NIS2 Policy

Identification:

Type	Group Policy (Class 2)		
Visibility	☐ Confidential	☐ Internal	☑ Public
Status	☐ In progress	☐ Draft	☑ Published

Approvals:

Activity	**Name**	**Date**
Approved by	Francesca Gusti	22 July 2026
Published by	Gloria Ghilardi	22 July 2026

Reviews:

Rev.	Date	Reason	Author RGQ	Approval DIR
0	22 July 2026	First issue	22 July 2026	22 July 2026

Summary

1. Purpose and scope 4
1.1 Policy objectives 4
1.2 Definitions and relevant terminology 4
1.3 Scope 4
1.4 Distinction between Essential Entities and Important Entities 4
2. Regulatory framework and references 4
2.1 Legislative Decree 138/2024 – transposition of NIS2 4
2.2 Other regulatory references 4
3. Governance and responsibilities 5
3.1 Corporate bodies and roles 5
3.2 Appointment of the NIS2 Responsible Person 6
3.3 Internal coordination and cross-functional responsibilities 6
3.4 Chain of responsibility towards suppliers and subcontractors 7
4. Risk analysis and risk management 8
4.1 Risk analysis method: identification, assessment and treatment 8
4.2 Criteria for accepting residual risk 9
4.3 Periodic review and updating of risk 9
4.4 Supply chain assessment – third parties 9
5. Technical and organisational security measures 11
5.1 Access controls and account management 11
5.2 Encryption and data protection 11
5.3 System monitoring, logging and auditing 11
5.4 Vulnerability management and patch management 11
5.5 Backup, resilience and business continuity 12
5.1 Network segmentation, perimeter defence and physical and environmental security 12
5.2 Defence against malware and advanced attacks 13
5.3 Change and configuration management 13
6. Security incident notification and management 13
6.1 Definition of a significant incident (criteria) 14
6.2 Internal detection, response and mitigation process 14
6.3 Notification flows to ACN and relevant authorities 14
6.4 External communications and reporting 14
6.5 Incident register and post-event analysis 15
7. Business continuity and recovery 15
7.1 Business continuity / disaster recovery plan 15
7.2 Recovery and restoration procedures 15
7.3 Periodic tests and simulations 16
7.4 Integration with corporate business continuity 16
8. Training, awareness and a culture of security 16
8.1 Training and awareness programmes 16
8.2 Simulations and drills 17

8.3 Roles requiring specific training 17
9. Assessment, internal audit and compliance 17
9.1 Internal NIS2 compliance audits 17
9.2 External checks and third-party audits 17
9.3 Continuous monitoring and KPIs 18
9.4 Internal reporting to senior management 18
10. Supervision, inspections and checks by the authorities 18
10.1 Cooperation with the relevant authorities 18
10.2 Inspection and verification procedures 19
10.3 Management of non-conformities and corrective action plans 19
10.4 Penalties and liability 19
11. Review and updating of the policy 19
11.1 Frequency and procedures for review 19
11.2 Circumstances giving rise to an extraordinary review 20
11.3 Versioning and approval 20
12. Appendices and technical references 20
12.1 List of measures and requirements in accordance with Annex 1 / Annex 2 20
12.2 Related documentation 20

1. Purpose and scope

1.1 Policy objectives

This Policy on the implementation of the NIS2 legislation (hereinafter the "Policy") sets out principles, requirements and responsibilities aimed at ensuring a high level of cybersecurity and operational resilience within the companies of the Diagram Group classified as important entities pursuant to Directive (EU) 2022/2555 (NIS2) and Legislative Decree 138/2024. The Group companies are ISO/IEC 27001 certified and have already adopted an Information Security Management System (ISMS) complete with ISO/IEC 27001 Security Policies. This Policy supplements these controls with the NIS2 requirements relating to risk management, service resilience and incident management.

1.2 Definitions and relevant terminology

Incident: an event that compromises or may compromise the availability, integrity, authenticity or confidentiality of networks, systems or data.
Information system: hardware and software infrastructure, networks, data, applications and business procedures.
Risk: the combination of the probability and impact of a threat on a vulnerability.
Technical and organisational measures: security controls adopted in accordance with NIS2 and ISO/IEC 27001.

1.3 Scope

This Policy applies to staff, collaborators, consultants and third parties who access the systems of Diagram Group companies designated as Important Entities under the NIS2 regulations.
It covers all ICT infrastructure, both on-premises and in the cloud, and all services relevant to the obligations applicable to important entities. This Policy complements the ISO/IEC 27001 ISMS already in place.
Agroconsulting Spa and all its subsidiaries are excluded from the scope of this policy as they are not subject to the management and control of Diagram Spa.

1.4 Distinction between Essential Entities and Significant Entities

NIS2 distinguishes between essential entities and important entities. Currently, within the Diagram Group, the companies classified as important entities at the time of publication of this policy are: Diagram S.p.A. and Abaco S.p.A., both of which have a certified ISO/IEC 27001 Management System.

2. Regulatory framework and references

2.1 Legislative Decree 138/2024 – transposition of NIS2

This Policy complies with Legislative Decree 138/2024, which transposes Directive (EU) 2022/2555 and sets out obligations regarding risk management, security measures, classification and incident reporting for significant entities.

2.2 Other regulatory references

- Regulation (EU) 2016/679 – GDPR.
- European and national regulations on operational resilience and ICT security.
- ISO/IEC 27001 and ISO/IEC 27002 standards, adopted by the Diagram Group.
- Internal policies of the ISO/IEC 27001 Management System.

- Operational procedures relating to access, incidents, business continuity and suppliers.

3. Governance and accountability

The Diagram Group adopts a cybersecurity governance model based on the clear allocation of roles, responsibilities, decision-making powers and information flows between corporate bodies, senior management and the technical, legal, compliance, privacy and control functions. The model is applied at Group level in accordance with common criteria, it being understood that each company falling within the scope of the NIS2 regulation retains responsibility for the obligations directly applicable to it.
Appointments and delegations of authority relating to information security and cybersecurity are formalised by senior management and, where required by legislation, the corporate structure or the scope of the powers conferred, are submitted to the relevant Board of Directors for approval or acknowledgement. Appointments are reviewed at least annually and whenever there are changes to legislation, organisational structure, technology or the scope of the relevant services.

3.1 Corporate bodies and roles

The **Board of Directors** and the other relevant administrative and management bodies approve the procedures for implementing information security risk management measures, oversee the fulfilment of NIS2 obligations and receive, either periodically or promptly depending on the severity of the incident, information on risks, incidents, significant vulnerabilities and notifications made to the authorities. Operational appointments and internal delegations of authority do not entail the transfer of the responsibilities assigned by law to the administrative and management bodies.

Company management ensures the implementation of the guidelines defined by the administrative bodies, provides adequate human, technical and financial resources, approves procedures and operational plans, and verifies that the functions involved have the necessary skills, authority and access to information to carry out their respective duties.
The risk management function, even when not assigned to a dedicated Risk Officer, ensures that cyber risk is identified, assessed, managed, monitored and integrated into the overall corporate risk management system. This activity is carried out in coordination with the Cyber Legal & Compliance Officer, the Information Security Officer/Cyber Security Manager, senior management and the departments responsible for the relevant processes and services.
The **Information Security Officer and Cyber Security Manager**, who, for the purposes of this Policy, carries out the organisational and technical oversight normally assigned to the CISO, coordinates the information security management system, supports the assessment of cyber risks and oversees the implementation of technical, operational and organisational measures. In the event of an incident or crisis, they assess whether to activate and convene the Crisis Committee, coordinate technical activities relating to containment, recovery and evidence collection, and ensure the prompt involvement of other relevant functions. The Cyber Security Manager may delegate specific operational activities to the internal Information Security Officers (RISI), without prejudice to their own coordinating role.
The Cyber Legal & Compliance Officer, reporting functionally to the Board of Directors and liaising with the Supervisory Body, oversees regulatory, legal and compliance aspects relating to cybersecurity and information security. They support the corporate bodies in interpreting applicable

obligations, coordinate the updating of NIS2 documentation, verify the consistency of delegated powers and information flows, and assist in assessing the legal, contractual and reputational consequences of incidents.

The **Data Protection Officer (DPO)** carries out the duties assigned to them by data protection legislation and is involved whenever a risk, vulnerability or security incident may affect personal data. The **Privacy Focal Point**, appointed at Group level, facilitates coordination between Group companies and their respective DPOs, ensuring the timely circulation of relevant information. The role of the DPO remains distinct from the operational responsibilities of the Cyber Security Manager and the decision-making responsibilities of the corporate bodies.

3.2 Appointment of the NIS2 Responsible Person

For the purposes of this Policy, the term **"NIS2 Responsible** Person" refers to the internal body responsible for coordinating compliance with NIS2 requirements and does not entail the transfer of responsibilities assigned by law to the administrative and management bodies.

Overall coordination of NIS2 compliance is ensured by the Cyber Legal & Compliance Officer, in close collaboration with the Information Security Officer/Cyber Security Manager, the NIS2 Point of Contact, the CSIRT Liaison Officer, senior management and other relevant functions. The coordinator is specifically responsible for:

- monitoring applicable obligations and deadlines;
- liaising between corporate governance, compliance and technical functions;
- organising the flow of information to the administrative bodies;
- co-ordinating the updating of the Policy, procedures and evidence of compliance;
- monitoring compliance plans and any corrective actions;
- liaising with consultants, auditors, authorities and supervisory bodies.

For each company subject to the NIS2 framework, a **NIS2 Contact Point** is formally designated, in accordance with Article 7 of Legislative Decree 138/2024, as well as a designated deputy. The NIS2 Contact Point acts as the official point of contact with the National Cybersecurity Agency, manages the registration and updating of information on the ACN platform, and ensures that any changes are communicated within the prescribed timeframes. Article 7 requires the designation of the NIS2 Contact Point and their deputy, as well as the notification of the responsible persons identified by the legislation.

The **CSIRT Liaison Officer** is also designated – referred to in the internal procedure as the 'CSIRT Communications Manager' – and is responsible for operational liaison with CSIRT Italia and for managing incident notifications. The CSIRT Liaison Officer works in coordination with the NIS2 Point of Contact, the Cyber Security Manager and the Cyber Legal & Compliance Officer, and has access to the information, authorisations and channels necessary to carry out the required communications. ACN's operational framework distinguishes between the Contact Point and the CSIRT Liaison Officer, assigning to the latter the responsibility for managing communications relating to incidents and notifications.

3.3 Internal coordination and cross-functional responsibilities

Cybersecurity management is a cross-functional responsibility and involves all functions that design, develop, procure, manage or use information systems, networks, data, infrastructure and digital services.

The Information Security Manager/Cyber Security Manager ensures technical and operational coordination; the Cyber Legal & Compliance Officer oversees regulatory, legal and compliance matters; the NIS2 Point of Contact and the CSIRT Liaison Officer manage institutional communications with n their respective areas of competence; the DPO and the Privacy Focal Point deal with matters relating to the protection of personal data. The IT, Engineering, Quality & Test, HR, Procurement, Legal, Administration and Communications departments, together with the heads of services and processes, collaborate within their respective areas of expertise.
In particular:

- service and process managers promptly report risks, anomalies, vulnerabilities and incidents relating to their areas of responsibility;
- the IT and technical departments implement measures for prevention, detection, containment, recovery and the preservation of evidence;
- HR supports the allocation of responsibilities, the management of authorisations, training, and the processes for the recruitment, transfer and termination of staff;
- Procurement and Legal ensure that cybersecurity requirements are included in contracts with third parties;
- Communications manages, subject to authorisation from senior management and in coordination with the relevant departments, communications with customers, users, stakeholders and the media;
- RGQA supports document traceability, audits, the management of non-conformities and coordination with certified management systems.

Significant incidents and risks are subject to an escalation process proportionate to their severity, operational impact, potential data compromise, regulatory significance and effects on customers and the services provided. The Board of Directors and senior management are kept informed on a regular basis and, in the event of significant incidents, without delay. Reports of significant incidents to CSIRT Italia follow the sequence and timelines set out in the regulations, including pre-notification, notification and the final report.

3.4 Chain of responsibility towards suppliers and subcontractors

The Diagram Group considers supply chain security to be an integral part of its cyber risk management system. The use of suppliers, outsourcers, cloud providers, consultants or subcontractors does not exempt the company concerned from the obligations and responsibilities arising from the NIS2 regulation.
Suppliers are classified according to the criticality of the products and services provided, access to data and systems, operational dependency, the substitutability of the service and the potential impact of an incident on the continuity and security of the Group's services. For critical suppliers, preventive and periodic checks are carried out concerning, amongst other things, certifications, technical and organisational measures, access management, secure development, vulnerabilities, business continuity, incident management and the use of subcontractors.
Contracts with relevant suppliers and subcontractors must provide for the following, in a manner proportionate to the risk:

- minimum security requirements and obligations to comply with the Group's Policies;
- obligations to report incidents, vulnerabilities and compromises in a timely manner;
- reporting times consistent with the Group's NIS2 notification obligations;
- cooperation in analysis, containment, recovery and notification activities;

- availability of the necessary evidence and records;
- the right to audit, verify or obtain independent certifications;
- requirements for business continuity, disaster recovery, backup and restoration;
- rules governing access to, return of and deletion of data;
- prior authorisation or notification regarding the use of subcontractors;
- extension to subcontractors of the security obligations applicable to the main supplier.

The main supplier is responsible, vis-à-vis the contracting Group company, for ensuring that its sub-suppliers fulfil their obligations and must ensure that the latter adopt measures commensurate with the criticality of the services entrusted to them. The Group assesses the specific vulnerabilities of direct suppliers, the quality of their security practices and the effectiveness of the measures implemented throughout the supply chain. The NIS2 regulation expressly requires that risk management includes supply chain security and the assessment of the vulnerabilities and security practices of direct suppliers and service providers.

For further details on the classification, qualification and handling of suppliers, please refer to the Group's internal procedure *"GRUPPO_PRO 07.03 Management of Outgoing Contracts and Supplier Qualification*".

4. Risk analysis and risk management

4.1 Risk analysis method: identification, assessment and treatment

The Diagram Group adopts a structured and iterative process for managing information security risks, consistent with the principles of the ISO/IEC 27001 and ISO/IEC 27005 standards. The process comprises the following stages: context definition, risk identification, analysis and assessment, treatment, residual risk acceptance, monitoring and review.

Risks are identified by considering the information assets, business processes, activities, products and services falling within the scope of the Information Security Management System. For each area, the sources of risk, threats, vulnerabilities, causes, potential events and their consequences are identified, including any cumulative or cascading effects. The analysis takes into account the internal and external context, past experience, legislative, regulatory and contractual requirements, existing procedures, available knowledge and the guidance contained in the ISO/IEC 27005 standard. Information may be gathered through interviews, site visits, document reviews, inspections and analyses of business processes and systems.

The risk assessment takes three parameters into account:

- the impact on the business, rated on a scale of 1 to 5;
- the probability of occurrence, rated on a scale of 1 to 5;
- the level of vulnerability to the threat, classified as low, medium or high.

The impact on the business is determined by considering, in particular, the classification of the information and assets involved, the loss of confidentiality, integrity or availability, the consequences for operations, financial or commercial losses, reputational damage and the breach of contractual, legal or regulatory obligations. The combination of these three parameters, using the company's assessment matrix, results in a risk level ranging from 1 to 11.

Depending on the level identified, the risk is classified as non-existent, minimal, medium or unacceptable. For unacceptable risks, risk treatment measures must be defined and implemented with the aim of reducing the probability of occurrence, vulnerability or impact. For each measure, the objective, the activities to be carried out, the necessary resources, responsibilities and implementation timelines are identified. Following the application of the controls, a new assessment

is carried out to determine the residual risk. If the risk treatment does not enable an acceptable level to be achieved, the assessment and treatment process is repeated, revising the context and criteria used where necessary.

4.2 Criteria for accepting residual risk

Risk acceptance is based on the level of residual risk remaining after the application of control measures and on the level of governance associated with the asset, process or threat under consideration.

The level of governance reflects the Organisation's ability to manage risk through management strategies, formalised procedures and instructions, operational practices, monitoring activities, corrective actions and the assessment of their effectiveness. This level is classified as excellent, good, adequate or poor and is used to determine the level of materiality according to the following relationship:

Significance level = Residual risk × Governance

Residual risks classified as non-significant are considered acceptable, provided that the existing measures are adequate in relation to the context, the organisation's objectives and the applicable obligations. Risks with a materiality level of 15 or higher are considered significant and require the definition of specific actions in the Risk Action and Treatment Plan, with priorities and timelines proportionate to the level identified.

The acceptance of residual risk must be explicit, documented and approved by the relevant managers within the Organisation. Such approval is particularly important when the implementation of additional controls is omitted, deferred or deemed unsustainable in relation to costs, the necessary resources or operational requirements. Acceptance does not preclude subsequent monitoring of the risk nor the possibility of reassessing it should significant changes occur.

4.3 Periodic review and updating of risk

The information security risk analysis is reviewed at least annually, as a preliminary step to the review of the organisation's objectives and programmes and as input to the management review.

The assessment must also be updated whenever significant changes occur concerning the internal or external environment, activities, processes, products, services, information assets, technologies used or regulatory and contractual obligations. The review may also be triggered as a result of security incidents, non-compliance, organisational changes, the introduction of new systems or services, changes in threats and vulnerabilities, or significant changes in the supply chain.

The defined risk treatment actions are included in the Risk Action and Treatment Plan and monitored in terms of progress, adherence to timelines, assigned responsibilities and the effectiveness of the measures implemented. Should the monitoring reveal that the controls are insufficient or that the level of risk has increased, a new iteration of the assessment process is carried out and further mitigation measures are identified. The outcomes of the reviews and any decisions regarding risk acceptance are recorded and retained as evidence of the process carried out.

4.4 Supply chain assessment – third parties

The Diagram Group assesses and monitors risks arising from suppliers and other third parties who may have access to company information, systems, infrastructure or processes, or who may affect business continuity, regulatory compliance and the security of the services provided.

Critical suppliers must undergo pre-qualification prior to the commencement of the contractual relationship. The assessment takes into account, at a minimum, technical and professional

suitability, commercial reputation, financial and organisational capacity, compliance with information security standards, and possession of relevant certifications, such as ISO/IEC 27001, ISO 9001, ISO 14001 or ISO 45001, as well as the existence of a Code of Ethics and an Organisational Model in accordance with Legislative Decree 231/2001, where applicable.
Critical suppliers are classified as:

- **high-risk suppliers**, where they process personal data or sensitive information, manage critical ICT infrastructure, operate directly on company systems or may have a significant impact on compliance and business continuity;
- **standard-risk suppliers**, where they provide goods or services for general use or with a limited impact on security and business operations.

High-risk suppliers are subject to assessment at least once a year, whilst standard-risk suppliers are reassessed at least every three years. Reassessment may be brought forward in the event of non-compliance, incidents or security breaches, corporate changes, reports, a deterioration in performance or other circumstances that may alter the relevant risk profile.
For ICT, cloud, SaaS, IaaS and other services with a high cyber impact, the assessment also covers the location of data centres, data protection measures, security certifications, SLAs, availability levels, incident management, business continuity, the identification of cybersecurity points of contact and system administrators, as well as the terms governing service termination, migration and the return or deletion of data.
Contracts with third parties must set out, on a risk-based basis, minimum cybersecurity requirements, confidentiality and data protection obligations, notification and cooperation obligations in the event of an incident, service levels, audit rights, staff competence requirements, business continuity, subcontracting management and termination clauses in the event of serious breaches.
Supplier performance is monitored by assessing the compliance of the product or service with the order and the contract, timeliness, quality, value for money, support and the ability to liaise with business functions. In the event of a negative assessment, corrective actions and a subsequent review may be requested, or the supplier may be removed from the Register of Qualified Suppliers.
Assessments, contracts, certifications and qualification documentation are recorded in the company's system to ensure full traceability of the process.

5. Technical and organisational security measures

5.1 Access controls and account management

The Organisation implements measures to ensure that access to systems, applications and company information is granted exclusively to authorised users, based on their role and actual operational needs. Accounts are personalised and managed throughout their entire lifecycle, from creation to modification or revocation, with periodic checks on assigned privileges and the use of appropriate authentication mechanisms and credential protection. Full details are set out in a single procedure applied by all Group companies: *"GRUPPO_IST 07.05 Internal Procedure for Access Management*".

5.2 Encryption and data protection

DIAGRAM adopts cryptographic measures designed to ensure the confidentiality, integrity and security of information, whilst preventing the exposure of services via unencrypted protocols. Communications between corporate networks and the Internet, VPN access and services provided to third parties are protected using appropriate cryptographic protocols and algorithms, including AES256 and HTTPS with certificates issued by accredited providers. Private keys and encryption keys are stored in secure areas of the file server, accessible only to authorised personnel. Device and database encryption is enabled based on the classification of information, the client's security requirements and the findings of the risk assessment, whilst also taking into account any potential impact on system performance and business continuity.
Full details are set out in the procedure *'IST 07.06 Internal Procedure for the Development of Information* Systems', which is specific to each company within the Group.

5.3 System monitoring, logging and auditing

Event logs are managed and collected via the standard services of the Windows and Linux operating systems, namely Event Viewer and SysLog respectively.
The log on the server subject to any changes contains the following information:
both failed and successful login attempts, showing the username, date and time of the event, and the IP address of the machine from which the event originated.
The main operations carried out on the machine
The logs recorded on individual servers are accessible only to the system administrator.
At the start of 2026, an integrated log management platform was implemented.
Full details are set out in a single procedure applied by all Group companies: *"GRUPPO_IST 07.05 Internal Procedure for Access Management*".

5.4 Vulnerability management and patch management

The DIAGRAM Group adopts a structured process for the identification, assessment and management of technical vulnerabilities relating to networks, devices, servers, web applications, services and corporate infrastructure. Monitoring is carried out periodically by an external provider specialising in cybersecurity, through vulnerability assessments, web assessments and proactive agent-based systems, with monthly reports produced and analysed by the Compliance, IT and Production departments. Detected vulnerabilities are recorded in the project management system, classified according to severity and managed through specific remediation activities and, where necessary, through the installation of patches and corrective updates. The target times for escalation

and resolution are 24 hours for critical vulnerabilities, 72 hours for high-severity vulnerabilities, 30 days for medium-severity vulnerabilities and 90 days for low-severity vulnerabilities. Particularly serious vulnerabilities may trigger the security incident management process, whilst any risks that cannot be eliminated or whose resolution would be excessively costly are formally assessed and accepted. The completion of activities and the effectiveness of the measures adopted are subject to periodic checks.
Full details are set out in a single procedure applied by all Group companies: *"GRUPPO_IST 07.09 Management of Technical Vulnerabilities and Protection against Malware*".

5.5 Backup, Resilience and Business Continuity

The Group adopts structured and predominantly automated procedures for backing up data, systems, applications, databases and source code repositories, using copies stored on both internal infrastructure and in cloud environments. Data is protected through mechanisms such as redundancy, replication, synchronisation, versioning, snapshots and, where applicable, immutable copies, in order to ensure its availability and recovery in the event of failures, accidental deletion, unauthorised modifications or system downtime.
The frequency and retention periods of backups are determined according to the type, criticality and classification of the information and may include daily, weekly, incremental or differential copies. The outcome of these operations is monitored via automatic notifications and verified by the designated technical staff, who intervene in the event of an error by taking the appropriate corrective actions and assessing whether the backup should be repeated immediately. The integrity and actual recoverability of the copies are verified through periodic recovery tests, carried out at least annually and formally documented, with particular attention paid to systems processing personal data and to services considered essential for business continuity.
Full details are set out in a procedure entitled *'IST 07.01 Internal Backup* Procedure', specific to each company within the Group.

5.1 Network segmentation, perimeter defence, and physical and environmental security

The Group adopts a multi-layered security model based on network segmentation, IT perimeter protection and physical and environmental control of infrastructure. Corporate and cloud networks are divided into distinct environments according to the type of users, devices and services provided, separating networks for guests and personal devices from those dedicated to employees, servers, application systems, databases and externally exposed services; access and communications between the various segments are governed by the principle of least privilege, through specific authorisations, network rules and encrypted connections. Perimeter defence is ensured by redundant and constantly updated equipment, equipped with intrusion prevention, web filtering, application control and protection against viruses and malware, supported by systems for authentication, monitoring, event logging and alert management; attacks based on known patterns are automatically countered, whilst anomalous events are subject to analysis and specialist intervention. Physical and environmental security ensures that access to premises and technical rooms is restricted exclusively to authorised personnel, via personalised badges or keys, the registration and escorting of visitors, the definition of access time slots and, where applicable, the use of alarm and video surveillance systems. The premises housing the IT infrastructure are also protected by continuous air-conditioning , uninterruptible power supply systems, sensors for detecting temperature and the presence of water, fire-fighting equipment, cabling that is protected

and separated from electrical circuits, regular maintenance, and procedures for managing faults and emergencies.
Full details are set out in the *"IST 07.18 Physical and Environmental* Security" procedure, which is specific to each Group company.

5.2 Defence against malware and advanced attacks

The Group implements multi-layered protection measures against malware, exploit attempts and other advanced cyber threats, applied to servers, workstations and network infrastructure. Security systems operate in real time to detect and block anomalous behaviour, malicious code and attempts at compromise, automatically isolating suspicious files in quarantine areas accessible only to authorised personnel. Users cannot disable or remove the security solutions, which are managed via centralised consoles from which events are monitored and actions for removal, authorisation or containment are defined. This protection is complemented by continuous monitoring of the network and devices, periodic analysis of events logged by perimeter systems, and threat intelligence activities aimed at promptly identifying new threats and assessing their potential impact on business services. In the event of significant anomalies or threats, technical staff and security specialists carry out the necessary analyses and implement appropriate containment and remediation measures.
Full details are set out in a single procedure applied by all Group companies: *"GRUPPO_IST 07.09 Management of Technical Vulnerabilities and Protection against Malware*".

5.3 Change and Configuration Management

The Group adopts a structured process for managing changes made to infrastructure, information systems, applications, hardware and software components, and cloud environments. Every change must be described, assessed and approved in advance by the relevant manager, taking into account the purpose of the change, technical requirements, necessary resources and licences, costs, implementation timescales and testing procedures. The assessment also includes an analysis of risks and potential impacts on business continuity, service availability, and data confidentiality and integrity. Activities, responsibilities, changes made and their outcomes are recorded in the internal project management system, with each intervention assigned a priority level commensurate with the risk. Before being put into operation, new components and modifications to existing systems undergo acceptance, reliability, connectivity, performance and security testing, using, where necessary, temporary or separate environments to verify correct operation and reduce the risk of interruptions or faults.
Full details are set out in the procedure "IST 07.06 Internal Procedure for the Development of Information Systems", which is specific to each Group company.

6. Reporting and management of security incidents

The Group adopts a formalised process for the detection, assessment, management and reporting of incidents that may compromise the confidentiality, integrity or availability of information, information systems, cloud services and corporate assets. Management is coordinated by the Information Security Manager, with the support of the technical team, the compliance and privacy functions and, for the most serious incidents, the Incident Response Team. The process includes prompt reporting, classification of the incident, containment, elimination of the threat, restoration of services, notification to the relevant authorities where necessary, and subsequent analysis of the causes and improvement measures.

6.1 Definition of a significant incident (criteria)

The significance of an incident is determined through an assessment based on six criteria: the number of users or counterparties involved and the associated reputational impact; the duration of the incident or service disruption; geographical scope; compromise of data confidentiality, integrity or availability; the criticality of the services and functions affected; and economic impact. Each criterion is assigned a score from 1 to 3, corresponding to a low, medium or high level. An overall score of 6 to 9 identifies a non-significant incident; 10 to 13, a significant incident to be assessed on a case-by-case basis; and 14 to 18, a high or major incident, subject to the applicable notification requirements.

6.2 Internal detection, response and mitigation process

Incidents may be detected through staff reports or via automated monitoring systems, log analysis, firewalls, antivirus software, intrusion detection tools and infrastructure monitoring services. Anomalies must be reported immediately and, in any event, within one hour of detection, using the designated company channels and subsequently ensuring a written and archivable record is produced. Technical staff carry out an initial analysis to verify the nature, source and severity of the incident, correlate the available logs and alerts, and distinguish genuine incidents from false positives. Once the incident has been confirmed, containment measures are implemented, such as isolating systems, locking accounts or disabling at-risk access; this is followed by the elimination of the threat through the removal of malicious code, updates, patches and the changing of compromised credentials, as well as the controlled restoration of systems using verified backups, integrity checks, hardening measures and final validation tests.

6.3 Notification flows to ACN and the relevant authorities

The Information Security Manager, with the support of the Incident Response Team and the legal and privacy departments, assesses whether the incident needs to be reported to the relevant authorities. For incidents classified as high or major, the CSIRT Manager handles operational communication with ACN and CSIRT Italia via the designated official channel, submitting an initial notification within 24 hours, a detailed update within 72 hours and a final report within one month. Medium-level incidents, on the other hand, are assessed on a case-by-case basis, formalised through a report by the Incident Response Team. Should the incident involve a personal data breach, the obligation to notify the relevant supervisory authority within 72 hours is also assessed; for foreign companies, the procedures for reporting to their respective national supervisory bodies apply.

6.4 External communications and reporting

Communications relating to incidents are coordinated by the Information Security Manager and must be approved by senior management where they have external or reputational implications. The relevant business functions are informed promptly and, for significant incidents, internal communication must take place within two hours of classification. Communications to customers, suppliers, partners, insurers or other stakeholders are made only with prior authorisation from senior management and in compliance with contractual and regulatory obligations. s and reports must specify at least the date and time of the incident, the systems and services affected, the impact on security and data, the corrective measures taken, the estimated time to recovery, and contact

details for further updates. Where necessary, a public statement may be prepared to manage reputational impacts and to keep stakeholders properly informed.

6.5 Incident Register and Post-Incident Analysis

Every incident must be recorded in the Incident, Non-conformity and Complaints Register, documenting the report, classification, actions taken, decisions made, notifications issued and the outcome of the incident handling. Logs, system images, network traces and other relevant digital evidence must be collected, secured, attached to the organisation's document management systems and retained for at least five years, unless otherwise required by regulatory obligations. Once the incident is resolved, a root cause analysis is carried out to identify the root cause, the vulnerabilities exploited and any organisational or technical factors that contributed to the incident. The conclusions and recommendations are set out in a final report, which is used to assess the effectiveness of the response, identify recurring incidents, update security measures, operational procedures and staff training, and share the lessons learnt with senior management.

7. Business Continuity and Recovery

The Group adopts a structured business continuity and disaster recovery model designed to ensure the continuation of critical services, minimise operational losses and restore systems, data and infrastructure compromised by serious or prolonged incidents as quickly as possible. The model applies to internal infrastructure, cloud services, archives, systems used by staff and company data, and involves a Crisis Committee tasked with assessing the severity of the incident, defining response priorities, coordinating technical activities and managing communications with internal departments, customers, suppliers and, where necessary, the relevant authorities.

7.1 Business Continuity / Disaster Recovery Plan

The Disaster Recovery Plan sets out the sequence of actions to be taken in the event of natural, technological, accidental or malicious incidents that significantly compromise the availability, integrity or operation of information systems and business services. Following the declaration of a disaster, the Crisis Committee assesses the extent of the damage, initiates internal communications and sets out the procedures for maintaining a minimum level of operations, including through remote working. The plan sets out differentiated priorities for service restoration, giving priority to systems necessary for development, authentication, data management and technical support, and defines specific maximum data loss objectives and recovery times. For the general corporate infrastructure, an RPO of 24 hours and an estimated RTO of 5 working days are specified, whilst for critical SaaS services, an RPO of 2 hours and an RTO of 2 days are specified.

7.2 Recovery and restoration procedures

Recovery procedures first involve verifying the availability of backup copies and residual infrastructure, followed by the restoration of the operational site, hardware components, corporate networks and servers in accordance with the defined order of priority. System recovery is carried out using verified backups and, where necessary, by rebuilding the infrastructure on alternative platforms. For incidents involving cloud or SaaS services, technical staff contact the provider' , jointly assess the scale of the incident and proceed to restore the service; should this not be possible, the system is rebuilt on a new infrastructure in accordance with the dedicated technical procedure.

Activities also include verifying data integrity, restoring connections between sites, the gradual reactivation of services, and informing customers of the recovery procedures and timelines.

7.3 Periodic tests and simulations

The effectiveness of the plan is verified through disaster simulations carried out at least once a year, involving both Italian sites and, in specific exercises, overseas sites. The simulations are designed to verify the Crisis Committee's ability to mobilise, the correct application of communication procedures, the availability of backups, the readiness of technical staff and the ability to restore services in accordance with established priorities and timelines. Staff are informed in advance via defined channels and within specified timeframes, whilst in the event of scheduled maintenance or planned infrastructure downtime, alternative organisational measures are put in place, such as the use of remote working. The results of the tests and simulations are documented and used to identify any shortcomings and update procedures.

7.4 Integration with corporate business continuity

The disaster recovery plan is integrated with general business continuity measures, incident management procedures, backup procedures, information security procedures and service level agreements entered into with external suppliers. Emergency management takes into account not only the technical restoration of systems, but also the continuity of essential business activities, customer support, communications and staff operations. Decisions taken by the Crisis Committee are formalised and coordinated with the relevant business functions, whilst outsourced services are managed in line with the contractually agreed levels of availability, maintenance and support. In this way, technological recovery is embedded within a broader framework of continuity management, aimed at reducing the operational, financial, contractual and reputational impacts arising from adverse events.

8. Training, awareness and a culture of security

The organisation promotes a widespread culture of security through structured training, refresher and awareness-raising programmes aimed at all staff. These initiatives are tailored to the roles and responsibilities held and focus, in particular, on cybersecurity, the Quality Management System, information security and the principles of secure development. Training is supplemented by regular communications, simulations and drills designed to maintain a high level of awareness of cyber risks and to test the organisation's response capabilities.

8.1 Training and awareness programmes

All new recruits undertake a compulsory training programme delivered via a dedicated platform, with content tailored to their role and the tasks they perform. The programme includes modules on cybersecurity, the Quality and Information Security Management System and, for relevant technical roles, secure software development. The initial programme is complemented by ongoing awareness-raising activities organised by the IT Department, through updates, communications and in-depth information on the main threats, the correct behaviour to adopt and how to report suspicious incidents.

8.2 Simulations and drills

The organisation carries out security incident simulations and business continuity tests every six months, with the aim of verifying the effectiveness of procedures, the coordination capacity of the departments involved and the readiness of staff to manage critical situations. Plans are also in place for simulated phishing campaigns, designed to measure users' awareness levels, identify any areas of risk and define targeted training initiatives. The results of the exercises are analysed to identify critical issues and progressively improve organisational and security measures.

8.3 Roles requiring specific training

System administrators and staff in the Research and Development Department receive specialist training commensurate with the responsibilities and privileges associated with their roles. For system administrators, the training covers the secure management of infrastructure, privileged access, configurations, vulnerabilities and incidents. For Research and Development staff, the training focuses on the principles of 'secure by design', secure development practices, code and data protection, and the prevention of application vulnerabilities. The training programmes are updated periodically in line with technological developments, regulatory changes and identified threats.

9. Assessment, internal audit and compliance

The Organisation periodically verifies the adequacy and effectiveness of the measures adopted to manage cybersecurity risks and to comply with applicable NIS2 obligations. Verification activities are planned using a risk-based approach and include internal audits, documentary checks, technical verifications, monitoring of indicators and assessment of the implementation status of improvement plans. The results are documented, communicated to the responsible departments and submitted to the administrative and management bodies, which approve the procedures for implementing security measures, oversee their implementation and are informed periodically or promptly of incidents and key issues.

9.1 Internal NIS2 compliance audits

Internal audits are carried out in conjunction with internal audits for compliance with the ISO 27001 standard, based on a periodic programme approved by senior management and aimed at verifying compliance with regulatory requirements, risk management measures, company policies and operational procedures. The audits focus, in particular, on cybersecurity governance, asset and access management, supply chain security, vulnerability and incident management, business continuity, training, and communication and notification obligations. Auditors must operate with appropriate competence, independence from the activities under review, and access to the necessary evidence. Each audit concludes with a report identifying compliance, observations, non-conformities, residual risks and corrective actions, specifying those responsible and the deadlines for implementation.

9.2 External audits and third-party audits

The Organisation may subject its systems, processes and security measures to independent verifications conducted by qualified bodies, including in the context of certification, contractual obligations, customer requests or specific risk assessments. External audits may include document reviews, technical assessments, security tests, vulnerability scans and checks on relevant suppliers.

The documentation and evidence produced must be retained and made available to the competent authorities upon request. The competent national NIS authority may request reports, self-assessments, implementation plans, periodic or targeted audits and security scans, particularly in the event of significant incidents or possible breaches of regulatory obligations.

9.3 Continuous monitoring and KPIs

The Organisation defines and monitors a set of quantitative and qualitative indicators to assess the effectiveness of the cybersecurity management system over time, in coordination with those established for compliance with the ISO 27001 standard and set out in the Annual Management Review. KPIs may include the number and severity of incidents, detection and response times, adherence to notification deadlines, the status of vulnerability resolution, the level of system updates, the outcome of backups and recovery tests, completion of training, the results of phishing simulations, open non-conformities and the time taken to close corrective actions. The indicators are reviewed periodically, compared against defined thresholds and targets, and used to identify anomalies, trends and areas requiring action.

9.4 Internal reporting to senior management

The functions responsible for security prepare periodic reports for senior management and the governing bodies, containing the compliance status, trends in key indicators, significant incidents, residual risks, audit outcomes and the progress of corrective action plans, all summarised in the Management Review. Any critical issues that may significantly affect service continuity, information security or compliance with regulatory obligations must be reported without delay. Management assesses the results, sets priorities, approves the necessary resources and oversees the implementation of improvement measures, in line with the responsibilities assigned to the administrative and management bodies under the NIS2 framework.

10. Supervision, inspections and audits by the authorities

The Organisation recognises the powers of monitoring, supervision, verification, inspection and enforcement conferred on the competent national NIS authority and undertakes to ensure full cooperation in the performance of the relevant activities. To this end, it keeps up to date, readily available and traceable the policies, procedures, risk assessments, audit reports, technical evidence, notifications, records and compliance plans necessary to demonstrate the effective implementation of security measures. The ACN, in its capacity as the competent national NIS authority, monitors compliance with obligations and may request information, self-assessments, audits and specific verification activities.

10.1 Cooperation with the competent authorities

All requests from the National Competent Authority for NIS, CSIRT Italia or other authorised authorities must be dealt with promptly and coordinated by the designated corporate functions. The Organisation shall provide complete, accurate and verifiable information, facilitate access to the requested documentation and evidence, and ensure the support of the relevant technical, legal and organisational staff. Communications are formally recorded and retained, detailing the requests received, the responses provided, the decisions taken and any commitments to comply. Failure to cooperate with the competent national NIS authority or with CSIRT Italia constitutes a punishable breach.

10.2 Inspection and verification procedures

The competent authority may carry out checks on the documentation and information submitted, on-site or remote inspections – including unannounced ones – and request access to data, documents and any further necessary information. The organisation shall designate in advance the contact persons responsible for assisting the inspectors, coordinating the collection of evidence and ensuring that all activities are carried out in accordance with the instructions received and confidentiality requirements. Requests, reports, evidence submitted and the outcomes of the assessment must be recorded and retained. For entities classified as significant, inspection powers are exercised where there is evidence or information suggesting a possible breach.

10.3 Management of non-conformities and corrective action plans

Non-conformities identified through audits, internal checks or inspections by the authorities are recorded, analysed and classified according to their severity and the associated risk. For each non-conformity, a corrective action plan is drawn up, setting out the causes, the measures to be taken, those responsible, the necessary resources, deadlines and the procedures for verifying effectiveness. Actions are monitored until they are fully resolved, and their status is reported to senior management and, where required, to the competent authority. The latter may issue binding instructions, require the rectification of deficiencies, order the implementation of recommendations arising from audits, mandate the cessation of non-compliant behaviour and, in the event of non-compliance, issue a formal warning.

10.4 Penalties and liability

Breaches of NIS2 obligations may result in corrective measures, formal warnings, administrative fines and further measures provided for by law. For private essential operators, the most serious breaches may be penalised with fines of up to 10 million euros or, if higher, up to 2 per cent of global annual turnover; for important entities, up to €7 million or, if higher, up to 1.4 per cent of global annual turnover. In the cases provided for, the Authority may also impose temporary measures on natural persons holding managerial positions. The administrative and management bodies are responsible for approving and supervising risk management measures and may be held liable for breaches in accordance with the applicable provisions.

11. Review and updating of the policy

This policy is subject to periodic review to ensure its suitability in relation to the organisational context, threats, technologies used and applicable regulatory obligations. The review takes into account audit findings, security indicators, incidents that have occurred, changes to processes and services, the results of risk assessments and guidance received from the competent authorities. Any update must be formally approved, communicated to the relevant functions and accompanied by the updating of the relevant operational procedures and training activities.

11.1 Frequency and method of review

The policy is reviewed at least annually by the departments responsible for security, compliance and information systems, with the involvement of other relevant company departments. The review verifies the document’s consistency with the corporate strategy, the risk assessment, developments in the technological and organisational scope, and current regulatory requirements. Proposed

amendments are documented, submitted to senior management and approved by the relevant bodies before they come into force.

11.2 Circumstances requiring an extraordinary review

Irrespective of the periodic review, the policy must be updated in the event of significant incidents, new threats or material vulnerabilities, regulatory changes or guidance from the competent authority, the introduction of new technologies, substantial changes to infrastructure or services, acquisitions and reorganisations, changes in the supply chain, or adverse audit and test results. The need for a review is also assessed when indicators show a deterioration in the level of security or the ineffectiveness of existing measures.

11.3 Versioning and approval

Each version of the policy must include at least the revision number, the date of issue, a brief description of the changes, the person responsible for drafting it, and the persons responsible for reviewing and approving it. Obsolete versions are archived in accordance with document retention rules and made unavailable for operational use, whilst ensuring their traceability is maintained. The current version is published on authorised company channels and communicated to the relevant staff; substantial changes must be accompanied, where necessary, by specific information or training activities.

12.Appendices and technical references

12.1 List of measures and requirements in accordance with Annex 1 / Annex 2

All relevant requirements of Annex 1 are applied. The technical implementation procedures are set out and updated at least annually in the document ‘Security measures for important NIS entities’ linked to the ISO 27001 SOA.

12.2 Related documentation

Group companies maintain a constantly updated register of documentation for all management systems and regulatory compliance (4.01 MOD EDS List of system documentation).