POLICY

PP–048 v 3.0

GROUP SECURITY POLICY

COVER

Title	Group Security Policy
Classification	Policy
Document code	PP-048
Approved by	Nexi SpA BoD
Approval date	08/05/2024
Date of entry into force	08/05/2024

UPDATES

Version	Date	Code	Updates
1.0	22/12/2021	PP-048 v 1.0	First issue.
2.0	05/04/2023	PP-048 v 2.0	Updated version of the Group Security Policy.
2.1	01/09/2023	PP-048 v 2.1	Aligned references to Group Security Standard in Appendix B.
3.0	08/05/2024	PP-048 v 3.0	Annual review. Minor changes and terminology alignment.

TABLE OF CONTENTS

1 INTRODUCTION

As information is one of the most valuable assets for Nexi Group ("Group"), trust in the Group's ability to safeguard customers' assets is essential for the success of the Group's business. Therefore, security in Nexi Group must be highly prioritized and must comply with applicable laws, regulations and customer contracts.

1.1 PURPOSE

This Group Security Policy ("Policy") is the top-level policy which reflects Management commitment to security. It is supported by internal regulations that provide the core directions for preserving the confidentiality, integrity and availability of the Group's information assets.

The purpose is to instill trust towards Nexi Group and manage security risks by establishing Group-wide requirements for effective security practices and governance across people, processes and technology.

Nexi Group promotes an environment of ethical and controlled information handling to protect information and information systems against security threats that may adversely affect the Group and its stakeholders.

Nexi Group has established this Policy to:

- Support the Group's strategy by making security a key business factor and an integral part of service offerings
- Define the baseline expectations with regards to the Group's security posture and promote a secure environment
- Foster a security culture and establish responsibility and accountability for security in the Group
- Set basis for the Group Security Framework ("Security Framework") and the internal security regulation as part of the Security Framework
- Establish a common ground for a consistent way of implementing technical, organizational, administrative and physical security controls in the Group
- Ensure compliance with legal and regulatory obligations applicable to the Group.

1.2 APPLICABILITY

This Policy applies to all legal entities of Nexi Group.

This Policy applies to all Group's functions, mangers, employees, collaborators, partners, outsourcers, suppliers and other parties who may have access to non-public corporate information when it is stored, transferred or processed.

Its content must, therefore, be brought to the attention of anyone who participates, even partially, in the operation and management of business processes.

1.3 ENFORCEMENT

Deviations from this Policy or related internal regulations must be formally approved and appropriately managed in accordance with the Security Framework.

Failure to comply with this Policy may lead to disciplinary actions in accordance with applicable local legislation.

1.4 APPROVAL AND REVIEW

This Policy is approved by the Board of Directors (BoD) of Nexi SpA.

This Policy must be approved by local Board of Directors of the Group's legal entities. Where local regulations and requirements are stricter than this Policy, the local regulations will be enforced by the respective Group company.

Group Risk Management and Group Security functions are responsible for updating this Policy to meet the security requirements. It must be reviewed at least annually and whenever deemed necessary based on changes in the Group's internal or external environment, such as changes in organizational structure, cyber threat landscape, technology, or laws and regulations, mergers & acquisitions and incidents, and following supervisory instructions or conclusions derived from relevant digital operational resilience testing or audit processes.

2 PRINCIPLES

- Group Chief Information Security Officer (Group CISO) has the mandate to make decisions affecting security across the Group and leads the Group-wide security function
- Managers are responsible for security within their management area
- Employees, and other parties entrusted with Group's assets, are responsible for security within their area of responsibility and for acting with due care
- Accountability cannot be delegated
- Nexi Group adopts a risk-based approach to security
- Nexi Group adopts the Three Lines of Defense governance model to enhance the management of risks and Three Levels of Controls model on internal controls
- The Security Framework defines baseline internal regulations for security to be implemented across the Group, such as performance measurement, minimum security requirements, related mandatory guidelines, processes and procedures, including governance and management
- Security Framework must be kept appropriate and effective.

3 ROLES AND RESPONSIBILITIES

The realization of the Nexi Group's strategic security objectives depends on their proper incorporation into the business functions and the organizational structure of the Group and Group companies. This chapter introduces the key security roles and their main security related responsibilities.

3.1 GROUP LEVEL

The following key roles with Group-wide responsibilities have been defined to ensure consistent and extensive approach to security throughout Nexi Group.

Group Chief Information Security Officer (Group CISO)

Group Chief Information Security Officer is the head of Group security function. The Group CISO is responsible for the security strategy, Security Framework and overseeing security programs and activities on both Group and local levels.

Group Risk Management

Group Risk Management defines, together with the Group security function, the Group Security Policy and monitors the update and implementation status. Group Risk Management verifies that the Security Framework is consistent with the Group companies' operations and risk profiles.

3.2 LOCAL LEVEL

All Group companies must ensure effective operation of the Security Framework at local level. Additional local roles and corresponding security responsibilities required for the local operations may be defined and assigned. The following local key security roles have been defined.

Local Security Focal Point (LSFP)

Each Group company has a Local Security Focal Point who acts as the Group company's primary security representative. The LSFPs are responsible for supporting the development, implementation and governance of the Security Framework and the local adaptation of it within the Group company. They head the Local Security Team (LST) if one is required due to the size and complexity of the Group company.

Local Risk Management Focal Point (LRMFP)

The Local Risk Management Focal Point is responsible for monitoring the local implementation of the Group Security Policy, defining, if needed, the local security policy together with the LRMFP and monitoring the performance and effectiveness of the local Security Framework.

Managers

Each manager is responsible for security within their management area ensuring the compliance with this Policy, the Security Framework and the local implementation, including the daily activities executed by the employees and Third Parties under their supervision. Managers are also responsible for providing users with appropriate security training based on their role or area of responsibility.

Users

Users of Nexi Group's information and IT assets and resources are responsible for performing their assignments and activities responsibly and in compliance with this Policy and internal security regulation. Users' responsibilities are defined in the Group End User Security Code of Conduct and Group Contractor Security Code of Conduct.

Other entity specific roles

Each Nexi Group company must define and assign additional entity specific roles and the corresponding security responsibilities. The operations of each organization must be properly documented and carried out in a way that minimizes the possibility for conflicting duties that may give rise to the potential for fraud or error and, where necessary, enforce the four-eyes principle.

3.3 EXTERNAL STAKEHOLDERS

Customers

Nexi Group strives to achieve high level of security in the management of customer information in accordance with contractual obligations, applicable legislation and security standards and well-known industry best practices. Group's responsibility to protect customer information, security controls and reporting of security incidents and imminent threats must be officially documented in the respective contractual agreements.

Third Parties

Third Parties are obliged to perform their assignments in accordance with the contractual agreement between the Third Party and Nexi Group and the relevant parts of the Security Framework. All security requirements and obligations are formally specified and contractually agreed. Third Parties are responsible for promptly reporting any suspicious events to the Group. The most critical Third Parties are identified and included in the scope of risk management activities.

Authorities

Nexi Group collaborates with the competent police, judicial, audit, supervisory and other public authorities by satisfying the relevant requests or other obligations. Appropriate contacts are maintained with supervisory and regulatory authorities on security-related matters, including external auditors, payment schemes, Data Protection and European Banking Authorities and other local government bodies and institutions. Nexi Group is committed to complying with all applicable laws, regulations, standards, guidelines and rules set out by these authorities by implementing appropriate technical and organizational controls and providing sufficient evidence of conformity as well as adequate information and reporting, when necessary.

Special Interest Groups

Nexi Group maintains contacts with special interest groups on security matters and monitors the evolving operating environment and threat landscape on a regular basis. In this context, it actively collaborates with institutions such as Euro Cyber Resilience Board and national CERT authorities, thus contributing to the enhanced collective cyber defensive capabilities of a broader community.

4 SECURITY DOMAINS

This chapter describes the security domains that define the structure of the Group Security Standards (listed in appendix B) and the other internal security regulation documentation. In particular, all the security domains must be enforced to preserve the availability, authenticity, integrity, and confidentiality of information assets owned or governed by Nexi Group.

4.1 APPLICATION SECURITY

Application Security domain establishes mandatory security requirements of Group's applications throughout their lifecycle (including applications such as Commercial off-the-Shelf - COTS, Generative AI tools and SaaS).

Objective is to ensure that applicable security requirements are identified, appropriate security controls are implemented, and secure software development techniques (S-SDLC) are used to safeguard the confidentiality, integrity and availability of information processing and the continuity of business services throughout the application lifecycle.

4.2 CLOUD SECURITY

Cloud Security domain establishes mandatory security requirements for Nexi Group's cloud service providers and the related cloud services.

Objective is to ensure that:

- Security requirements are identified and enforced during and upon termination of cooperation with cloud service providers
- Cloud services consumed by the Group comply with relevant security-related regulatory and contractual requirements and industry best practices.

Cloud services provided by Nexi Group are subject to all relevant internal security regulation as well as relevant external regulations and industry best practices.

4.3 CYBER DEFENSE

Cyber Defense domain establishes mandatory security requirements in the areas of security logging and monitoring and threat intelligence.

Objective is to ensure that:

- Information systems produce sufficient logs to enable monitoring of the information systems' operation and performance, facilitate timely detection and investigation of security events and incidents and verify compliance with established security controls
- Current and emerging security threats are timely detected, analyzed and reported to enable risk-aware decisions that efficiently strengthen defenses and preempt future attacks.

4.4 DATA SECURITY

Data Security domain establishes mandatory security requirements for protecting information assets owned or governed by Nexi Group.

Objective is to ensure that:

- Nexi Group's information assets in any form (e.g. physical, digital, electronic) are adequately and efficiently protected throughout their lifecycle based on their business criticality and sensitivity regarding confidentiality, integrity, authenticity and availability.

- Information assets at rest, in transit and in use are adequately protected from internal and external threats, including the intentional and accidental leakage, loss or corruption.

4.5 ENDPOINT SECURITY

Endpoint Security domain establishes mandatory security requirements for Nexi Group's endpoints.

Objective is to ensure that:

- Workstations and mobile devices are properly and securely managed to protect Group's information assets
- Appropriate security controls are enforced to safeguard the operation of workstations and mobile devices
- Anti-malware, data loss prevention and other security mechanisms are implemented to protect Group's information assets.

4.6 IDENTITY AND ACCESS MANAGEMENT

Identity and Access Management domain establishes mandatory security requirements for identity and access management in Nexi Group.

Objective is to ensure that access to information and IT resources is authorized, controlled, and managed according to the business needs and security requirements to protect the availability, authenticity, integrity and confidentiality of information assets.

4.7 NETWORK AND COMMUNICATIONS SECURITY

Network and Communications Security domain establishes mandatory security requirements for Nexi Group's networks and electronic communications.

Objective is to ensure the:

- Protection of Group's information assets in transit
- Provision of secure connectivity to untrusted and external networks
- Protection of Group's networks from internal and external threats
- Hardening of network services

4.8 PERSONNEL SECURITY

Personnel Security domain establishes mandatory security requirements which must be met during the employment lifecycle of Nexi Group's personnel.

Objective is to ensure that:

- Personnel security is managed throughout the employment lifecycle
- Personnel security requirements are implemented to reduce risks caused by human mistake, abuse and fraud
- Nexi Group's employees
    - Understand their responsibilities in protecting the Group's information and IT assets
    - Are well informed about the security implications of their actions with respect to the protection

of the Group's information assets

- Have been sufficiently trained on security matters.

4.9 PHYSICAL SECURITY

Physical Security domain establishes mandatory security requirements applicable to Nexi Group's premises.

Objective is to ensure that adequate and proper security measures are implemented to prevent and deal with both intentional and unintentional physical and environmental threats that can cause damage to information and IT assets and information processing premises.

4.10 SECURITY GOVERNANCE

Security Governance domain establishes mandatory security requirements for the governance of security in Nexi Group.

Objective is to ensure that:

- Security requirements are considered in the design of processes, projects, systems and controls through "security by design" process
- Security requirements, processes and controls are designed and implemented taking into account requirements arising from relevant laws, regulations, standards and contractual obligations towards the customers
- The suitability, effectiveness and efficiency of the security processes and controls are monitored, evaluated based on measurements to ensure continuous improvement and reported to the Top Management regularly.

4.11 SECURITY INCIDENT MANAGEMENT

Security Incident Management domain establishes mandatory security requirements for managing security incidents in Nexi Group.

Objective is to ensure:

- A consistent approach to the management of security incidents
- Effective handling of security incidents
- Immediate and effective communication of security incidents.

4.12 SECURITY TESTING AND VULNERABILITY MANAGEMENT

Security Testing and Vulnerability Management domain establishes mandatory security requirements for security testing and vulnerability management in Nexi Group.

Objective is to ensure that vulnerabilities are identified and remediated in a timely manner to minimize the attack surface and mitigate related IT and security risks.

4.13 SYSTEM SECURITY

System Security domain establishes mandatory security requirements for Nexi Group's information systems.

Objective is to ensure stable and secure operation of Nexi Group's information systems.

4.14 THIRD PARTY SECURITY

Third Party Security domain establishes mandatory security requirements for Nexi Group's Third-Party engagements.

Objective is to ensure that:

- Security requirements are identified and enforced during, and upon termination of, cooperation with Third Parties
- Contractors are well-informed about their responsibilities in protecting the Group's information and IT assets.

APPENDIX A – REFERENCES

A.1 EXTERNAL REGULATION

- Regulation (EU) 2016/679 (GDPR)
- Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market (PSD2)
- Regulation (EU) 2021/728 of the European Central Bank of 29 April 2021 amending Regulation (EU) No 795/2014 on oversight requirements for systemically important payment systems (ECB/2021/17)
- Cyber resilience oversight expectations for Financial Market Infrastructure
- Guidelines on business continuity for market infrastructures
- CODISE - Working Group for operational crisis management coordination in the Italian financial marketplace
- EBA/GL/2019/04 EBA Guidelines on ICT and security risk management
- Regulation (EU) 2022/2554 (DORA)

A.2 INTERNATIONAL STANDARDS AND INDUSTRY BEST PRACTICES

- ISO/IEC 27001:2013 - Information technology - Security techniques - Information security management systems - Requirements
- ISO/IEC 27002:2013 - Information technology - Security techniques - Code of practice for information security controls
- ISO/IEC 27005:2011 - Information technology - Security techniques - Information security risk management
- ISO/IEC 27017:2015 - Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services
- ISO/IEC 27018:2014 - Information technology - Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
- ISO/IEC 27701:2019 - Security techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines
- Payment Card Industry (PCI) Standards
- COBIT Security Framework
- NIST Cybersecurity Framework
- ISF Standard of Good Practice for Information Security

APPENDIX B – GROUP SECURITY STANDARD

The Group Security Standard document STD-001 Group Security Standard contains security requirements for the following domains:

01 – Application Security

02 – Cloud Security

03 – Cyber Defense

04 – Data Security

05 – Endpoint Security

06 – Identity and Access Management

07 – Network and Communications Security

08 – Personnel Security

09 – Physical Security

10 – Security Governance

11 – Security Incident Management

12 – Security Testing and Vulnerability Management

13 – System Security

14 – Third Party Security