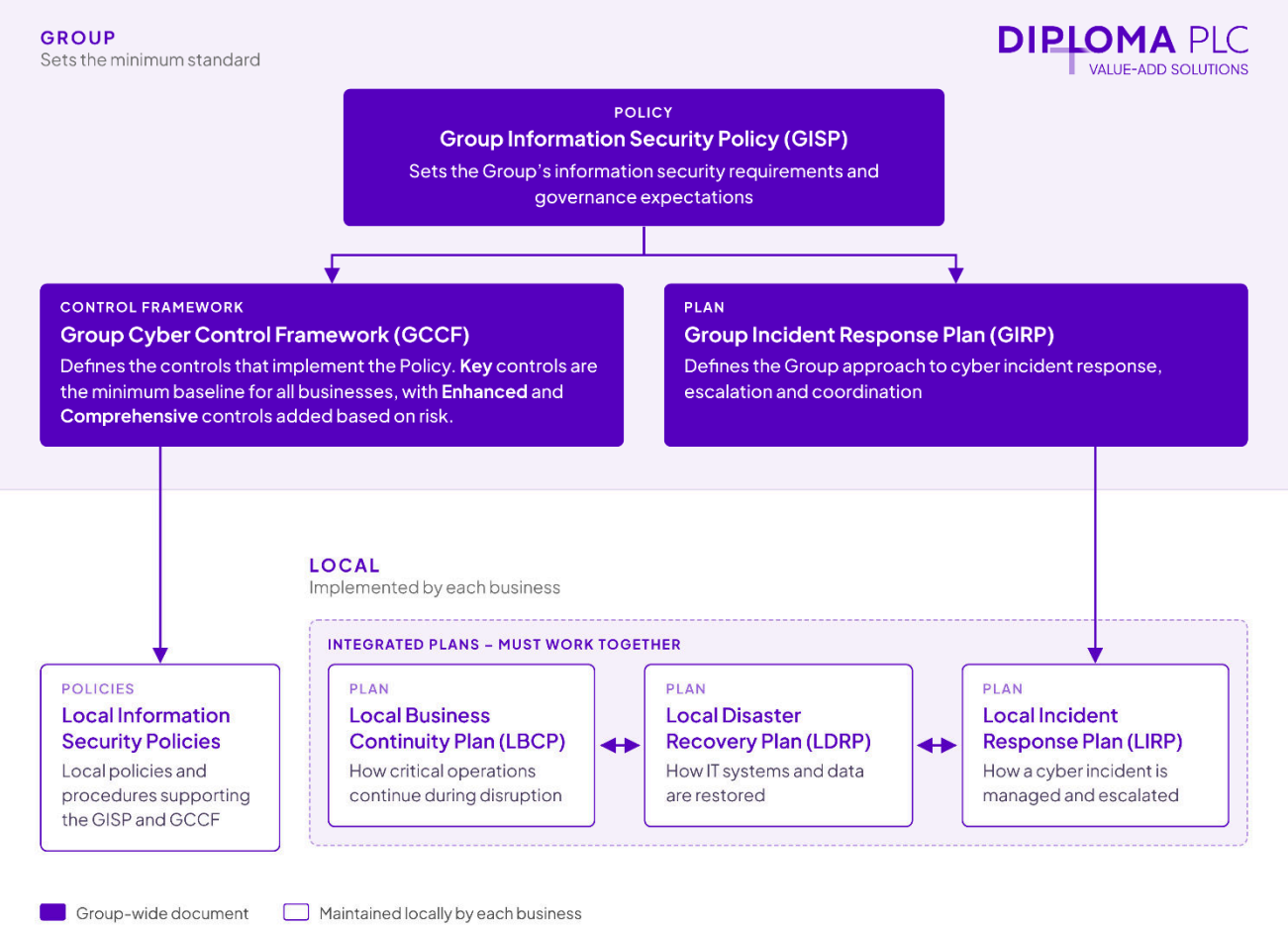
- adopt this GISP and the supporting GCCF;
- progress towards full implementation of the KCC minimum baseline as a priority. Any gaps identified during due diligence or post-acquisition onboarding must be documented, prioritised and incorporated into a remediation plan until the minimum baseline is achieved;
- establish and maintain a LIRP aligned with the GIRP and integrated with its LDRP and LBCP; and
- participate in the Group's cyber security monitoring and assurance arrangements as applicable.

Progress towards the KCC minimum baseline, identified control gaps and remediation activity will be monitored through the Group's cyber security governance arrangements until the required baseline is achieved.

5 Group Cyber Security Framework

The Group Cyber Security Framework brings together the policies, control framework, incident response arrangements and locally maintained plans through which Diploma manages cyber security risk across the Group.

The Group Information Security Policy (GISP) establishes the overarching requirements and governance expectations. The Group Cyber Control Framework (GCCF) defines the tiered controls used to implement those requirements, while the Group Incident Response Plan (GIRP) establishes the Group approach to cyber incident response, escalation and coordination.



A collection of Group-wide cyber security policies, frameworks and plans can be found on the Group website and Learning Management System (Purple Portal).

6 Compliance & Non-Compliance

The Group CFO is the executive sponsor for the Group Cyber Security Framework. The Group Integration Director, as Cyber Security Lead, is responsible for overseeing the operation, monitoring and ongoing development of the framework across the Group.

All businesses, employees, contractors and relevant third parties must comply with this Policy and the applicable requirements of the Group Cyber Security Framework.

For Group businesses, this includes maintaining the Key Cyber Controls (KCC) minimum baseline and implementing applicable additional controls in accordance with the Group Cyber Control Framework (GCCF).

Compliance is monitored through the Group's cyber security governance and assurance activities. Identified gaps must be documented, remediated and tracked to closure. Failure to comply with this Policy or applicable cyber security requirements may result in appropriate escalation and corrective action.

7 Contacts

Group Integration Director | Cyber Security Lead

For questions relating to this Policy, the Group Cyber Security Framework, GCCF requirements, KCC implementation or cyber security matters.

Carolyne.Dick@diplomaplc.com

Cyber Security Incidents

Cyber security incidents must be managed and escalated in accordance with the GIRP and the business's LIRP. Incident specific escalation contacts and responsibilities are maintained within the GIRP and LIRP.

Definitions

Acronym	Definition	Description
BISR	Business Information Security Representative	A designated local representative responsible for supporting information security compliance, coordinating local security activities and supporting cyber incident preparedness and response.
GCCF	Group Cyber Control Framework	The Group's tiered cyber control framework comprising Key, Enhanced and Comprehensive controls. The KCCs form the minimum baseline required across all Group businesses, with additional controls applied where appropriate. The GCCF is aligned with NIST CSF.
GIRP	Group Incident Response Plan	A Diploma document describing the approach to managing cyber incidents.
GISP	Group Information Security Policy	The Group policy that establishes information security requirements and governance expectations across Diploma businesses.
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).
KCC	Key Cyber Controls	The minimum cyber security baseline required across all Group businesses.
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.
LDRP	Local Disaster Recovery Plan	A local document outlining how IT systems and data will be restored to a "known good state" following an incident. Supports technical recovery post-cyberattack.
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.
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 designated technical representative responsible for supporting implementation of security controls and typically fulfilling the Incident Response Leader role during a cyber security incident.
-	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.
-	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.