STANDARD

STD–001 v 3.1

GROUP SECURITY STANDARD

COVER

Title	Security Standard
Classification	Standard
Document code	STD-001
Approved by	Nexi Group CISO
Approval date	21-11-2024
Date of entry into force	21-11-2024

UPDATES

Version	Date	Code	Updates
1.0	14-07-2022	STD-001	First issue of the STD-001 Application Security Standard.
2.0	10-07-2023	STD-001	Document scope and name changed to include all 14 v 1.0 Security Standards into one Group Security Standard. Updates to requirements based on EBA guidelines, Bilag 5 and received feedback.
2.1	22-12-2023	STD-001	Minor corrections and adjustments based on feedback and an audit finding.
3.0	30-09-2024	STD-001	Periodical review. Integrated new relevant DORA, PCI and Generative AI security requirements.
3.1	21-11-2024	STD-001	Minor updates.

TABLE OF CONTENTS

1. INTRODUCTION

1.1 PURPOSE

The purpose of this Standard is to establish mandatory security requirements for Nexi Group.

This document consists of two parts:

- Chapter 2 contains the **baseline** security requirements
- Chapter 3 contains **extended** security requirements relevant for PCI DSS, PCI 3DS and PCI PIN requirements.

The security requirements can be supplemented with Technical Security Standards, Security Guidelines, Processes and other Security documents as needed.

1.2 APPLICABILITY

This Standard applies to all Nexi Group Companies and Third Parties providing services to Nexi Group in accordance with their contractual obligations.

The requirements set forth in this Standard must be met in accordance with applicable laws, regulations, statutory and contractual requirements as well as other baseline security requirements in this document.

2. SECURITY REQUIREMENTS

The objective of each security domain is described in the Nexi Group Security Policy. In particular, all the security domain requirements must be enforced to preserve the availability, authenticity, integrity, and confidentiality of information assets owned or governed by Nexi Group. The security requirements are designed taking into account the approved information classification scheme and the IT risk assessment processes.

2.1 APPLICATION SECURITY

Applicability:

Application Security requirements apply to all Nexi Group Companies and cover all Group's applications regardless of whether they are developed inhouse, outsourced or purchased off-the-shelf.

2.1.1 GENERAL PRINCIPLES

Req ID	Requirement
01.01	All applications must be assigned a business owner and an IT owner with clearly defined management responsibilities and authority.
01.02	All security requirements applicable to the applications must be identified, documented and complied with throughout the application's lifecycle. *The identification of security requirements must take into consideration applicable requirements in the Group Security Standard, Security by Design process and checklist as well as other relevant security, regulatory and contractual requirements.*
01.03	Security controls addressing the identified security requirements must be defined, implemented and documented throughout the application's lifecycle.

Req ID	Requirement
01.04	Information systems and applications must be designed to protect the information processed, transmitted or stored from threats in alignment with the classification and protection needs of the information throughout the application's lifecycle.
01.05	Information systems and applications must be classified according to their business criticality, risk profile and classification level of the information assets processed or retained in the applications.
01.06	The principles of security architecture must be defined and documented.
01.07	Inventories of software components, including third-party and open sources libraries, and components off-the-shelf (i.e. COTS), used in applications must be maintained. **This requirement is a best practice until 17 January 2025, after which it will be required.** **Until 17 January 2025, the mandatory requirement is the following:** Inventories of software components, including third-party libraries, used in applications must be maintained.
01.08	For Information systems and applications supporting critical or important function, with the collaboration of the third-parties as appropriate, must be monitored the related third-party libraries version and possible updates. **This requirement is a best practice until 17 January 2025, after which it will be required.**
01.09	Vendor vulnerability and patch availability announcements on software components and third-party libraries used must be monitored. The identified patches must be applied according to a patch management process.

2.1.2 SECURE DEVELOPMENT

Req ID	Requirement
01.10	Software development processes must, at a minimum, address common vulnerabilities provided by OWASP top 10.
01.11	The defined principles of security architecture must be applied when designing new applications.
01.12	Applications must be able to support a mapping of roles and the assigned user IDs.
01.13	Modifications to software packages must be limited to what is necessary for the software to function as intended and follow the defined change management process.
01.14	Software applications must implement adequate data validation checks in order to avoid security errors, weaknesses and targeted attacks.
01.15	Access to application source code must be restricted to the authorized personnel or Third Parties.

Req ID	Requirement
01.16	Changes to production source code must be strictly controlled according to the defined change management process.
01.17	Source code and libraries must not be stored in production environment.
01.18	Source code must be retained in a version control infrastructure.
01.19	Applications must be tested to ensure that they meet the identified security requirements at functional and technical levels.
01.20	Prior to releasing to production, application security testing must be performed to ensure that application is developed in accordance with the secure coding guidelines.
01.21	Information Systems must be hardened, and nonessential services and ports must be turned off prior to releasing to production.
01.22	All remnants of testing must be securely removed from information system before it is deployed into production. *Examples of removable items: test data, test users, test configuration.*
01.23	The operation, support and maintenance duties in development and production environments must be controlled to ensure effective segregation of duties between the environments.
01.24	The development methodology used by the Third Party of outsourced development services must include relevant secure software development activities.

2.1.3 WEB APPLICATION FIREWALL

Req ID	Requirement
01.25	Internet-facing applications must be protected by web application firewall. Alternatively, application vulnerability security assessments must be performed at least annually and after significant changes prior to deployment.
01.26	Application-level firewall configuration must be kept current and reviewed at least annually.

2.1.4 GENERATIVE AI SECURITY

Req ID	Requirement
01.27	Gen AI tools input/learning data must be collected for a specific purpose to create a dataset with the sole aim to train the AI model dedicated strictly to the contracted services.
01.28	Gen AI tools must have in place mechanisms to enforce: • Dataset diversity and data collection quality assurances • Regular algorithmic auditing to identify and rectify bias.
01.29	Gen AI tools provided by Third Parties deployed as a cloud service and used also by other Third Parties' customers, must not use Nexi-provided inputs to train the generic LLM (business data or conversations uploaded to train a dedicated LLM instance).
01.30	The source/origin of the Gen AI tools training dataset must be established.

Req ID	Requirement
01.31	Protection against the Gen AI tools prompt manipulation must be based upon both the syntax and context analysis. This includes filtering of both Gen AI tools inputs and outputs. The intended result of this control is preventing output of incorrect automated responses (e.g. hallucinations, data manipulation, data poisoning etc.).
01.32	Whenever feasible, features provided by the Gen AI tools must be tested and evaluated within a dedicated “sandbox” environment.

2.2 CLOUD SECURITY

Applicability:

Cloud Security requirements apply to all Nexi Group Companies and cover all types of cloud services consumed by the Group.

2.2.1 GENERAL PRINCIPLES

Req ID	Requirement
02.01	The selection of a Cloud Service Provider and cloud service contracts must adhere to the Third-Party security requirements in the Group Security Framework. *Cloud services used by the Group are subject to all applicable security requirements in the Group Security Standard as well as any additional service-specific security requirements.*
02.02	Prior to the adoption of cloud services following Security by Design process, a security risk assessment must be carried out to identify and evaluate relevant security risks. *Considering:* • *The security implications of the cloud service* • *The security features provided by the Cloud Service Provider.*
02.03	Prior to the use of a cloud service, adequate security mechanisms must be implemented to mitigate identified risks and to sufficiently protect Group's information.
02.04	Cloud service contracts must clearly define all applicable security aspects depending on the services provided, in compliance with Third Party security requirements, including: • Geographical locations where information processing may take place • Legal jurisdictions governing the cloud service.
02.05	Cloud Service Provider must follow the security requirements defined in the Security Testing and Vulnerability Management domain. If Nexi Group cannot perform the testing, the Cloud Service Provider must provide evidence of conducted security testing and vulnerability scanning and remediation.
02.06	Cloud services acquired must be hardened according to the industry best practices. *Example of industry best practices: Center for Internet Security (CIS) hardening guidelines.*
02.07	Cloud Service Provider must provide evidence of compliance with all applicable legal and contractual requirements upon request.
02.08	Connection between the Group and Cloud Service Provider's infrastructure must be via secure and protected channels. *Examples of secure and protected channels: VPN, IP whitelisting.*
02.09	Multi-Factor Authentication mechanisms, access controls, network segregation and encryption must be implemented in cloud services to prevent unauthorized access to and disclosure of the cloud service information and resources.

Req ID	Requirement
02.10	Cloud services integration with the Group's security logging and monitoring solutions must be evaluated. *Integration is not always technically possible but must be done if evaluated feasible.*
02.11	Cloud Service Provider must provide the following: • Logging and monitoring capabilities concerning at least security events, service level and resource usage • Information about implemented security controls • Information about technical vulnerability management • Information about changes that could adversely affect the provided cloud service.
02.12	Each Group's virtual instance running on a cloud service must be isolated from the virtual instances of other customers and protected from unauthorized network access attempts.
02.13	Segregation of access must be enforced in the following cases: • Between tenants in a multi-tenant environment • Between Cloud Service Provider's internal administration environment and the cloud environments of the customer.
02.14	Termination of the cloud service must be done in a secure and controlled manner according to the contractual obligations. *Examples of termination actions to be verified, where applicable:* • *Termination of communication links and access* • *Secure removal and/or return of Group information and IT assets hosted or stored in the cloud service.*

2.3 CYBER DEFENSE

Applicability:

Cyber Defense requirements apply to all Nexi Group companies and cover Nexi Group's IT environments.

2.3.1 SECURITY MONITORING

Req ID	Requirement
03.01	Capabilities to monitor and detect anomalous activity and events must exist and cover relevant internal and external factors and threats. *Capabilities cover people, processes and technology and include monitoring of user activity and security events in e.g. connections, devices and software, both internal and Third-Party services.*
03.02	Defined mechanisms for security logging and monitoring must exist, including: • Onboarding of log sources to a centralized log management system • Formalized criteria for evaluation and selection of logs and events for security logging • Definition of log correlation rules and relevant use cases.
03.03	Detection capabilities, baseline profile of system activities as well as criteria, parameters and triggers must be documented, implemented, periodically reviewed, tested and updated appropriately in a controlled manner. *To enable timely detection of deviations from the baseline, such as anomalous activities and events.*
03.04	Information systems and IT infrastructure components must generate logs that include, at a minimum: • Security events • Activities performed by service accounts • Standard and privileged users' activities and send them to a centralized log management system. *Examples of activities to be logged: file transfer activities, database activities, privilege elevation and modification attempts and requests, modification of system configurations.* *IT infrastructure components include network devices and databases.*
03.05	Applications must generate logs that include, at a minimum, standard and privileged users' activities. *Examples of activities to be logged: log-in, log-out and log-fail events.*
03.06	The following events on users' activities related to Information systems and IT infrastructure must, at a minimum, be logged: • Authentication and authorization events including invalid logon attempts • Actions taken by an individual with root or administrative privileges • Access to all audit trails • Successful and failed attempts to escalate user privileges

Req ID	Requirement
	• Creation, modification, and deletion of system-level objects • System shutdown, start-up, and restart • Initialization, stopping and pausing of audit logs. *Examples of system level objects in this context: users, groups, critical files and directories secret and private keys.*
03.07	Logs must contain sufficient detail to enable the reproduction of any action, including: • User ID • Event type • Date and time • Success or failure indication • Origin of the event: hostname or IP address, as applicable • Identity or name of affected data, system component, or resource.
03.08	Logged user activities must be traceable to a unique user.
03.09	Logs must not contain the following information in clear text: • Full Primary Account Number (PAN) • Sensitive Authentication Data (SAD) • Passwords and authentication factors • Sensitive personal data (GDPR) • Biometric data (GDPR).
03.10	The logs subject to security monitoring must be reviewed and analyzed regularly to identify potential security incidents.
03.11	Logged information must be available to support security incident management process. *Analysis of logged information can help to understand the nature of incidents and identify trends.*
03.12	Logs must be collected through automated monitoring tools that create appropriate alerts and consolidated reports.
03.13	Security alerts must be monitored continuously to address events in a timely manner. *Including monitoring of and alerts from network devices.*
03.14	Security alert criteria, parameters and thresholds must be defined to trigger and facilitate the incident response process.
03.15	Logs must be properly managed to support forensic investigation.
03.16	Access to logs and the use of detection and analysis tools must be limited to authorized individuals.

Req ID	Requirement
03.17	In compliance with any applicable laws, only the Cybersecurity departments and the Control Functions are authorized to request the extraction of logs or recordings from the Privileged Access Management (PAM) systems. Extraction requests may be made for security reasons, such as: • Investigation of security incidents or breaches where access to privileged accounts or actions taken by privileged users are suspected • Incident response activities requiring analysis of privileged access activities for threat detection and mitigation • Compliance internal or external audits or regulatory inquiries that necessitate access to privileged access logs for verification purposes • Routine security monitoring and analysis to ensure compliance with security policies and standards • During operational troubleshooting or debugging scenarios requiring analysis related to privileged access controls • Any other circumstances approved by the Group/Local Chief Information Security Officer (CISO).
03.18	Logs and the log management system must be protected against accidental or intentional alteration. *Examples of protection mechanisms: file integrity monitoring software, change detection software, physical segregation, and/or network segregation.*
03.19	Logs must be retained for at least twelve months with a minimum of three months immediately available and in accordance with the applicable retention requirements. *Applicable retention requirements cover e.g. customer contracts and other business requirements, local laws, and regulatory requirements.*
03.20	The performance and capacity parameters of applications, information systems, and networks must be monitored continuously to detect indications of service degradation or availability issues that may be associated with cyber-attacks.
03.21	Employees and contractors monitoring and analyzing logs must be trained to identify and report anomalous activity and events.

2.3.2 THREAT INTELLIGENCE

Req ID	Requirement
03.22	A security threat intelligence capability, supported by analytical tools and threat information sharing with approved partners, must be established.
03.23	Threat information on adversarial attacks must be collected both from internal and external sources. *Examples of internal sources: event logs, alerts, and past incident reports* *Examples of external sources: industry and subject matter experts, government intelligence agencies and Computer Emergency Response Teams (CERTs), information sharing groups and partnerships that provide information on security threats and vulnerabilities, media reports and other publicly available information.*
03.24	The collected threat information must be analyzed continuously by skilled and experienced analysts to identify potential threat events, early warnings and insights taking into consideration the Group's business objectives, priorities and operating environment.
03.25	The analysis of collected threat information must include tactics, techniques and procedures (TTPs) of real-life attackers, their modus operandi and information on geopolitical developments.
03.26	A Cyber Threat Dashboard that contains the identified results of the threat information classification and analysis must be developed and maintained. *The Cyber Threat Dashboard may be integrated into risk reporting.* **This requirement is a best practice until 17 January 2025, after which it will be required.** **Until 17 January 2025, the mandatory requirement is the following:** A Cyber Threat Dashboard that contains the identified results of the threat information analysis must be developed and maintained. *The Cyber Threat Dashboard may be integrated into risk reporting.*
03.27	Threat intelligence results must be timely communicated to relevant stakeholders to: • Assist in determining acceptable business risks, optimizing resource allocation for security and proactively respond to the modern threat landscape • Assist in mitigating security risks at the strategic, tactical and operational levels • Inform about targeted improvements to existing security controls and processes to defend against or mitigate potential attacks • Support incident response and post-incident activities. *Example: Security testing plan updated based on the received threat intelligence information to ensure its alignment with the latest threat landscape, attacker's modus operandi and vulnerabilities.*

2.4 DATA SECURITY

Applicability:

Data Security requirements apply to all Nexi Group Companies as well as contractors and Third Parties who have access to or provide services that store, transfer or process information assets owned or governed by the Group.

2.4.1 DATA PROTECTION

Req ID	Requirement
04.01	Information assets must have an assigned Information Owner. Information ownership is assigned to business leaders who have management responsibility and accountability for controlling the entire lifecycle of the information assets supporting their operations.
04.02	A formal and structured information classification scheme must exist. The classification scheme must define: • Classification levels • Protection requirements for each level • Evaluation criteria that take into account confidentiality, integrity, authenticity and availability requirements.
04.03	Information assets must be classified in accordance with the information classification scheme.
04.04	Inventories of information assets must be maintained, including classification levels and assigned Information Owners of the registered information assets.
04.05	Information assets must be protected throughout their lifecycle in accordance with the information classification scheme.
04.06	Information assets classified as confidential or strictly confidential must be protected with the use of either strong cryptographic functions or other strong data obfuscation techniques when at rest. *Including information assets stored in databases.* *Data obfuscation, i.e. data masking, is the act of anonymization, pseudonymization, scrubbing, or de-identification.* *Obfuscation techniques: encryption, tokenization, scrambling, nulling out or deletion, value variance, substitution, shuffling, redaction.*
04.07	Non-public information must be protected by strong encryption and secure protocols when in transit over public or untrusted networks.
04.08	Where encryption of data in use is not possible, it must be processed in a separated and protected environment accordingly to CHAPTER 2.7.2. **This requirement is a best practice until 17 January 2025, after which it will be required.**
04.09	Information assets' classification and labelling must be kept up to date throughout their lifecycle and re-evaluated in the event of significant changes to the information asset or the

Req ID	Requirement
	applicable security requirements.
04.10	Information assets stored and/or processed within an IT asset must be identified for the proper classification of the IT asset and the related services.
04.11	Databases and other IT assets used to store or process information assets must be protected with security controls in accordance with the information classification of the stored data. *Examples of database security controls: DB firewall, encryption.*

2.4.2 DATA RETENTION

Req ID	Requirement
04.12	A retention period must be specified for information assets. The retention period, and the information to be stored, must be limited to what is required for legal, regulatory, and business purposes.
04.13	A process to identify and securely delete information assets no longer needed or when their retention period expires must exist. The process must cover: • Media types where information assets are stored • Required controls for the deletion of information assets depending on the classification. *Examples of media types: backup media, internal storage media and external storage media, such as USB sticks.*
04.14	Information assets must be deleted in accordance with the defined secure deletion process.

2.4.3 FILE TRANSFER

Req ID	Requirement
04.15	File transfers must be specifically agreed between the exchanging parties. The agreement must specify the relevant security requirements and the tools and procedures to be used.
04.16	File transfers must: • Use approved secure communication protocols • Enforce approved encryption • For, at least, confidential and strictly confidential information assets occur only upon secure authentication of the sender and receiver in server-to-server transfer. *Examples of secure communication protocols: SFTP, SCP.*

2.4.4 ENCRYPTION

Req ID	Requirement
04.17	Cryptographic technologies must implement strong and industry-accepted algorithms, not proprietary ones.

Req ID	Requirement
04.18	The asymmetric and symmetric keys and cryptographic hashing algorithms used must be recommended by NIST or an equivalent standard-setting organization.
04.19	Obsolete, deprecated or insecure algorithms must not be used.

2.4.5 KEY MANAGEMENT

Req ID	Requirement
04.20	Key management procedures must be developed, documented and implemented for the entire key lifecycle, including key compromise and destruction.
04.21	Implemented cryptographic controls must be documented and kept up to date. The documentation must: • Detail the used encryption algorithms and protocols • Detail the encryption keys and their usage • Contain an inventory of HSMs and other Secure Cryptographic Devices used for key management.
04.22	Cryptographic keys must be managed by dedicated and competent teams (Key Managers and Key Custodians).
04.23	Teams managing cryptographic keys must be adequately trained and have formally accepted their roles.
04.24	Cleartext cryptographic keys must be managed under dual control and split knowledge throughout their lifecycle.
04.25	Cryptographic keys must be strongly protected against disclosure and misuse.
04.26	Cryptographic keys must be uniquely identified by a name.
04.27	Each cryptographic key must be limited to only its intended function.
04.28	Cryptographic keys must not be shared between production and non-production environments.
04.29	Every cryptographic key ceremony must be supervised and logged.
04.30	Cryptographic key sizes must be within the ranges approved by the corresponding NIST publications or an equivalent standard-setting organization.
04.31	Cryptographic keys and certificates must be renewed regularly according to their rotation period and before of their expiration. **This requirement is a best practice until 17 January 2025, after which it will be required.** **Until 17 January 2025, the mandatory requirement is the following:** Cryptographic keys must be renewed regularly according to their rotation period.

Req ID	Requirement
04.32	An inventory of trusted keys, certificates and certificate storing devices for at least IT assets supporting critical or important services shall be maintained and kept updated. **This requirement is a best practice until 17 January 2025, after which it will be required.**

2.4.6 HSM

Req ID	Requirement
04.33	Procedures for Secure Cryptographic Device lifecycle must be maintained.
04.34	Secure Cryptographic Devices must be managed by dedicated and competent teams (Key Managers and Key Custodians).
04.35	Teams managing Secure Cryptographic Devices must be adequately trained and have formally accepted their roles.
04.36	Secure Cryptographic Devices must be managed under dual control and split knowledge throughout their lifecycle.
04.37	Secure Cryptographic Devices must be certified against industry standards to perform the specific activities.
04.38	Serial numbers for Secure Cryptographic Devices must be transmitted over an out-of-band channel and cross-checked prior to commissioning the devices.
04.39	Secure Cryptographic Devices must be properly configured to allow minimal necessary functionality before being put into production.
04.40	Secure Cryptographic Devices must be decommissioned, and their memory properly erased before being returned.

2.4.7 TEST DATA

Req ID	Requirement
04.41	Production data must not be used for testing purposes. *Test data can be created by:* • *Obfuscating production data* • *Creation of test data by obfuscating confidential and strictly confidential information and PII requires a valid business justification and for PII a consent from the data subjects* • *Generating artificially* • *Acquiring test data from customers or Third Parties* *Data obfuscation, i.e. data masking, is the act of anonymization, pseudonymization, scrubbing, or de-identification.* *Obfuscation techniques: encryption, tokenization, scrambling, nulling out or deletion, value variance, substitution, shuffling, redaction.* ***Note**: In PCI DSS terminology "masking" refers to a method of concealing a segment of data when displayed or printed and relates to protection of PAN, used when there is no business requirement to view the entire PAN.*
04.42	Security controls protecting test data must ensure the required level of protection of the information assets in question.

2.4.8 MEDIA HANDLING

Req ID	Requirement
04.43	Electronic and non-electronic media must be appropriately and securely handled throughout their lifecycle in accordance with the need of protection and classification level of the information assets stored on the media.
04.44	Non-public information on removable storage media must be encrypted.

2.5 ENDPOINT SECURITY

Applicability:

Endpoint Security requirements apply to all Nexi Group Companies and cover workstations and mobile devices accessing Group's information and IT assets as well as the anti-malware, other security mechanisms and software installed or used in the workstations and mobile devices.

2.5.1 WORKSTATION SECURITY

Req ID	Requirement
05.01	A registry of workstations must be maintained.
05.02	Only managed workstations may be granted direct access to Group's internal network.
05.03	Workstation configuration standards must be documented in accordance with applicable security requirements.
05.04	Changes to the workstation configuration standards must be reviewed, approved and documented.
05.05	Workstations must be configured and maintained in compliance with the documented configuration standards.
05.06	The workstations' operating system settings must be configured according to the hardening standards.
05.07	Access to O365 desktop and collaboration applications and tools must only be allowed from corporate managed workstations.
05.08	Workstations must apply appropriate user authentication mechanisms. *Examples of user authentication mechanisms: username/password, PIN code, biometrics.*
05.09	Workstations must be kept up to date with the latest software updates and security patches. *Where possible, critical and security patches must be technically enforced with no delay.*
05.10	The local disk of the workstations must be encrypted.
05.11	Granting local administrator privileges to workstations must require an explicit approval based on justified business needs. Standard users must not have administrative privileges on the workstations.
05.12	A registry of users with administrative privileges to workstations must be maintained, including business justification for privileged access.
05.13	The use of external storage devices from workstations must be disabled by default.
05.14	Workstations and related storage media must be securely wiped when decommissioned or re-assigned.
05.15	Workstations must be inspected regularly and detected unauthorized, unlicensed, illegal or obsolete software must be reported and addressed.

Req ID	Requirement
05.16	The following corporate security tools must be deployed and run continuously on workstations: • Antivirus • EDR (Endpoint Detection and Response) • DLP (Data Loss Prevention) • DRM (Digital Rights Management) • DNS security client.
05.17	Each corporate endpoint security control and tool must have a documented, enforced and maintained policy. *Examples: A conditional access policy for O365 desktop and collaboration applications and tools; Web Access policy (proxy); DLP policy.*

2.5.2 MOBILE DEVICE SECURITY

Req ID	Requirement
05.18	A registry of mobile devices accessing Group information or IT assets must be maintained.
05.19	Mobile devices that access Group information or IT assets must be controlled through a properly configured corporate Mobile Device Management (MDM) solution, which enforces baseline security requirements and at least: • Device encryption • Automatic locking • User authentication mechanism with PIN code, username/password or biometrics • SIM PIN, that is separate from device PIN • Separation of corporate information from users' personal information into partitions • Application whitelist from corporate marketplace on work partition • Remote wiping of corporate information. *Corporate information will be wiped in case of theft, loss or other security compromise.*
05.20	Only mobile devices managed by corporate MDM solution may be granted access to Group's information and IT assets.
05.21	Mobile devices must be kept up to date with the latest software updates and security patches. *Where possible, critical and security patches must be technically enforced with no delay.*
05.22	Mobile Device Management solution must perform regular scans and report on compliance with baseline security requirements.
05.23	Access to O365 desktop and collaboration applications and tools must only be allowed from corporate managed mobile devices.
05.24	Mobile devices and related storage media must be securely wiped when decommissioned or re-assigned.

2.5.3 ANTI-MALWARE

Req ID	Requirement
05.25	Workstation management must include an approved anti-malware solution.
05.26	The deployed anti-malware solution must be properly configured and kept up to date with the latest signatures and definitions.
05.27	Anti-malware solutions must perform periodic scans and logs from scans must be retained.
05.28	Anti-malware solutions must run continuously and be protected from unauthorized disabling or alteration.

2.5.4 DATA LOSS PREVENTION

Req ID	Requirement
05.29	Workstations and mobile devices must have a Data Loss Prevention solution implemented.
05.30	The Data Loss Prevention solution must be able to identify defined types of information assets.
05.31	The Data Loss Prevention solution must have the capability to control attempted functionality based on the identified information asset type.

2.5.5 SOFTWARE SECURITY

Req ID	Requirement
05.32	A procedure to request, assess and approve software must be established, documented and maintained.
05.33	A list of approved software must exist and be maintained.
05.34	Software installation activities must be controlled and restricted to authorized users.
05.35	Only approved software may be installed to workstations.

2.5.6 E-MAIL SECURITY

Req ID	Requirement
05.36	All incoming and outgoing e-mails must be systematically scanned for malware.
05.37	E-mails from external domains must be clearly marked.
05.38	Anti-spam mechanisms to detect and block spam e-mails must be in place.
05.39	Mechanism to report phishing/spam e-mails must exist.
05.40	E-mails must only be sent from approved domains.

2.5.7 WEB PROXY

Req ID	Requirement
05.41	Outbound connections to untrusted networks must be explicitly authorized and monitored.
05.42	Outbound connections from corporate managed end-user devices towards untrusted networks must be filtered, monitored and inspected for malware.
05.43	Rules restricting access to prohibited websites must be enforced, and automated tools controlling network traffic to and from the Internet must be used. *Examples of prohibited websites: websites with offensive or inappropriate content, webmail, unapproved remote storage services.*

2.6 IDENTITY AND ACCESS MANAGEMENT

Applicability:

Identity and Access Management requirements apply to all Nexi Group Companies and cover logical access to Group's information assets and IT resources.

Contractors' and Third Parties' access permissions must be restricted to the information and activities required to fulfil their contractual obligations.

2.6.1 GENERAL PRINCIPLES

Req ID	Requirement
06.01	Identity and Access Management processes must be established, documented and implemented. The processes must cover the entire identity and user account lifecycles. *The process covers all accounts: standard and privileged user accounts, service accounts, shared and emergency accounts.*
06.02	Access management process must be implemented using access management mechanisms, that address the principles of identification, authentication, authorization, accountability and management of credentials. The process must also include controls for monitoring anomalies.

2.6.2 IDENTIFICATION

Req ID	Requirement
06.03	A unique identity must be assigned to each user who requires access to information, information systems, applications or IT infrastructure components.
06.04	An inventory of all the identities must be developed and kept current. **This requirement is a best practice until 17 January 2025, after which it will be required.**
06.05	Each user account and service account must be assigned to an employee accountable for the account. *Service accounts are assigned to the nominated owner of the information system, application, IT asset.*
06.06	Each user must be assigned a standard user account in information systems and applications.
06.07	User accounts with a known expiry date must be set to expire automatically on that date.
06.08	Standard and privileged user accounts must be disabled or deleted after no more than ninety (90) days of inactivity.
06.09	All user accounts and related access privileges must be reviewed and validated as follows: • Where changes are necessary • At least once a year for all Information systems • At least every six months for Information systems supporting critical or important

Req ID	Requirement
	functions **This requirement is a best practice until 17 January 2025, after which it will be required.** **Until 17 January 2025, the mandatory requirement is the following:** Access permissions must be reviewed and validated at least once a year.
06.10	Privileged access must be restricted to dedicated privileged user accounts. Users with privileged user accounts must use their standard user account for day-to-day operations that do not require elevated privileges.
06.11	There must be a valid business reason to create emergency user accounts. Emergency user accounts must be deactivated as soon as the emergency has been resolved.
06.12	Service accounts: • Must be used only for interaction between IT resources • Must be set to prohibit interactive logon. Service account passwords can be set to “never expire”.
06.13	Default accounts must be disabled or deleted after installing and configuring information systems and applications or, if this is not possible, the account must be renamed, and the password changed.
06.14	Default accounts must not be used to perform any operational activities.
06.15	The use of shared accounts must be prohibited.

2.6.3 AUTHENTICATION

Req ID	Requirement
06.16	Multi-Factor Authentication must be enforced in the following cases: • Privileged access • Remote access • Applications exposed on Internet • IT assets supporting critical or important function. *It is recommended to enable Multi-Factor Authentication for all the other cases.* **This requirement is a best practice until 17 January 2025, after which it will be required.** **Until 17 January 2025, the mandatory requirement is the following:** Multi-Factor Authentication must be enforced in the following cases: • Privileged access • Remote access. *It is recommended to enable Multi-Factor Authentication for all the other cases.*
06.17	Privileged access must be controlled using Multi-Factor Authentication methods through Privileged Access Management (PAM) solutions. *Examples of activities requiring elevated privileges: administration, monitoring, development* *Includes privileged access to databases.*
06.18	Authentication credentials must be assigned to an individual user. *Examples of authentication credentials: access tokens, passwords, keys, digital certificates, biometrics.*
06.19	Authentication credentials must be properly protected at rest, in use and in transit.
06.20	Authentication credentials at rest must be encrypted or hashed.
06.21	Authentication credentials must not be hardcoded. *In, for example, login scripts, software code or executable program files.*
06.22	Authentication credentials in transit must be encrypted and transmitted using secure communication protocols.
06.23	Authentication credentials, when distributed, must be sent separately from the User ID with which they are associated.
06.24	In the event of a failed login attempt, the error message must not indicate what part of the identification or authentication procedure has failed.

Req ID	Requirement
06.25	User accounts must be locked after five (5) consecutive failed login attempts for at least thirty (30) minutes or until reset by administrators. User accounts may only be unlocked after the user has been successfully verified.
06.26	Accounts must be deactivated immediately if there is any suspicion that the authentication credentials have been compromised.
06.27	User sessions must be locked after fifteen (15) minutes or less of inactivity and the user must be required to re-authenticate to reactivate the terminal or session.
06.28	The maximum session lifetime after which the user must re-authenticate the terminal or session must be defined.

2.6.4 PASSWORD MANAGEMENT

Req ID	Requirement
06.29	All passwords must comply with the Group Password Policy.
06.30	The implemented password management system must: • Allow users to select their own passwords • Set a limit on how many times a user is allowed to change their password in a twenty-four (24) hour period • Enforce the Group Password Policy or more stringent rules • Not display plaintext passwords on screen as default when they are entered or in logs • Maintain a record of previous six (6) passwords.
06.31	Initial and temporary passwords generated by a person or process other than the user to which they are assigned must be: • Random and secure in accordance with the Group Password Policy • Unique to each user • Set to expire upon the first/next user login forcing the user to create a new password • Set to automatically expire twenty-four (24) hours after their distribution.
06.32	Password reset mechanism must be implemented and provide a new temporary password upon request. *In cases of e.g. forgotten or compromised password.*
06.33	Whenever a password reset is requested, the user's identity must be verified prior to resetting and providing a temporary password.
06.34	Users must be able to change their passwords on information systems and applications through secure protocols.
06.35	The password change function must: • Include entry of the current password followed by the entry of the new password twice. Both entries of the new password must match to successfully complete the password change. • Verify the password strength in accordance with the configured password requirements before accepting the change.

2.6.5 AUTHORIZATION

Req ID	Requirement
06.36	Access to information, information systems and applications must be prohibited by default unless specifically authorized and in compliance with the Group Information Classification scheme.
06.37	Access permissions must be assigned following the principle of “least privileges”. *Applies to all access permissions, including privileged access.*
06.38	Access permissions must be assigned following the principle of “need-to-know”, “need to use” and be based on the specific job responsibilities, roles and valid business needs. **This requirement is a best practice until 17 January 2025, after which it will be required.** **Until 17 January 2025, the mandatory requirement is the following:** Access permissions must be assigned following the principle of “need-to-know” and be based on the specific job responsibilities, roles and valid business needs.
06.39	Assignment of access permission must ensure effective segregation of duties.

2.7 NETWORK AND COMMUNICATIONS SECURITY

Applicability:

Network and Communication Security requirements apply to all Nexi Group Companies and cover networks managed by the Group’s and communications to untrusted and external networks.

2.7.1 ARCHITECTURE

Req ID	Requirement
07.01	Network architecture must be designed to ensure high availability and resilience in alignment with network architecture security principles (withstanding current and predicted loads, including malicious attack traffic). *Examples of high-availability: e.g. fail-secure systems, disaster recovery procedures.* *Examples of related principles: “defense in depth”, “secure by default”, “secure by design”.*
07.02	Network configuration standards and baselines must be defined and documented in accordance with applicable security requirements. *Examples of applicable security requirements: Group Security Framework requirements, device vendor guidelines, applicable business, customer and regulatory requirements as well as industry accepted hardening standards.*

Req ID	Requirement
07.03	Networks and network devices must be configured and maintained in compliance with the relevant documented configuration standards and baselines, enabling only the required services and changing the vendor default settings.
07.04	Network device configurations must be documented with a clear description of the associated business purpose and must be reviewed regularly.
07.05	Information systems and network devices must use private IP addresses.
07.06	Network devices must be configured not to disclose private IP addresses or routing information to unauthorized parties and networks. Network Address Translation (NAT) must be utilized to prevent propagation of proprietary routing information.
07.07	Information systems must be configured so that network bridging is not possible.
07.08	Direct inbound and outbound connections between the Internet and internal networks must be prohibited. Also, unauthorized outbound traffic from internal networks to the Internet must not be permitted. *Proxy is the approved method for outbound traffic as long as the internal resource is always authenticated.*
07.09	The use of insecure protocols must be prohibited. *Examples of **secure** protocols: SSH, SFTP, HTTPS, TLS 1.2 or newer, IPSec.* *Examples of **insecure** protocols: Telnet, FTP, TFTP, HTTP, SLS 3.0, TLS 1.1 or lower.*
07.10	Network infrastructure and systems must be protected from internal and external unauthorized access and actions through the definition of appropriate perimeter security measures concerning both the wired and wireless network. *Examples of network perimeter security measures: firewall, IDS/IPS, WAF.*
07.11	Network Intrusion Detection and Prevention (NIDPS) must be deployed at the perimeter of all networks where critical components are placed. *Examples of critical components: VLANs with confidential or strictly confidential information assets, infrastructure or security tools, user networks.*
07.12	Network connections and data-flow diagrams across systems and networks must be defined, documented updated upon changes to the environment. **This requirement is a best practice until 17 January 2025, after which it will be required.**
07.13	A separate and dedicated network must be exclusively used for administration of IT assets. **This requirement is a best practice until 17 January 2025, after which it will be required.**

2.7.2 SEGREGATION

Req ID	Requirement
07.14	Network architecture must provide segmentation between network zones with different risk levels, purposes, classification of the information and regulatory requirement zones. Segregation must include, but is not limited to, segregation of: • Environments hosting production data from environments hosting test data • Voice and video services from data services • Physical security device network from other networks. *Examples of physical security devices: IP-cameras, badge-readers, IR/glass-break sensors, revolving door -systems.*
07.15	Unmanaged devices may only be connected to dedicated guest networks. *Examples of guest networks: On-site LAN & WLAN access.*
07.16	System components that expose services to untrusted networks must be placed in a DMZ network.
07.17	Inbound traffic from untrusted networks must be limited to specifically allowed connections within the DMZ.
07.18	Measures to temporarily isolate, where necessary, subnetworks and network components and devices must be implemented. **This requirement is a best practice until 17 January 2025, after which it will be required.**

2.7.3 MANAGEMENT

Req ID	Requirement
07.19	Network devices and firewalls must be managed by designated teams with defined roles and responsibilities and dedicated accounts.
07.20	An inventory of network devices must be developed and kept current.
07.21	The network architecture must be described in network and connectivity diagrams that are kept up to date.
07.22	An inventory of network device subnets and IP allocation must be developed and kept current.
07.23	The classification level of networks must be assigned based on the classification level of the applications, services and information processed in the network.
07.24	External connections must be listed, and the document must contain a business justification, setup, protocols used and any additional security controls of each connection.

Req ID	Requirement
07.25	A list of services, protocols and ports used in the network devices must be created, maintained and kept up to date. The list must, at least, contain the following: • Business justification for each • Approval for the use of each • Documentation of security features implemented for used services and protocols considered to be insecure.
07.26	Tools that can affect the availability of information systems or capture and disclose sensitive information must be prohibited unless explicitly approved. *For example, network and security tools used for port scanning, reconnaissance and/or packet inspection.*

2.7.4 FIREWALL

Req ID	Requirement
07.27	Firewalls must be configured to deny all packets unless explicitly allowed.
07.28	Firewalls must be placed to control access between different network zones based on the network architecture.
07.29	A procedure to request, assess and approve firewall requests must be established, documented and maintained.
07.30	Firewall requests must have a valid business justification and be approved and documented.
07.31	Firewall request and implementation procedures must enforce segregation of duties.
07.32	Firewall rulesets must be kept current and reviewed bi-annually to identify obsolete or insecure permissions. The result of the review must be documented.

2.7.5 ACCESS

Req ID	Requirement
07.33	Access to internal and external network services must be strictly controlled and monitored.
07.34	All user access to Group IT environments must be implemented to go through dedicated secure access infrastructure. The secure access infrastructure in production environment must be separate from the non-production environments' infrastructure. *Examples of secure access infrastructure: Jump Host, VDI, PAM.*
07.35	Direct access from workstations and VPN networks to production environments must be prohibited.
07.36	Access from unmanaged devices must go through VDI.
07.37	Non-console administrative access to network devices must be limited to corporate managed workstations.
07.38	Non-console administrative access must be encrypted using strong cryptography and use Multi-Factor Authentication.

Req ID	Requirement
07.39	Network zones containing database servers must be unreachable from Internet and untrusted networks.
07.40	Users must not have direct access to databases, but only through authorized application software.

2.7.6 WIRELESS NETWORK

Req ID	Requirement
07.41	An inventory of authorized wireless networks and access points, including a documented business justification for each wireless network, must be maintained.
07.42	Access to wireless network must require authentication and utilize secure protocols and strong cryptography.
07.43	Wireless guest networks must provide access to a limited number of resources and for a limited time. Access to internal resources from a wireless guest network must be granted once the user has established a VPN connection.
07.44	Vendor defaults must be changed for wireless environments connected to corporate networks, in particular: • Encryption keys should be changed at installation and whenever anyone with knowledge of the keys leaves the Group or changes position • Default SNMP community strings should be changed • Default passwords / passphrases on access points should be changed • Firmware on wireless devices should be updated to support strong encryption for authentication and transmission.

2.7.7 REMOTE ACCESS

Req ID	Requirement
07.45	Remote access connections must be protected with secure protocols and strong cryptography.
07.46	Remote access connections from untrusted networks must be authenticated using Multi-Factor Authentication.
07.47	Direct remote access to corporate network must be prohibited. *Must go through e.g. Jump Host or VDI.*
07.48	Remote access connections from Third Parties must have a valid business justification and be explicitly authorized before access is granted.
07.49	Remote access connections from Third Parties must be disabled by default and only enabled when needed.
07.50	Remote end-user device access connections must use VPN.
07.51	VPNs designed for remote end-user device access must utilize connectivity timeouts with mandatory re-authentication after ten (10) hours.

Req ID	Requirement
07.52	Split tunneling must be prohibited when remotely connected to Group network.
07.53	Remote access must provide users the same access rights as on-site.
07.54	Remote access to plaintext cryptographic keys or key components and shares must be prohibited.
07.55	Only one concurrent remote session per user can be allowed.

2.8 PERSONNEL SECURITY

Applicability:

Personnel Security requirements apply to all Nexi Group Companies and cover all personnel, including temporary and part-time employees.

2.8.1 RECRUITMENT

Req ID	Requirement
08.01	Background checks on employee candidates must be performed prior to employment in compliance with local laws and regulations. *Criminal background checks should be conducted on employee candidates for positions where a certificate of a clear criminal record is required.*
08.02	Employee candidates must accept the terms and conditions of employment in writing, including a non-disclosure agreement and the End User Security Code of Conduct.
08.03	The security-related obligations of employees must be explicitly defined in job descriptions and contracts. *Examples of security related obligations: cryptographic key management responsibilities, specific security responsibilities of a database administrator.*
08.04	Prior to employment, employees must be introduced to the Group's security requirements and their acknowledgement of the Security Framework must be recorded.
08.05	Prior to employment, employees must acknowledge the need to protect Group's information assets and to perform their daily job responsibilities in compliance with the Security Framework.
08.06	Prior to employment, employees must confirm that they understand their security obligations and roles, including the terms of the non-disclosure agreement, remain valid after their employment.
08.07	Employees must receive introductory training that provides them with the knowledge and skills needed to meet the expected security behavior within two weeks of starting employment.

2.8.2 DURING EMPLOYMENT

Req ID	Requirement
08.08	Employees must annually acknowledge that they have read and understood the Security Policy and End User Security Code of Conduct.
08.09	A security awareness program must exist. The program must include an annual security awareness plan defining the communication channels, target audiences and the recurrence of specific trainings throughout the year. *The security awareness plan must include annual training for specified roles, such as secure coding techniques training for developers.*

Req ID	Requirement
08.10	Employees must receive annual security awareness training.
08.11	Employees must receive security training relevant to their roles and responsibilities periodically.
08.12	Non-compliance with the Security Framework must be investigated, and disciplinary actions taken against an employee who attempted or committed a security breach in accordance with local laws, regulations and personnel policies.
08.13	A procedure to track changes on employee's position, job description and assigned privileges must exist.

2.8.3 TERMINATION

Req ID	Requirement
08.14	Upon change or termination of employment, logical and physical access must be revoked. The revocation of access must be recorded.
08.15	Upon change or termination of employment, Group's information assets and equipment no longer needed, including mobile devices, tokens and similar, must be returned. The action must be recorded.

2.9 PHYSICAL SECURITY

Applicability:

Physical Security requirements apply to all Nexi Group Companies and cover all premises where Nexi Group has operations.

2.9.1 SECURITY OF PREMISES

Req ID	Requirement
09.01	Controlled, protected and secure areas on Group's premises must be defined and documented based on the evaluated risks related to: • Criticality and sensitivity of the assets hosted in the area • Criticality and requirements of the business operations performed in the area • Physical and environmental threats of the location. *Examples of threats: sabotage (physical threat), flood or fire (environmental threats).*
09.02	Information assets and IT equipment must be protected within and outside Group's premises against unauthorized access, tampering, theft, damage, and operational disruption with the use of appropriate physical security measures. *Examples of physical security measures: video surveillance, physical access control mechanisms, mantrap.* **This requirement is a best practice until 17 January 2025, after which it will be required.** **Until 17 January 2025, the mandatory requirement is the following:** Information assets and IT equipment must be protected against unauthorized access, tampering, theft, damage, and operational disruption with the use of appropriate physical security measures. *Examples of physical security measures: video surveillance, physical access control mechanisms, mantrap.*
09.03	Physical security measures and safeguards to protect the premises must be implemented based on the protection needs of the defined areas residing in the premises. *Perimeter security controls aim to:* • *Prevent (e.g. security guards, patrols, barriers)* • *Detect (e.g. security cameras, alarm systems, motion sensors) and* • *Deter (e.g. audible alerts) possible invasion attempts.*
09.04	Physical security measures and safeguards must be maintained at the same level in all Group premises that may host production data, whether active or inactive. **This requirement is a best practice until 17 January 2025, after which it will be required.**

Req ID	Requirement
09.05	The implemented physical security measures and safeguards of premises must be documented, reviewed and, if needed, adjusted.
09.06	The implemented physical security measures and safeguards must not affect the safety and emergency measures in any way.
09.07	The implemented physical security measures and safeguards must be tested regularly. The conducted tests and test results must be documented.
09.08	Entry to protected and secure areas must be strictly controlled, monitored taking in account the criticality of the area and restricted to authorized parties through physical access control and surveillance mechanisms. *Examples of physical access controls and surveillance mechanisms:* • *Physical barriers* • *Manned reception areas* • *Security cameras* • *Card or PIN-based authentication systems.* **This requirement is a best practice until 17 January 2025, after which it will be required.** **Until 17 January 2025, the mandatory requirement is the following:** Entry to protected and secure areas must be strictly controlled, monitored and restricted to authorized parties through physical access control and surveillance mechanisms. *Examples of physical access controls and surveillance mechanisms:* • *Physical barriers* • *Manned reception areas* • *Security cameras* • *Card or PIN-based authentication systems.*
09.09	Physical access to protected and secure areas must only be granted to authorized and trusted employees, contractors and other parties based on legitimate business needs after approval.
09.10	Physical access to protected and secure areas must be granted in accordance with the principle of least privilege, “need-to-know” or on an ad-hoc basis and revoked immediately when it is no longer needed. **This requirement is a best practice until 17 January 2025, after which it will be required.** **Until 17 January 2025, the mandatory requirement is the following:** Physical access to protected and secure areas must be granted in accordance with the principle of least privilege and revoked immediately when it is no longer needed.

Req ID	Requirement
09.11	Physical access logs must be monitored regularly and retained for at least three months, unless otherwise restricted by local law.
09.12	Physical access rights to secure areas must be reviewed regularly and updated; identified unnecessary access rights must be revoked immediately.
09.13	Secure areas must have security personnel available 24/7 within agreed response time based on the risk assessment of the premises.
09.14	Delivery and loading areas must be physically isolated from protected and secure areas and monitored.

2.9.2 ENVIRONMENTAL SECURITY

Req ID	Requirement
09.15	Premises must comply with the local fire safety, anti-flooding, lightning protection and anti-seismic standards. The susceptibility to natural disasters and accessibility to emergency authorities must be taken into consideration.
09.16	Premises must be equipped with environmental security mechanisms based on the availability and continuity requirements of the hosted information and performed business operations.
09.17	Environmental conditions in secure areas must be monitored continuously using sensors that send alerts when secure operational thresholds are exceeded.
09.18	Critical IT equipment must be protected against damage and operational disruption with the use of environmental security measures. *Examples of environmental security measures:* *To protect from power supply failures and fluctuations* • *Uninterruptible Power Supply (UPS)* • *Backup electricity generator.* *To protect from fire, heat and water damage* • *Smoke and water sensors connected to a central alarm system monitored in the local operation center or remotely* • *Fire suppression system* • *Cooling equipment with sufficient capacity* • *Temperature and humidity measuring equipment.*
09.19	Emergency and supporting equipment must be serviced regularly according to manufacturers' specifications.
09.20	Primary and backup infrastructure must be tested regularly to verify their normal operation. The conducted tests and results must be documented.
09.21	Internal cabling and network components must be structured, labelled and protected from interception, interference and damage. *Examples of internal cabling: power, telecommunication.*

2.9.3 EMPLOYEE AND VISITORS ACCESS

Req ID	Requirement
09.22	Keys and access cards that have not been issued to employees, contractors or other authorized parties must be stored securely.
09.23	Keys and access cards issued to employees, contractors and other authorized parties must be registered and returned when they are no longer needed.
09.24	Employees and contractors and other authorized parties must wear a Group issued ID or access cards visible at Group premises.
09.25	The ID and access cards issued to fixed term employees or contractors must be set to expire at the end of the contract.
09.26	Visitors must be identified and registered before entering the premises.
09.27	There must be a valid Group business reason for a visitor to enter the premises.
09.28	Visitors must wear a dated visitor badge that clearly distinguishes them from onsite personnel when visiting the premises.
09.29	Visitors must be escorted by an employee or an authorized Third Party.
09.30	Visitors in secure areas must at all times be under the supervision of an employee who is authorized to access the secure area.

2.10 SECURITY GOVERNANCE AND BY DESIGN

Applicability:

Security Governance requirements apply to all Nexi Group Companies.

2.10.1 SECURITY FRAMEWORK

Req ID	Requirement
10.01	The Group must establish, operate, maintain and continuously improve a Security Framework that includes: • Security governance roles and responsibilities • Security governance processes and procedures • Minimum security requirements • Performance evaluation measurement.
10.02	The Group Security Framework must be implemented in Group companies. If local versions of internal security regulations or a local security framework are needed to address company-specific security, business, and compliance requirements, they must be in alignment with the Group Security Framework.
10.03	Security roles and responsibilities must be clearly defined, communicated, and properly allocated within the Group.
10.04	Security requirements must be kept relevant and updated, and they must reflect statutory, regulatory, contractual and business requirements at Group and local level.
10.05	Local security requirements that exceed or fall below the Group security baseline must be identified and documented at the local level.
10.06	The Security Framework and any additional security requirements must be communicated to and acknowledged by employees, contractors and other Third Parties who have access to Group information assets.
10.07	The selection, prioritization and implementation of security measures must be based on the identification, analysis and treatment of security risks to which information assets are exposed throughout their lifecycle.

2.10.2 SECURITY PERFORMANCE MEASUREMENT

Req ID	Requirement
10.08	Security processes, measures and objectives must be established and documented to measure, monitor, and evaluate their effectiveness, performance and compliance through appropriate and meaningful metrics.
10.09	Group Top Management must review the Group Security Framework regularly to: • Assess its suitability, adequacy, effectiveness, and performance • Evaluate changes in the Group's internal and external environment to ensure their appropriate incorporation into the Security Framework • Ensure sufficient resources are available for its operation, maintenance, and continuous improvement.

Req ID	Requirement
10.10	The overall Group compliance with the Group Security Policy must be monitored and reported to Group Top Management.
10.11	Local compliance of the Group companies with the Group Security Policy and local adaptation of the Group Security Framework must be monitored and reported on regularly.
10.12	Compliance with the Group Security Framework in Group Companies must be assessed regularly by independent audits, reviews or gap assessments. *Examples of independent auditors and reviewers: Internal Audit function, external auditors, regulators, and other supervisory bodies.*
10.13	Records showing compliance with the Group Security Framework and any additional security requirements must be generated, stored for validation and audit, and retained. Record retention time must adhere to applicable statutory, regulatory, contractual and business requirements.

2.10.3 SECURITY BY DESIGN & SDLC

Req ID	Requirement
10.14	The Security by Design process must be established, documented and implemented.
10.15	The Security by Design process must be initiated, prior to any new project, pilot initiatives product development and new major change. In case of Gen AI pilot initiatives, an additional Security Preliminary Assessment must be carried out to identify and evaluate relevant security risks.
10.16	The broader System Development Lifecycle (SDLC) process must be established, documented, implemented and it must: • Incorporate information security throughout the system development lifecycle • Include the initial identification of security requirements in the analysis phase (e.g. Security by Design checklist) • Address the identified security requirements in the application development and subsequent phases • Be based on industry standards and best practices. Examples of industry standards and best practices: OWASP, SANS Foundation guidelines, PCI Secure Software Standard (SSF), PCI Secure Software Lifecycle (SLC).

2.10.4 SEGREGATION OF DUTIES

Req ID	Requirement
10.17	To the extent possible and considering the protection needs, conflicting duties and areas of responsibility must be segregated or other countermeasures to reduce the risk of unauthorized and unintentional modification or misuse of corporate information assets must be implemented. *When to and who should address potential conflicting duties and areas or responsibility:* • *Introducing new or developing existing critical processes, services and systems, including duties, responsibilities and workflows across processes, services and systems – Process Owners, Application Owners, Service Owners* • *Defining roles and their responsibilities – Process Owners and Service Owners* • *Assigning new or changing roles/responsibilities of an employee – Line Managers.*
10.18	The 4-eyes principle must be enforced to prevent errors, fraud, abuse, or unauthorized actions when modifying payment details or executing payments manually. Specifically: • Any manual transfer of funds or change to payment or account details (e.g., payment coordinates, recipient's name, IBAN, or other sensitive financial data) must be reviewed and approved by a different individual than the one initiating the request, before execution • Requests for manual changes to payment or account details must be independently verified through an external, trusted, and previously established channel, separate from the one used for the original request. For instance, by contacting the client, vendor, or merchant via a previously known and verified phone number or another secure communication method, before implementing any changes • All actions must be logged for review. As part of sound and prudent management, it is recommended that all departments regularly review access profiles for critical transactions, particularly following organizational changes.

2.11 SECURITY INCIDENT MANAGEMENT

Applicability:

Security Incident Management requirements apply to all Nexi Group Companies and cover potential security incidents involving Nexi Group's information assets and IT environments that can have a negative effect on the confidentiality, integrity or availability of Group's information assets or business operations. These requirements also apply to services provided by Third Parties.

2.11.1 GOVERNANCE

Req ID	Requirement
11.01	Security Incident Management function(s) must be established in the Group.
11.02	Group's Security Incident Management functions must consist of qualified individuals.
11.03	A Security Incident Response Plan (IRP) must be established and maintained. The plan must include at least: • Roles and responsibilities • Communication channels • Escalation paths • Classification requirements.
11.04	The Security Incident Response Plan (IRP) must cover the entire security incident lifecycle, including: • Detection/reporting • Investigation and analysis • Classification and assignment • Response and containment • Eradication, recovery and closure • Reporting, including defined reporting procedures for security incidents related to personal data under GDPR and cardholder data • Lessons learned and forensics.
11.05	The Security Incident Response Plan and process must be tested at least annually with the participation of all involved parties.

2.11.2 DETECTION

Req ID	Requirement
11.06	Suspected security breaches and incidents must be reported without undue delay. *Security incidents include security control failures and unauthorized wireless access points.*
11.07	Security event logging and detection tools must be used to timely detect and respond to security events and incidents.

2.11.3 HANDLING

Req ID	Requirement
11.08	Security incidents must be registered, classified based on their urgency and potential impact, and assigned for immediate handling in accordance with the security incident response plan and process.
11.09	Adequate and valid evidence of security incidents must be collected and retained to facilitate a possible forensic investigation. The integrity and authenticity of evidence must be preserved when accessed, used or transferred (i.e. chain of custody).
11.10	Security forensics must only be executed by authorized and skilled personnel supported by the Security Incident Management functions and in accordance with the documented process.
11.11	An internal post-incident review must be conducted for critical security incidents. The post-incident report must include the facts related to the incident, how the incident was solved, and lessons learned.

2.11.4 REPORTING

Req ID	Requirement
11.12	Security incidents must be communicated and escalated in accordance with the defined Security Incident Response Plan and process to ensure effective response and collaboration with relevant stakeholders.
11.13	The need to notify affected customers, payment schemes, other supervisory, regulatory and police authorities and other external parties must be assessed and, where required, appropriate procedures for cooperation initiated.

2.12 SECURITY TESTING AND VULNERABILITY MANAGEMENT

Applicability:

Security Testing and Vulnerability Management requirements apply to all Nexi Group Companies and cover information systems, applications and networks storing, transferring or processing information assets owned or governed by Nexi Group regardless of how they are hosted (in-house, outsourced, cloud).

2.12.1 GENERAL PRINCIPLES

Req ID	Requirement
12.01	Security testing must be performed on all information systems and IT infrastructure based on their criticality, assessed risks and contractual and regulatory requirements. *Information systems include systems, applications, IT infrastructure components, network components. Security testing includes vulnerability scans (incl. discovery), penetration testing, wireless scans, code reviews, specific LLM tests for Gen AI Tools and Threat-Led Penetration Testing.* **This requirement is a best practice until 17 January 2025, after which it will be required.** **Until 17 January 2025, the mandatory requirement is the following:** Security testing must be performed on all information systems and IT infrastructure based on their criticality, assessed risks and contractual and regulatory requirements. *Information systems include systems, applications, IT infrastructure components, network components.* *Security testing includes vulnerability scans (incl. discovery), penetration testing, wireless scans, code reviews and red teaming.*
12.02	Security testing methods must be kept up to date and incorporate scenarios of relevant and known potential attacks based on the security threats observed and the changes made to information systems and IT environment.
12.03	Security testing must be performed by an independent and qualified, internal or external, assessor approved by the Group, utilizing regulatory and industry frameworks. For example, Third Parties are not allowed to perform security testing without an explicit approval from the Group Security function.
12.04	Security testing plans must be created at least annually in accordance with business and regulatory requirements, be based on the criticality and risk profile of the information systems being tested and kept up to date. The security testing plans must include: • Type of security testing covered by the plan • Information systems in scope of the security testing • Frequency and schedule of regular security testing • Identified main stakeholders to be notified for information systems in scope.

Req ID	Requirement
12.05	The security testing planning must evaluate the need for including Threat-Led Penetration Testing (TLPT) in compliance with DORA regulation.
12.06	Security testing must be scheduled taking into consideration the continuity of business operations and production services. All relevant involved parties must be notified.
12.07	Security testing must be performed in accordance with the defined security testing processes for each type of security testing.
12.08	Security testing must be performed taking reasonable precautions to minimize adverse impact of information systems and business operations.
12.09	Security testing must produce a report that contains the following: • Scope of the conducted security testing • Detected vulnerabilities and their severity score • Recommended mitigation actions for each detected vulnerability.
12.10	Defined procedures for the disclosure of detected vulnerabilities to impacted stakeholders must exist. *Examples of impacted stakeholders: national authorities, Third Parties and customers based on contractual obligations.*
12.11	Security testing must be performed on new information systems and after significant changes on information systems already in use prior to deployment to production.
12.12	Relevant results of security testing must be considered for reporting to the Top Management of the Group and Group companies.

2.12.2 PENETRATION TESTING

Req ID	Requirement
12.13	The defined penetration testing process must: • Include application and infrastructure penetration testing • Include retesting after remediation of detected vulnerabilities • Identify the used testing methodologies • Comply with relevant regulatory standards.
12.14	The need for internal and external penetration testing must be evaluated and testing performed, if so evaluated, after any significant change to information systems or IT environment.
12.15	Internal penetration testing on information systems must be performed regularly.
12.16	External penetration testing on information systems must be performed regularly.

2.12.3 VULNERABILITY SCANNING

Req ID	Requirement
12.17	New information systems added to production must be included in the vulnerability scanning scope.
12.18	Vulnerability scans on information systems and IT infrastructure must be performed regularly.
12.19	Internal and external vulnerability scans must be performed after any significant changes.

2.12.4 APPLICATION SECURITY TESTING

Req ID	Requirement
12.20	Application-level penetration testing must be performed according to the Dynamic Application Security Testing (DAST) method.
12.21	Secure code review must be performed according to the Static Application Security Testing (SAST) method.
12.22	Application security assessments must be conducted on new applications and after significant changes prior to deployment to production.
12.23	Application security assessments must be conducted regularly according to the criticality, classification and characteristics of the application.

2.12.5 WIRELESS SCANNING

Req ID	Requirement
12.24	Scans to detect wireless connections to the information systems and wireless access points at the Group premises must be performed at least quarterly.
12.25	Unauthorized wireless access points must be treated as security incidents.

2.12.6 VULNERABILITY MANAGEMENT

Req ID	Requirement
12.26	Reputable sources for security vulnerability information must be used to identify new security vulnerabilities.
12.27	A defined vulnerability management process to classify, monitor, report and address detected security vulnerabilities must exist. *A remediation plan must be defined for each detected vulnerability.*
12.28	Relevant and trustworthy information resources must be identified and updated to build and maintain awareness about vulnerabilities. **This requirement is a best practice until 17 January 2025, after which it will be required.**

Req ID	Requirement
12.29	For the IT assets supporting critical or important services, automated vulnerability scanning and assessments shall be performed at least on a weekly basis. **This requirement is a best practice until 17 January 2025, after which it will be required.**
12.30	Detected security vulnerabilities must be classified in accordance with the defined vulnerability severity levels.
12.31	The addressing of detected vulnerabilities must be prioritized according to their severity level and the criticality of the information system.
12.32	Detected vulnerabilities must be addressed to achieve an acceptable risk level.
12.33	Detected critical and high vulnerabilities must be addressed prior to deploying new information systems or changes to production.

2.13 SYSTEM SECURITY

Applicability:

System Security requirements apply to all Nexi Group Companies and cover all Group's information systems.

2.13.1 IT ASSET MANAGEMENT

Req ID	Requirement
13.01	An inventory of IT assets used in production, development and testing of business services and supporting processes must be developed and kept up to date. The ownership, classification and location of the IT asset and links and interdependencies with other IT assets must be documented. *Example inventory: CMDB* *IT assets cover e.g. servers and network devices.*
13.02	IT assets must be assigned a business owner and an IT owner with clearly defined management responsibilities and authority.
13.03	Defined procedures for IT asset lifecycle must be established, documented and implemented.
13.04	IT assets must be classified based on the protection needs of the highest classified information asset processed or retained in the IT asset and the criticality of the performed operations.
13.05	Information assets must be securely sanitized from IT assets when the IT asset is decommissioned, reused or re-assigned.

2.13.2 OPERATION

Req ID	Requirement
13.06	Processes and procedures for the administration and operation of information systems must be documented. *Examples of administrative and operational processes and procedures: Change management, incident management, patch management, and other ITIL processes/operational procedures.*
13.07	Change and release management processes that cover the change lifecycle must be established and implemented. The processes must cover the change lifecycle and be in line with the leading industry practices. *Change lifecycle: request, impact/risk assessment, approval, planning, design, implementation, testing, rollout and back-out.*
13.08	Changes to information systems, operational environments and IT infrastructure must be controlled and managed by the defined change management process.
13.09	Changes in production environments must be sufficiently verified prior to releasing to production to avoid potential adverse impacts on business services, operations, and security.

Req ID	Requirement
13.10	The installation and upgrade of information systems, applications and software on operational environments must be controlled and restricted to authorized personnel.
13.11	Regular checks on operational environments to identify, report and address unauthorized, unlicensed, illegal or obsolete applications or software must be performed.
13.12	The incident management process must be integrated with the security incident management process.

2.13.3 CONFIGURATION

Req ID	Requirement
13.13	Baseline security configuration standards for information systems, applications and IT infrastructure components must be documented, approved and maintained. The baselines must comply with applicable security requirements and be based on industry-accepted hardening standards. *Examples of industry-accepted hardening standards: CIS, ISO, SANS Institute and NIST Cybersecurity Framework.*
13.14	Information systems, applications and IT infrastructure components must be configured and maintained in accordance with the approved configuration baselines.
13.15	The vendor's recommended settings should be considered when defining hardening rules. **This requirement is a best practice until 17 January 2025, after which it will be required.**
13.16	Production environments must be segregated from test and development environments to reduce the risk of unauthorized access and changes to information assets and IT resources.
13.17	Test and development environments must be secured according to the classification and required protection of the information assets processed in the application under development.

2.13.4 SOFTWARE SECURITY

Req ID	Requirement
13.18	A procedure to request, assess and approve software must be established, documented and maintained.
13.19	A list of approved software must exist and be maintained.

2.13.5 CYBER RESILIENCE

Req ID	Requirement
13.20	Redundancy of critical information resources must be properly set up to ensure resiliency on all levels and sustain business operations and service levels in accordance with SLAs, Business Continuity and Disaster Recovery Plans.

Req ID	Requirement
	Redundancy on, for example, premises, telecommunications, systems, information.
13.21	Security controls must be configured based on high availability requirements to avoid business or service disruptions.
13.22	Security controls must be maintained at the same level for all systems that may host production data, whether active or inactive.
13.23	Mechanisms to protect information assets from cyber security threats and incidents must be defined, documented, implemented and maintained to fulfil the required protection level. The defined protection mechanisms must contain preventive, detective, reactive and recovery methods.
13.24	Information systems must be protected by applicable and centralized anti-malware mechanisms.
13.25	The deployed anti-malware mechanisms must be properly configured and kept up to date with the latest signatures and definitions.
13.26	Anti-malware mechanisms must perform periodic scans and logs from scans must be retained.
13.27	Anti-malware mechanisms must run continuously and be protected from unauthorized disabling or alteration.
13.28	Change detection mechanisms must be deployed to alert to unauthorized modification of critical system, configuration or content files and perform critical file comparisons at least weekly. *Example of change detection mechanisms: file-integrity monitoring tool.*

2.13.6 PATCH MANAGEMENT

Req ID	Requirement
13.29	A patch management process to ensure that information systems, applications and IT infrastructure components are kept up to date with the latest security patches must be established and implemented. The process must include: • A mechanism to prioritize patches based on the information asset classification, patch type and criticality and available information on the attack surface • Actions to minimize negative effects on production environment • Documenting patch implementation.
13.30	Information systems, applications and IT infrastructure must be patched regularly in accordance with the defined patch management process.
13.31	Security patches must be installed based on their criticality and the classification of the system as well as the classification of the information contained in the system.
13.32	Mitigating actions (compensating controls) must be applied when a security patch cannot be installed promptly or a patch to a known vulnerability or risk is not yet available.

Req ID	Requirement
13.33	Secure Cryptographic Devices must be regularly updated to prevent obsolescence and ensure that it remains resilient against cyber threats. If the device becomes outdated, mitigation and monitoring measures must be adopted to maintain resilience against cyber threats. **This requirement is a best practice until 17 January 2025, after which it will be required.**

2.13.7 BACKUP

Req ID	Requirement
13.34	A defined process for backup and restore must exist and be tested at least once a year.
13.35	Backup schedules must be documented and determine the backup frequency and retention period taking into account the information classification, Recovery Point Objective (RPO), business and regulatory requirements.
13.36	Information systems, configuration files and system- and software images in production must be backed up according to a backup schedule and process. *Including network devices and their configuration files.*
13.37	Source code backups must be taken on a regular basis.
13.38	Backup media must be handled and protected based on the highest classification level and protection requirements of information contents. *For example, encryption is applied to the storage media in accordance with relevant regulatory requirements.*
13.39	Backup media must be securely stored at locations that are sufficiently remote from the primary site and protected against physical and environmental threats and unauthorized access.
13.40	Critical production system backups must be stored at an off-site facility, i.e. an alternate or disaster recovery site or a Group-approved commercial storage facility.
13.41	The restoration of backed up information must be tested at least once a year to validate the completeness, integrity, and availability of the information and the restorability of the backup. The test results must be documented.

2.13.8 TIME SYNCHRONIZATION

Req ID	Requirement
13.42	The time of information systems, applications and other IT infrastructure components must be synchronized with central time servers that receive time data from external industry-accepted time sources. *IT infrastructure components include network devices.*
13.43	Access to time data and settings must be limited to authorized individuals.

2.14 THIRD PARTY SECURITY

Applicability:

Third Party Security requirements apply to all Nexi Group Companies and cover all types of Third-Party engagements, including outsourcing and cloud services.

2.14.1 THIRD PARTY SELECTION

Req ID	Requirement
14.01	When assessing the potential collaboration with Third Parties the relevant security requirements must be specified. The following must be taken into account: • Required physical and logical accesses • Classification of accessed information, including its protection and the information lifecycle • Responsibilities within the scope of collaboration and their nature • Group Security Framework requirements • Security monitoring • Requirements on the location of information and data centers • Applicable legal, regulatory, statutory and contractual requirements. *The applicable security requirements must be defined in the specification documents (RfI / RfP).*
14.02	A defined procedure for assessing the security posture of a Third Party before concluding a contract must exist.
14.03	An assessment of the security posture of the Third Party must be conducted; only reputable and reliable Third Parties must be considered.

2.14.2 THIRD PARTY CONTRACTS

Req ID	Requirement
14.04	Third Party contracts must clearly define all applicable security aspects depending on the provided services. *Examples of security aspects:* • *Roles and responsibilities* • *Identified security and business continuity requirements, security controls, and the defined evaluation criteria, including requirements related to development, operation and maintenance of systems and applications* • *Security activities required to guarantee minimal operational disruption in the event of scheduled or unexpected termination of the collaboration* • *Communication channels, procedures and escalation paths* • *Confidentiality and non-disclosure agreements* • *Service level agreements* • *Right-to-audit clauses* • *Mandatory security awareness and training activities.*

Req ID	Requirement
14.05	Contractual obligations must extend to the entire lifecycle and supply chain of IT products and services under the Third Party's responsibility.
14.06	Third Parties must provide information about the subcontractors used to fulfil their contractual obligations and any relevant changes thereto.
14.07	An inventory of Third-Party contracts must be maintained, including a description of the services provided by the Third Parties.
14.08	The Third Party is required to participate and to fully cooperating in Nexi Group's Threat Led Penetration Testing - TLPT activities when these kind of testing is formally required by one of the competent Authorities.

2.14.3 THIRD PARTY MONITORING

Req ID	Requirement
14.09	Third Parties' security performance and compliance with the contractual obligations must be monitored and assessed regularly based on the defined criteria.
14.10	Third Party security risk assessments must be conducted regularly in accordance with the Group Third Party Risk Assessment procedure.
14.11	Third Parties must immediately report detected security incidents and vulnerabilities that could compromise the services they provide or the Group's information assets.
14.12	Third Parties must handle vulnerabilities related to the IT services provided and promptly report the critical vulnerabilities and corresponding trends. In particular, the Third Parties should investigate the relevant vulnerabilities, analyze the root causes and implement appropriate mitigating actions. **This requirement is a best practice until 17 January 2025, after which it will be required.**
14.13	Appropriate actions must be taken in the event of poor performance or non-compliance with the agreed security requirements by the Third Party, including renegotiation or cancellation of the Third-Party contract(s) and the activation of alternative arrangements to maintain security and ensure continuity of business operations.

2.14.4 THIRD PARTY TERMINATION

Req ID	Requirement
14.14	Termination of the Third Party - contract must be done in a secure and controlled manner and the termination actions taken must be recorded. This includes: • Revocation of physical and logical access rights to Group's premises and IT infrastructure • Return or secure disposal of Group's information assets and IT resources • Confidentiality requirements related to the contractual obligations remain valid after the termination.

2.14.5 CONTRACTOR SECURITY

Req ID	Requirement
14.15	Third Parties must, prior to commencing the assignment, perform background verification checks on their employees working as contractors for the Group in compliance with local laws and regulations.
14.16	Contractors must accept the terms and conditions of the contract in writing, including a non-disclosure agreement.
14.17	The security-related obligations of contractors must be explicitly defined in the contracts.
14.18	Contractors must confirm that they understand their security obligations, including the terms of the non-disclosure agreement, remain valid after change or termination of the contract.
14.19	Contractors and other external users who have been granted access to the Group's information assets and premises must be associated with a Group employee.
14.20	Contractors must acknowledge the need to protect Group's information assets and to perform their daily job responsibilities in compliance with the Security Framework.
14.21	Contractors must receive security training and instructions relevant to their assignment and security-related obligations.
14.22	Upon change or termination of the contractor assignment, logical and physical access must be revoked. The revocation of access must be recorded.
14.23	Upon change or termination of the contractor assignment, Group's information assets and equipment no longer needed, including mobile devices, tokens and similar, must be returned. The action must be confirmed in a legally binding manner.

3. EXTENDED REQUIREMENTS

3.1 PCI DSS

In addition to the above defined baseline requirements, the PCI DSS requirements are mandatory for items within the PCI DSS scope. This chapter contains a list of selected PCI DSS requirements in version 4.0.

Req ID	Requirement
Application Security	
3.4.1	PAN is masked when displayed (the BIN and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see more than the BIN and last four digits of the PAN.
6.2.3 **6.2.3.1**	Bespoke and custom software is reviewed prior to being released into production or to customers, to identify and correct potential coding vulnerabilities, as follows: • Code reviews ensure code is developed according to secure coding guidelines • Code reviews look for both existing and emerging software vulnerabilities • Appropriate corrections are implemented prior to release. If manual code reviews are performed for bespoke and custom software prior to release to production, code changes are: • Reviewed by individuals other than the originating code author, and who are knowledgeable about code-review techniques and secure coding practices • Reviewed and approved by management prior to release.
6.5.2	Upon completion of a significant change, all applicable PCI DSS requirements are confirmed to be in place on all new or changed systems and networks, and documentation is updated as applicable (as per Security By Design Process).
6.5.5	Live PANs are not used in pre-production environments, except where those environments are included in the CDE and protected in accordance with all applicable PCI DSS requirements.
Cyber Defense	
10.3.3	Audit log files, including those for external-facing technologies, are promptly backed up to a secure, central, internal log server(s) or other media that is difficult to modify.
10.3.4	File integrity monitoring or change-detection mechanisms is used on audit logs to ensure that existing log data cannot be changed without generating alerts.
10.4.1	The following audit logs are reviewed at least once daily: • All security events • Logs of all system components that store, process, or transmit CHD and/or SAD • Logs of all critical system components • Logs of all servers and system components that perform security functions (for example, network security controls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers).
10.4.1.1	Automated mechanisms are used to perform audit log reviews. **This requirement is a best practice until 31 March 2025, after which it will be required.**
10.4.2	Logs of all other system components (those not specified in Requirement 10.4.1) are reviewed periodically.
10.4.2.1	The frequency of periodic log reviews for all other system components (not defined in

Req ID	Requirement
	Requirement 10.4.1) is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1. **This requirement is a best practice until 31 March 2025, after which it will be required.**
10.4.3	Exceptions and anomalies identified during the review process are addressed.
10.7.1	Additional requirement for service providers only: Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of the following critical security control systems: • Network security controls • IDS/IPS • FIM • Anti-malware solutions • Physical access controls • Logical access controls • Audit logging mechanisms • Segmentation controls (if used).
Data Security	
3.2.1	Account data storage is kept to a minimum through implementation of data retention and disposal policies, procedures, and processes that include at least the following: • Coverage for all locations of stored account data • Coverage for any sensitive authentication data (SAD) stored prior to completion of authorization. **This bullet is a best practice until 31 March 2025, after which it will be required as part of Requirement 3.2.1 and must be fully considered during a PCI DSS assessment.** • Limiting data storage amount and retention time to that which is required for legal or regulatory, and/or business requirements • Specific retention requirements for stored account data that defines length of retention period and includes a documented business justification • Processes for secure deletion or rendering account data unrecoverable when no longer needed per the retention policy • A process for verifying, at least once every three months, that stored account data exceeding the defined retention period has been securely deleted or rendered unrecoverable.
3.3.1 **3.3.3**	SAD is not retained after authorization, even if encrypted. All sensitive authentication data received is rendered unrecoverable upon completion of the authorization process. Additional requirement for issuers and companies that support issuing services and store sensitive authentication data: Any storage of sensitive authentication data is: • Limited to that which is needed for a legitimate issuing business need and is secured • Encrypted using strong cryptography. **This bullet is a best practice until 31 March 2025, after which it will be required.**
3.3.2	SAD that is stored electronically prior to completion of authorization is encrypted using strong cryptography. **This requirement is best practice until 31 March 2025, after which it will be required.**
3.5.1	PAN is rendered unreadable anywhere it is stored by using any of the following approaches:

Req ID	Requirement
	• One-way hashes based on strong cryptography of the entire PAN • Truncation (hashing cannot be used to replace the truncated segment of PAN) If hashed and truncated versions of the same PAN, or different truncation formats of the same PAN, are present in an environment, additional controls are in place such that the different versions cannot be correlated to reconstruct the original PAN • Index tokens • Strong cryptography with associated key management processes and procedures.
3.5.1.1	Hashes used to render PAN unreadable (per the first bullet of Requirement 3.5.1) are keyed cryptographic hashes of the entire PAN, with associated key-management processes and procedures in accordance with Requirements 3.6 of PCI DSS v4.0 and 3.7. **This requirement is best practice until 31 March 2025, after which it will be required.**
3.5.1.2	If disk-level or partition-level encryption (rather than file-, column-, or field-level database encryption) is used to render PAN unreadable, it is implemented only as follows: • On removable electronic media OR • If used for non-removable electronic media, PAN is also rendered unreadable via another mechanism that meets Requirement 3.5.1. **This requirement is best practice until 31 March 2025, after which it will be required.**
3.5.1.3	If disk-level or partition-level encryption is used (rather than file-, column-, or field-level database encryption) to render PAN unreadable, it is managed as follows: • Logical access is managed separately and independently of native operating system authentication and access control mechanisms • Decryption keys are not associated with user accounts • Authentication factors (passwords, passphrases, or cryptographic keys) that allow access to unencrypted data are stored securely.
3.6.1	Procedures are defined and implemented to protect cryptographic keys used to protect stored account data against disclosure and misuse that include: • Access to keys is restricted to the fewest number of custodians necessary • Key-encrypting keys are at least as strong as the data-encrypting keys they protect • Key-encrypting keys are stored separately from data-encrypting keys • Keys are stored securely in the fewest possible locations and forms.
3.6.1.1	Additional requirement for service providers only: A documented description of the cryptographic architecture is maintained that includes: • Details of all algorithms, protocols, and keys used for the protection of stored account data, including key strength and expiry date • Preventing the use of the same cryptographic keys in production and test environments **This bullet is a best practice until 31 March 2025, after which it will be required.** • Description of the key usage for each key • Inventory of any hardware security modules (HSMs), key management systems (KMS), and other secure cryptographic devices (SCDs) used for key management, including type and location of devices, as outlined in Requirement 12.3.4.
3.6.1.2	Secret and private keys used to encrypt/decrypt stored account data are stored in one (or more) of the following forms at all times: • Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key • Within a secure cryptographic device (SCD), such as a hardware security module (HSM) or

Req ID	Requirement
	PTS-approved point-of-interaction device • As at least two full-length key components or key shares, in accordance with an industry-accepted method.

3.7	Where cryptography is used to protect stored account data, key management processes and procedures covering all aspects of the key lifecycle are defined and implemented to include:
	• Generation of strong cryptographic keys used to protect stored account data
	• Secure distribution of cryptographic keys used to protect stored account data
	• Secure storage of cryptographic keys used to protect stored account data
	• Cryptographic key changes for keys that have reached the end of their cryptoperiod, as defined by the associated application vendor or key owner, and based on industry best practices and guidelines, including the following:
	  • A defined cryptoperiod for each key type in use
	  • A process for key changes at the end of the defined cryptoperiod.
	• The retirement, replacement, or destruction of keys used to protect stored account data, as deemed necessary when:
	  • The key has reached the end of its defined cryptoperiod
	  • The integrity of the key has been weakened, including when personnel with knowledge of a cleartext key component leaves the company, or the role for which the key component was known
	  • The key is suspected of or known to be compromised
	  • Retired or replaced keys are not used for encryption operations
	• Where manual cleartext cryptographic key-management operations are performed by personnel, managing these operations using split knowledge and dual control
	• The prevention of unauthorized substitution of cryptographic keys
	• That cryptographic key custodians formally acknowledge (in writing or electronically) that they understand and accept their key-custodian responsibilities.

3.7.9	Additional requirement for service providers only: Where a service provider shares cryptographic keys with its customers for transmission or storage of account data, guidance on secure transmission, storage and updating of such keys is documented and distributed to the service provider's customers.
4.2.1	Strong cryptography and security protocols are implemented as follows to safeguard PAN during transmission over open, public networks: • Only trusted keys and certificates are accepted • Certificates used to safeguard PAN during transmission over open, public networks are confirmed as valid and are not expired or revoked **This bullet is a best practice until 31 March 2025, after which it will be required.** • The protocol in use supports only secure versions or configurations and does not support fallback to, or use of insecure versions, algorithms, key sizes, or implementations • The encryption strength is appropriate for the encryption methodology in use.
12.3.3	Cryptographic cipher suites and protocols in use are documented and reviewed at least once every 12 months, including at least the following: • An up-to-date inventory of all cryptographic cipher suites and protocols in use, including purpose and where used • Active monitoring of industry trends regarding continued viability of all cryptographic cipher suites and protocols in use • A documented strategy to respond to anticipated changes in cryptographic vulnerabilities.

Req ID	Requirement
	This requirement is a best practice until 31 March 2025, after which it will be required.
4.2.1.1	An inventory of the entity's trusted keys and certificates used to protect PAN during transmission is maintained. **This requirement is a best practice until 31 March 2025, after which it will be required.**
4.2.2	PAN is secured with strong cryptography whenever it is sent via end-user messaging technologies.
9.4.1	All media with cardholder data is physically secured.
9.4.1.1 **9.4.1.2**	Offline media backups with cardholder data are stored in a secure location. The security of the offline media backup location(s) with cardholder data is reviewed at least once every 12 months.
9.4.3	Media with cardholder data sent outside the facility is secured as follows: • Media sent outside the facility is logged • Media is sent by secured courier or other delivery method that can be accurately tracked • Offsite tracking logs include details about media location.
9.4.2	All media with cardholder data is classified in accordance with the sensitivity of the data.
9.4.4	Management approves all media with cardholder data that is moved outside the facility (including when media is distributed to individuals).
9.4.5	Inventory logs of all electronic media with cardholder data are maintained.
9.4.5.1	Inventories of electronic media with cardholder data are conducted at least once every 12 months.
9.4.6	Hard-copy materials with cardholder data are destroyed when no longer needed for business or legal reasons, as follows: • Materials are cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed • Materials are stored in secure storage containers prior to destruction.
9.4.7	Electronic media with cardholder data is destroyed when no longer needed for business or legal reasons via one of the following: • The electronic media is destroyed • The cardholder data is rendered unrecoverable so that it cannot be reconstructed.
Endpoint Security	
1.5.1	Security controls are implemented on any computing devices, including company- and employee-owned devices, that connect to both untrusted networks (including the Internet) and the CDE as follows: • Specific configuration settings are defined to prevent threats being introduced into the entity's network • Security controls are actively running • Security controls are not alterable by users of the computing devices unless specifically documented and authorized by management on a case-by-case basis for a limited period.
Identity and Access Management	

Req ID	Requirement
6.5.6	Test data and test accounts are removed from system components before the system goes into production.
7.2.4	All user accounts and related access privileges, including third-party/vendor accounts, are reviewed as follows: • At least once every six months • To ensure user accounts and access remain appropriate based on job function • Any inappropriate access is addressed • Management acknowledges that access remains appropriate. **This requirement is a best practice until 31 March 2025, after which it will be required.**
7.2.5	All application and system accounts and related access privileges are assigned and managed as follows: • Based on the least privileges necessary for the operability of the system or application • Access is limited to the systems, applications, or processes that specifically require their use. **This requirement is a best practice until 31 March 2025, after which it will be required.**
7.2.5.1	All access by application and system accounts and related access privileges are reviewed as follows: • Periodically (at the frequency defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1) • The application/system access remains appropriate for the function being performed. • Any inappropriate access is addressed • Management acknowledges that access remains appropriate. **This requirement is a best practice until 31 March 2025, after which it will be required.**
7.2.3	Required privileges are approved by authorized personnel.
7.3.1	An access control system(s) is in place that restricts access based on a user's need to know and covers all system components.
8.2.7	Accounts used by third parties to access, support, or maintain system components via remote access are managed as follows: • Enabled only during the time period needed and disabled when not in use • Use is monitored for unexpected activity.
8.3.6	If passwords/passphrases are used as authentication factors to meet Requirement 8.3.1 of PCI DSS v.4.0, they meet the following minimum level of complexity: • A minimum length of 12 characters (or IF the system does not support 12 characters, a minimum length of eight characters) • Contain both numeric and alphabetic characters. **This requirement is a best practice until 31 March 2025, after which it will be required.**
8.3.9 **8.3.10.1**	If passwords/passphrases are used as the only authentication factor for user access, (i.e., in any single-factor authentication implementation) then either: • Passwords/passphrases are changed at least once every 90 days, OR • The security posture of accounts is dynamically analyzed, and real-time access to resources is automatically determined accordingly. Additional requirement for service providers only: If passwords/passphrases are used as the only

Req ID	Requirement
	authentication factor for customer user access, (i.e., in any single-factor authentication implementation) then either: • Passwords/passphrases are changed at least once every 90 days, OR • The security posture of accounts is dynamically analyzed, and real-time access to resources is automatically determined accordingly. **This requirement is a best practice until 31 March 2025, after which it will be required.**
8.3.10	Additional requirement for service providers only: If passwords/passphrases are used as the only authentication factor for customer user access to cardholder data (i.e., in any single-factor authentication implementation), then guidance is provided to customer users including: • Guidance for customers to change their user passwords/passphrases periodically • Guidance as to when, and under what circumstances, passwords/passphrases are to be changed.
8.3.8	Authentication policies and procedures are documented and communicated to all users including: • Guidance on selecting strong authentication factors • Guidance for how users should protect their authentication factors • Instructions not to reuse previously used passwords/passphrases • Instructions to change passwords/passphrases if there is any suspicion or knowledge that the password/passphrases have been compromised and how to report the incident.
8.2.2	Group, shared, or generic accounts, or other shared authentication credentials are only used, when necessary, on an exception basis, and are managed as follows: • Account use is prevented unless needed for an exceptional circumstance • Use is limited to the time needed for the exceptional circumstance • Business justification for use is documented • Use is explicitly approved by management • Individual user identity is confirmed before access to an account is granted • Every action taken is attributable to an individual user.
8.2.3	Additional requirement for service providers only: Service providers with remote access to customer premises use unique authentication factors for each customer premises.
8.4.2	MFA is implemented for all access into the CDE. **This requirement is a best practice until 31 March 2025, after which it will be required.**
8.5.1	MFA systems are implemented as follows: • The MFA system is not susceptible to replay attacks • MFA systems cannot be bypassed by any users, including administrative users unless specifically documented, and authorized by management on an exception basis, for a limited time period • At least two different types of authentication factors are used • Success of all authentication factors is required before access is granted. **This requirement is a best practice until 31 March 2025, after which it will be required.**
8.6.1	If accounts used by systems or applications can be used for interactive login, they are managed as follows: • Interactive use is prevented unless needed for an exceptional circumstance • Interactive use is limited to the time needed for the exceptional circumstance • Business justification for interactive use is documented

Req ID	Requirement
	• Interactive use is explicitly approved by management • Individual user identity is confirmed before access to account is granted • Every action taken is attributable to an individual user. **This requirement is a best practice until 31 March 2025, after which it will be required.**
8.6.2	Passwords/passphrases for any application and system accounts that can be used for interactive login are not hard coded in scripts, configuration/property files, or bespoke and custom source code. **This requirement is a best practice until 31 March 2025, after which it will be required.**
8.6.3	Passwords/passphrases for any application and system accounts are protected against misuse as follows: • Passwords/passphrases are changed periodically (at the frequency defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1) and upon suspicion or confirmation of compromise • Passwords/passphrases are constructed with sufficient complexity appropriate for how frequently the entity changes the passwords/passphrases. **This requirement is a best practice until 31 March 2025, after which it will be required.**
7.2.6	All user access to query repositories of stored cardholder data is restricted as follows: • Via applications or other programmatic methods, with access and allowed actions based on user roles and least privileges • Only the responsible administrator(s) can directly access or query repositories of stored CHD.
A1.1.1	Only for multi-tenant service providers: Logical separation is implemented as follows: • The provider cannot access its customers' environments without authorization • Customers cannot access the provider's environment without authorization. **This requirement is a best practice until 31 March 2025, after which it will be required.**
Network and Communications Security	
1.2.2	All changes to network connections and to configurations of Network Security Controls are approved and managed in accordance with the change control process defined at Requirement 6.5.1.
1.2.3	An accurate network diagram(s) is maintained that shows all connections between the CDE and other networks, including any wireless networks.
1.2.4	An accurate data-flow diagram(s) is maintained that meets the following: • Shows all account data flows across systems and networks • Updated as needed upon changes to the environment.
1.2.5 **1.2.6**	All services, protocols, and ports allowed are identified, approved, and have a defined business need. Security features are defined and implemented for all services, protocols, and ports that are in use and considered to be insecure, such that the risk is mitigated.
1.2.7	Configurations of Network Security Controls are reviewed at least once every six months to confirm they are relevant and effective.

Req ID	Requirement
1.2.8	Configuration files for NSCs are: • Secured from unauthorized access • Kept consistent with active network configurations.
1.4.4	System components that store cardholder data are not directly accessible from untrusted networks.
3.4.2	When using remote-access technologies, technical controls prevent copy and/or relocation of PAN for all personnel, except for those with documented, explicit authorization and a legitimate, defined business need. **This requirement is a best practice until 31 March 2025, after which it will be required.**
Personnel Security	
6.2.2	Software development personnel working on bespoke and custom software are trained at least once every 12 months as follows: • On software security relevant to their job function and development languages • Including secure software design and secure coding techniques. • Including, if security testing tools are used, how to use the tools for detecting vulnerabilities in software.
12.6.2	The security awareness program is: • Reviewed at least once every 12 months, and • Updated as needed to address any new threats and vulnerabilities that may impact the security of the entity's CDE, or the information provided to personnel about their role in protecting cardholder data. **This requirement is a best practice until 31 March 2025, after which it will be required.**
12.6.3.1	Security awareness training includes awareness of threats and vulnerabilities that could impact the security of the CDE, including but not limited to: • Phishing and related attacks • Social engineering. **This requirement is a best practice until 31 March 2025, after which it will be required.**
12.6.3.2	Security awareness training includes awareness about the acceptable use of end-user technologies in accordance with Requirement 12.2.1 of PCI DSS v.4.0. **This requirement is a best practice until 31 March 2025, after which it will be required.**
12.10.4.1	The frequency of periodic training for incident response personnel is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1. **This requirement is a best practice until 31 March 2025, after which it will be required.**
Physical Security	
9.2.2	Physical and/or logical controls are implemented to restrict use of publicly accessible network jacks within the facility.
9.2.4	Access to consoles in sensitive areas is restricted via locking when not in use.
9.3.4	A visitor log is used to maintain a physical record of visitor activity within the facility and within

Req ID	Requirement
	sensitive areas, including: • The visitor's name and the organization represented • The date and time of the visit • The name of the personnel authorizing physical access • Retaining the log for at least three months, unless otherwise restricted by law.
9.3.1	Procedures are implemented for authorizing and managing physical access of personnel to the CDE, including: • Identifying personnel. • Managing changes to an individual's physical access requirements • Revoking or terminating personnel identification • Limiting access to the identification process or system to authorized personnel.
9.3.2	Procedures are implemented for authorizing and managing visitor access to the CDE, including: • Visitors are authorized before entering • Visitors are escorted at all times • Visitors are clearly identified and given a badge or other identification that expires • Visitor badges or other identification visibly distinguishes visitors from personnel.
Security Governance	
12.3.1	Each PCI DSS requirement that provides flexibility for how frequently it is performed (for example, requirements to be performed periodically) is supported by a targeted risk analysis that is documented and includes: • Identification of the assets being protected • Identification of the threat(s) that the requirement is protecting against • Identification of factors that contribute to the likelihood and/or impact of a threat being realized • Resulting analysis that determines, and includes justification for, how frequently the requirement must be performed to minimize the likelihood of the threat being realized • Review of each targeted risk analysis at least once every 12 months to determine whether the results are still valid or if an updated risk analysis is needed • Performance of updated risk analyses when needed, as determined by the annual review. **This requirement is a best practice until 31 March 2025, after which it will be required.**
12.3.2	A targeted risk analysis is performed for each PCI DSS requirement that the entity meets with the customized approach, to include: • Documented evidence detailing each element specified in Appendix D: Customized Approach (including, at a minimum, a controls matrix and risk analysis) • Approval of documented evidence by senior management • Performance of the targeted analysis of risk at least once every 12 months.
12.4.1	Additional requirement for service providers only: Responsibility is established by executive management for the protection of cardholder data and a PCI DSS compliance program to include: • Overall accountability for maintaining PCI DSS compliance • Defining a charter for a PCI DSS compliance program and communication to executive management.
12.5.2	PCI DSS scope is documented and confirmed by the entity at least once every 12 months and upon significant change to the in-scope environment. At a minimum, the scoping validation

Req ID	Requirement
	includes: • Identifying all data flows for the various payment stages (for example, authorization, capture settlement, chargebacks, and refunds) and acceptance channels (for example, card-present, card-not-present, and e-commerce) • Updating all data-flow diagrams per Requirement 1.2.4 • Identifying all locations where account data is stored, processed, and transmitted, including but not limited to: 1) any locations outside of the currently defined CDE, 2) applications that process CHD, 3) transmissions between systems and networks, and 4) file backups • Identifying all system components in the CDE, connected to the CDE, or that could impact security of the CDE • Identifying all segmentation controls in use and the environment(s) from which the CDE is segmented, including justification for environments being out of scope • Identifying all connections from third-party entities with access to the CDE • Confirming that all identified data flows, account data, system components, segmentation controls, and connections from third parties with access to the CDE are included in scope.
12.5.2.1	Additional requirement for service providers only: PCI DSS scope is documented and confirmed by the entity at least once every six months and upon significant change to the in-scope environment. At a minimum, the scoping validation includes all the elements specified in Requirement 12.5.2. **This requirement is a best practice until 31 March 2025, after which it will be required.**
12.5.3	Additional requirement for service providers only: Significant changes to organizational structure result in a documented (internal) review of the impact to PCI DSS scope and applicability of controls, with results communicated to executive management. **This requirement is a best practice until 31 March 2025, after which it will be required.**
12.9.2	Additional requirement for service providers only: TPSPs support their customers' requests for information to meet Requirements 12.8.4 and 12.8.5 by providing the following upon customer request: • PCI DSS compliance status information for any service the TPSP performs on behalf of customers (Requirement 12.8.4) • Information about which PCI DSS requirements are the responsibility of the TPSP and which are the responsibility of the customer, including any shared responsibilities (Requirement 12.8.5).
Security Incident Management	
10.7.2	Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of the following critical security control systems: • Network security controls • IDS/IPS • Change-detection mechanisms • Anti-malware solutions • Physical access controls • Logical access controls • Audit logging mechanisms • Segmentation controls (if used) • Audit log review mechanisms • Automated security testing tools (if used).

Req ID	Requirement
	This requirement is a best practice until 31 March 2025, after which it will be required.
10.7.3	Failures of any critical security controls systems are responded to promptly, including but not limited to: • Restoring security functions • Identifying and documenting the duration (date and time from start to end) of the security failure • Identifying and documenting the cause(s) of failure and documenting required remediation • Identifying and addressing any security issues that arose during the failure • Determining whether further actions are required as a result of the security failure. • Implementing controls to prevent the cause of failure from reoccurring • Resuming monitoring of security controls. **This requirement is a best practice until 31 March 2025, after which it will be required.**
12.10.1	An incident response plan exists and is ready to be activated in the event of a suspected or confirmed security incident. The plan includes, but is not limited to: • Roles, responsibilities, and communication and contact strategies in the event of a suspected or confirmed security incident, including notification of payment brands and acquirers, at a minimum • Incident response procedures with specific containment and mitigation activities for different types of incidents • Business recovery and continuity procedures • Data backup processes • Analysis of legal requirements for reporting compromises • Coverage and responses of all critical system components • Reference or inclusion of incident response procedures from the payment brands.
12.10.3	Specific personnel are designated to be available on a 24/7 basis to respond to suspected or confirmed security incidents.
12.10.4	Personnel responsible for responding to suspected and confirmed security incidents are appropriately and periodically trained on their incident response responsibilities.
12.10.5	The security incident response plan includes monitoring and responding to alerts from security monitoring systems, including but not limited to: • Intrusion-detection and intrusion-prevention systems • Network security controls • Change-detection mechanisms for critical files • The change-and tamper-detection mechanism for payment pages **This bullet is a best practice until 31 March 2025, after which it will be required.** • Detection of unauthorized wireless access points.
12.10.7	Incident response procedures are in place, to be initiated upon the detection of stored PAN anywhere it is not expected, and include: • Determining what to do if PAN is discovered outside the CDE, including its retrieval, secure deletion, and/or migration into the currently defined CDE, as applicable • Identifying whether sensitive authentication data is stored with PAN • Determining where the account data came from and how it ended up where it was not expected • Remediating data leaks or process gaps that resulted in the account data being where it was

Req ID	Requirement
	not expected. **This requirement is a best practice until 31 March 2025, after which it will be required.**
A1.2.3	Only for multi-tenant service providers: Processes or mechanisms are implemented for reporting and addressing suspected or confirmed security incidents and vulnerabilities, including: • Customers can securely report security incidents and vulnerabilities to the provider • The provider addresses and remediates suspected or confirmed security incidents and vulnerabilities according to Requirement 6.3.1 of PCI DSS v.4.0. **This requirement is a best practice until 31 March 2025, after which it will be required.**
A3.3.1	Only for Designated Entities Supplement Validation (DESV): Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of: • Network security controls • IDS/IPS • FIM • Anti-malware solutions • Physical access controls • Logical access controls • Audit logging mechanisms • Segmentation controls (if used) • Automated audit log review mechanisms **(best practice until 31 March 2025)** • Automated code review tools (if used) **(best practice until 31 March 2025).**
Security Testing and Vulnerability Management	
11.2.1	Authorized and unauthorized wireless access points are managed as follows: • The presence of wireless (Wi-Fi) access points is tested for • All authorized and unauthorized wireless access points are detected and identified • Testing, detection, and identification occurs at least once every three months • If automated monitoring is used, personnel are notified via generated alerts.
11.3.1	Internal vulnerability scans are performed as follows: • At least once every three months • High-risk and critical vulnerabilities (per the entity's vulnerability risk rankings defined at Requirement 6.3.1 of PCI DSS v.4.0) are resolved • Rescans are performed that confirm all high-risk and critical vulnerabilities (as noted above) have been resolved • Scan tool is kept up to date with latest vulnerability information • Scans are performed by qualified personnel and organizational independence of the tester exists.
11.3.1.1	All other applicable vulnerabilities (those not ranked as high-risk or critical per the entity's vulnerability risk rankings defined at Requirement 6.3.1 of PCI DSS v.4.0) are managed as follows: • Addressed based on the risk defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1 • Rescans are conducted as needed. **This requirement is a best practice until 31 March 2025, after which it will be required.**
11.3.1.2	Internal vulnerability scans are performed via authenticated scanning as follows:

Req ID	Requirement
	• Systems that are unable to accept credentials for authenticated scanning are documented • Sufficient privileges are used for those systems that accept credentials for scanning. • If accounts used for authenticated scanning can be used for interactive login, they are managed in accordance with Requirement 8.2.2. **This requirement is a best practice until 31 March 2025, after which it will be required.**
11.3.2	External vulnerability scans are performed as follows: • At least once every three months • By a PCI SSC Approved Scanning Vendor (ASV) • Vulnerabilities are resolved and ASV Program Guide requirements for a passing scan are met • Rescans are performed as needed to confirm that vulnerabilities are resolved per the ASV Program Guide requirements for a passing scan.
11.4.3	External penetration testing is performed: • Per the entity's defined methodology • At least once every 12 months • After any significant infrastructure or application upgrade or change • By a qualified internal resource or qualified external third party • Organizational independence of the tester exists (not required to be a QSA or ASV).
11.4.2	Internal penetration testing is performed: • Per the entity's defined methodology • At least once every 12 months • After any significant infrastructure or application upgrade or change • By a qualified internal resource or qualified external third-party • Organizational independence of the tester exists (not required to be a QSA or ASV).
11.4.4	Exploitable vulnerabilities and security weaknesses found during penetration testing are corrected as follows: • In accordance with the entity's assessment of the risk posed by the security issue as defined in Requirement 6.3.1 of PCI DSS v.4.0 • Penetration testing is repeated to verify the corrections.
11.4.5	If segmentation is used to isolate the CDE from other networks, penetration tests are performed on segmentation controls as follows: • At least once every 12 months and after any changes to segmentation controls/methods • Covering all segmentation controls/methods in use • According to the entity's defined penetration testing methodology • Confirming that the segmentation controls/methods are operational and effective, and isolate the CDE from all out-of-scope systems • Confirming effectiveness of any use of isolation to separate systems with differing security levels (see Requirement 2.2.3) • Performed by a qualified internal resource or qualified external third party • Organizational independence of the tester exists (not required to be a QSA or ASV).
A1.1.4	Only for multi-tenant service providers: The effectiveness of logical separation controls used to separate customer environments is confirmed at least once every six months via penetration testing. **This requirement is a best practice until 31 March 2025, after which it will be required.**

Req ID	Requirement
11.4.7	Additional requirement for multi-tenant service providers only: Multi-tenant service providers support their customers for external penetration testing per Requirement 11.4.3 and 11.4.4. **This requirement is a best practice until 31 March 2025, after which it will be required.**
11.5.1.1	Additional requirement for service providers only: Intrusion-detection and/or intrusion-prevention techniques detect, alert on/prevent, and address covert malware communication channels. **This requirement is a best practice until 31 March 2025, after which it will be required.**

11.6.1	A change and tamper-detection mechanism is deployed as follows:
	• To alert personnel to unauthorized modification (including indicators of compromise, changes, additions, and deletions) to the HTTP headers and the contents of payment pages as received by the consumer browser
	• The mechanism is configured to evaluate the received HTTP header and payment page
	• The mechanism functions are performed as follows:
	  ○ At least once every seven days OR
	  ○ Periodically (at the frequency defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1).
	This requirement is a best practice until 31 March 2025, after which it will be required.

9.5.1.2.1	The frequency of periodic POI device inspections and the type of inspections performed is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1. **This requirement is a best practice until 31 March 2025, after which it will be required.**
System Security	
2.2.1b	System configuration standards are updated as new vulnerability issues are identified.
2.2.1.c	System configuration standards are applied when new systems are configured and verified as being in place before or immediately after a system component is connected to a production environment.
2.2.2	Vendor default accounts are managed as follows: • If the vendor default account(s) will be used, the default password is changed per Requirement 8.3.6 • If the vendor default account(s) will not be used, the account is removed or disabled.
2.2.3	Primary functions requiring different security levels are managed as follows: • Only one primary function exists on a system component, OR • Primary functions with differing security levels that exist on the same system component are isolated from each other, OR • Primary functions with differing security levels on the same system component are all secured to the level required by the function with the highest security need.
2.2.4	Only necessary services, protocols, daemons, and functions are enabled, and all unnecessary functionality is removed or disabled.
2.2.5	If any insecure services, protocols, or daemons are present: • Business justification is documented • Additional security features are documented and implemented that reduce the risk of using insecure services, protocols, or daemons.

Req ID	Requirement
2.2.6	System security parameters are configured to prevent misuse.
12.5.1	An inventory of system components that are in scope for PCI DSS, including a description of function/use, is maintained and kept current.
5.2.1	An anti-malware solution(s) is deployed on all system components, except for those system components identified in periodic evaluations per Requirement 5.2.3 that concludes the system components are not at risk from malware.
5.2.2	The deployed anti-malware solution(s): • Detects all known types of malware • Removes, blocks, or contains all known types of malware.
5.2.3	Any system components that are not at risk for malware are evaluated periodically to include the following: • A documented list of all system components not at risk for malware • Identification and evaluation of evolving malware threats for those system components • Confirmation whether such system components continue to not require anti-malware protection.
5.2.3.1	The frequency of periodic evaluations of system components identified as not at risk for malware is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1. **This requirement is a best practice until 31 March 2025, after which it will be required.**
5.3.1 **5.3.2** **5.3.3**	The anti-malware solution(s) is kept current via automatic updates. The anti-malware solution(s): • Performs periodic scans and active or real-time scans, OR • Performs continuous behavioral analysis of systems or processes. For removable electronic media, the anti-malware solution(s): • Performs automatic scans of when the media is inserted, connected, or logically mounted, OR • Performs continuous behavioral analysis of systems or processes when the media is inserted, connected, or logically mounted. **This requirement is a best practice until 31 March 2025, after which it will be required.**
5.3.2.1	If periodic malware scans are performed to meet Requirement 5.3.2, the frequency of scans is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1. **This requirement is a best practice until 31 March 2025, after which it will be required.**
5.3.5	Anti-malware mechanisms cannot be disabled or altered by users, unless specifically documented, and authorized by management on a case-by-case basis for a limited time period.
5.4.1	Processes and automated mechanisms are in place to detect and protect personnel against phishing attacks. **This requirement is a best practice until 31 March 2025, after which it will be required.**

Req ID	Requirement
6.3.2	An inventory of bespoke and custom software, and third-party software components incorporated into bespoke and custom software is maintained to facilitate vulnerability and patch management. **This requirement is a best practice until 31 March 2025, after which it will be required.**
12.3.4	Hardware and software technologies in use are reviewed at least once every 12 months, including at least the following: • Analysis that the technologies continue to receive security fixes from vendors promptly • Analysis that the technologies continue to support (and do not preclude) the entity's PCI DSS compliance • Documentation of any industry announcements or trends related to a technology, such as when a vendor has announced "end of life" plans for a technology • Documentation of a plan, approved by senior management, to remediate outdated technologies, including those for which vendors have announced "end of life" plans. **This requirement is a best practice until 31 March 2025, after which it will be required.**
6.3.3	All system components are protected from known vulnerabilities by installing applicable security patches/updates as follows: • Critical or high-security patches/updates (identified according to the risk ranking process at Requirement 6.3.1 of PCI DSS v.4.0) are installed within one month of release • All other applicable security patches/updates are installed within an appropriate time frame as determined by the entity (for example, within three months of release).
6.4.2	For public-facing web applications, an automated technical solution is deployed that continually detects and prevents web-based attacks, with at least the following: • Is installed in front of public-facing web applications and is configured to detect and prevent web-based attacks • Actively running and up to date as applicable • Generating audit logs • Configured to either block web-based attacks or generate an alert that is immediately investigated. **This requirement is a best practice until 31 March 2025, after which it will be required.**
6.4.3	All payment page scripts that are loaded and executed in the consumer's browser are managed as follows: • A method is implemented to confirm that each script is authorized • A method is implemented to assure the integrity of each script • An inventory of all scripts is maintained with written justification as to why each is necessary. **This requirement is a best practice until 31 March 2025, after which it will be required.**
6.5.1	Changes to all system components in the production environment are made according to established procedures that include: • Reason for, and description of, the change • Documentation of security impact • Documented change approval by authorized parties • Testing to verify that the change does not adversely impact system security • For bespoke and custom software changes, all updates are tested for compliance with Requirement 6.2.4 before being deployed into production • Procedures to address failures and return to a secure state.

Req ID	Requirement
10.6.1	System clocks and time are synchronized using time-synchronization technology and kept current.
10.6.2	Systems are configured to the correct and consistent time as follows: • One or more designated time servers are in use • Only the designated central time server(s) receives time from external sources • Time received from external sources is based on International Atomic Time or Coordinated Universal Time (UTC) • The designated time server(s) accept time updates only from specific industry-accepted • external sources • Where there is more than one designated time server, the time servers peer with one another to keep accurate time • Internal systems receive time information only from designated central time server(s).
10.6.3	Time synchronization settings and data are protected as follows: • Access to time data is restricted to only personnel with a business need • Any changes to time settings on critical systems are logged, monitored, and reviewed.
Third Party Security	
12.8.2	Written agreements with Third-Party Service Providers (TPSP) are maintained as follows: • Written agreements are maintained with all TPSPs with which account data is shared or that could affect the security of the CDE • Written agreements include acknowledgments from TPSPs that they are responsible for the security of account data the TPSPs possess or otherwise store, process, or transmit on behalf of the entity, or to the extent that they could impact the security of the entity's CDE.
12.8.4	A program is implemented to monitor TPSPs' PCI DSS compliance status at least once every 12 months.
12.8.5	Information is maintained about which PCI DSS requirements are managed by each TPSP, which are managed by the entity, and any that are shared between the TPSP and the entity.

3.2 PCI PIN

In addition to the above defined baseline requirements, the PCI PIN requirements are mandatory for items within the PCI PIN scope. This chapter contains a list of selected PCI PIN requirements in version 3.1.

Req ID	Requirement
Data Security	
Req. 3	For online interchange transactions, PINs must be only encrypted using ISO 9564–1 PIN-block formats 0, 1, 3 or 4. Format 2 must be used for PINs that are submitted from the IC card reader to the IC card.
Req. 8	Secret or private keys must be transferred by a) Physically forwarding the key as at least two separate key shares or full-length components (hard copy, smart card, SCD) using different communication channels, or b) Transmitting the key in ciphertext form. Public keys must be conveyed in a manner that protects their integrity and authenticity. It is the responsibility of both the sending and receiving parties to ensure these keys are managed securely during transport.
8-2	A person with access to one component or share of a secret or private key, or to the media conveying this value, must not have access to other components or shares of this key or to any other medium containing other components or shares sufficient to form the necessary threshold to derive the key.
13-5	Any media (electronic or otherwise) containing secret or private key components or shares used for loading cryptographic keys must be maintained in a secure storage location and accessible only to authorized custodian(s). When removed from the secure storage location, media or devices containing key components or used for the injection of clear-text cryptographic keys must be in the physical possession of only the designated component holder(s), and only for the minimum practical time necessary to complete the key-loading process. The media upon which a component resides must be physically safeguarded at all times when removed from secure storage. Key components that can be read (for example, those printed on paper or stored on magnetic cards, PROMs, or smartcards) must be managed so they are never used in a manner that would result in the component being displayed in clear text to anyone who is not a designated custodian for that component.
13-8	A person with access to any component or share of a secret or private key, or to the media conveying this value, must not have access to other components or shares of this key or to any other medium containing other components or shares of this key that are sufficient to form the necessary threshold to derive the key.
13-9.4.9	If the PC application reads or stores clear-text key components, for example, BDKs or TMKs, from portable electronic media (e.g., smart cards), the media must be secured as components under dual control when not in use. The key components must be manually entered at the start of each key-injection session from components that are maintained under dual control and split knowledge.
18-3	Encrypted symmetric keys must be managed in structures called key blocks. The key usage must be cryptographically bound to the key using accepted methods. The phased implementation dates are as follows:

	• Phase 1 – Implement Key Blocks for internal connections and key storage within Service Provider Environments – this would include all applications and databases connected to hardware security modules (HSM). Effective date: 1 June 2019 • Phase 2 – Implement Key Blocks for external connections to Associations and Networks. Effective date: 1 January 2023 • Phase 3 – Implement Key Block to extend to all merchant hosts, point-of-sale (POS) devices and ATMs. Effective date: 1 January 2025
Req. 21	Secret keys used for enciphering PIN-encryption keys or for PIN encryption, or private keys used in connection with remote key distribution implementations, must never exist outside of SCDs, except when encrypted or securely stored and managed using the principles of dual control and split knowledge.
Req. 25	Access to secret or private cryptographic keys and key material must be: a) Limited to a need-to-know basis so that the fewest number of key custodians are necessary to enable their effective use, and b) Protected such that no other person (not similarly entrusted with that component) can observe or otherwise obtain the component.
29-1.1	All POIs and other SCDs must be protected against compromise. Any compromise must be detected. Loading and use of any financial keys after the compromise must be prevented.

3.3 PCI 3DS

In addition to the above defined baseline requirements, the PCI 3DS requirements are mandatory for items within the PCI 3DS scope. This chapter contains a list of selected PCI 3DS requirements in version 1.0.

Req ID	Requirement
Identity and Access Management	
4.3.4	Remote access privileges are monitored and/or reviewed at least quarterly by an authorized individual to confirm access is still required.
5.1.1 (P2)	Policies and procedures for usage, flow, retention, and disposal of 3DS data are maintained and implemented.
5.2.2 (P2)	Fallback to insecure cryptographic protocols and configurations is not permitted.
5.4.1	Storage of 3DS sensitive data is limited to only permitted data elements.
5.4.2	Strong cryptography is used to protect any permitted storage of 3DS sensitive data.