

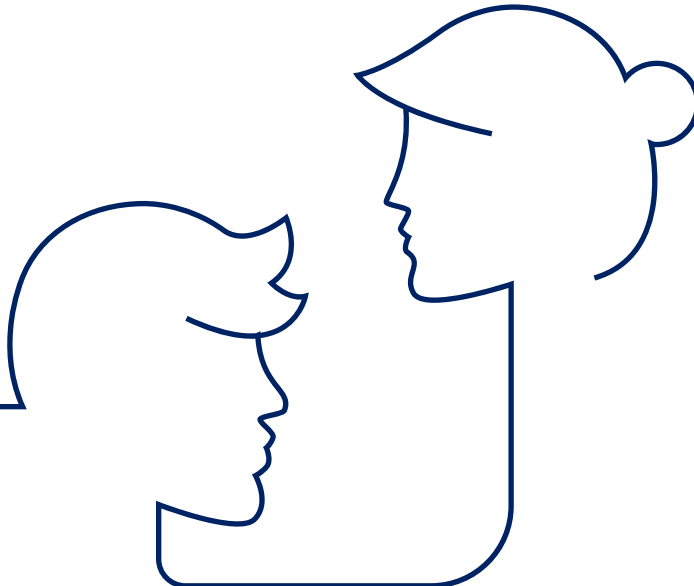
Insuring
a more
open world



CNP Assurances

Group Cybersecurity Policy Summary

May 2026



Introductory Note

This document is a condensed version of the CNP Assurances Group's cybersecurity policy - GR/DCSG/POL001 (the "**Policy**"). It is intended primarily for external stakeholders and offers a concise overview of the measures in place to secure information within each entity of the CNP Assurances Group, consisting of CNP Assurances Holding and all of its direct and indirect subsidiaries (the "**Group**").

1. Purpose and Scope of the Policy

- The Group places strategic importance on cybersecurity in order to ensure the digital resilience of its operations, comply with its obligations and strengthen the confidence of its stakeholders.
- The Policy defines the fundamental guidelines for information security. It applies to all entities of the Group, as well as to its personnel, partners and service providers that have access to its data or information systems.
- In compliance with applicable legal and regulatory requirements, the Policy aims to guarantee the confidentiality, integrity and availability of information processed by aligning itself with the state of the art in cybersecurity.
- Initially approved by the Executive Committee (COMEX) and upon any significant change by the Group Risk Committee (CRG), the Policy reflects the cybersecurity strategy overseen by the Group's Board of Directors. It is reviewed annually to account for technological, regulatory and security standards developments, as well as the constantly evolving dynamics of cyber threats.

2. Guiding Principles

The Group's cybersecurity is built on the following guiding principles. Aligned with leading international standards, these principles guide all protection efforts and ensure dynamic management of cyber risks:

2.1. Risk-Based Approach and Continuous Improvement

- The Group is committed to a proactive security approach in line with the ISO/IEC 27001 standard's "Plan-Do-Check-Act" (PDCA).
- Risk analyses are conducted continuously to identify, assess and effectively address threats to information and related assets.
- This approach supports a structured continuous improvement process based on regular controls and corrective or enhancement actions, taking into account the risk appetite defined by the Group.

2.2. Protection of Information and Associated Assets

- The Group protects its information assets, as well as the systems, applications and infrastructures supporting them, to prevent any data leakage, alteration, unavailability or unauthorized access.
- This protection is based on measures commensurate with the relevant stakes and risks, designed to ensure the confidentiality, integrity, availability and traceability of information throughout its entire lifecycle.
- The principles of *Security by Design* and *Privacy by Design* are embedded from the scoping and design phases of projects. They are implemented through the identification of security requirements, the conduct of risk assessments, their documentation within project records, their translation into appropriate measures, as well as the validation of personal data processing activities prior to their implementation, including through the performance of Data Protection Impact Assessments where required by applicable regulations (DPIAs).

2.3. Monitoring and Threat Response

- Continuous monitoring of system security and emerging threats is performed.
- Detection and alert mechanisms enable the rapid identification of events, intrusion attempts or suspicious activities.
- The Group has a proven security incident response capability with escalation procedures that enable effective handling of any cyber incident and limit its impact on the Group's activities and customers.

2.4. Shared Responsibility and Security Culture

- Within the Group, information security is everyone's responsibility. Strongly committed to cybersecurity, the Board of Directors and the Executive Committee (COMEX) ensure that every employee is aware of the protection rules and the need to apply them daily.
- An ongoing awareness and training program is implemented to foster a true culture of security. All employees are required to complete annual training to learn best practices and the obligations related to information security.

2.5. Third-Party Risk Management

- The Group requires its partners and external contractors to maintain a level of security commensurate with the risks associated with their activities and aligned with the Group's own standards where they access its systems, services or data.
- This requirement is supported by a due diligence process, contractual clauses, security assurance plans and cybersecurity audit campaigns. In this respect, the Group ensures in particular that third parties receive appropriate awareness training on information system security risks, proportionate to the nature of their services and the conditions under which they operate.

3. Governance, Roles and Responsibilities

A clear and structured governance forms the foundation of a robust and effective Information Security Management System (ISMS). To this end, the Group has adopted a governance model structured between central bodies and operational entities to ensure consistent implementation of the Policy at all levels of the organization:

3.1. Central Governance Structure

- The Board of Directors, upon recommendation of its specialized committee, the Audit and Risk Committee (**CAR**), approves the Group's risk appetite and cybersecurity strategy. The CAR provides regular oversight of information systems and data security matters. In this capacity, it reviews strategic orientations, major risks, potential incidents, key indicators and the associated action plans in order to inform the Board of Directors in the discharge of its responsibilities.
- The Executive Committee (COMEX) bears ultimate responsibility for information systems security. It ensures the effective application of the Policy and its integration into the Group's overall strategy.
- The Group Chief Information Security Officer (Group CISO), as Head of the Group Cybersecurity Department, develops the Policy, drives the implementation of the ISMS, measures its performance and reports regularly to the Executive Committee and specialized committees: the Information Systems Security Committee (CSSI), the Group Risk Committee (CRG), and the Audit and Risk Committee (CAR).
- In order to ensure the cross-functional steering of the ISMS and its continuous adaptation, this governance relies on monthly Information Systems Security Committees (CSSI), comprising notably the key Risk, IT, Data Protection functions, as well as members of the Executive Committee.
- The organization follows a three-lines-of-defense model, ensuring a separation of responsibilities between implementation and operations (first line), steering and second-level control (second line), independent audit (third line):
 - Comprised of IT and business teams, the first line applies security measures within the company's operational activities. The IT team, fulfilling detection, protection and continuity functions, designs, deploys and operates security solutions. Acting as the guarantor of technical security measures and their operational maintenance, it carries out first-level controls and supports projects on security matters.
 - Comprised of the Risk Management Function (including the Group Cybersecurity Department), the second line is responsible for defining, steering and monitoring the ISMS. It identifies and tracks cyber risks, ensures compliance with regulations in coordination with the Compliance Department and performs regular controls on the measures in place.
 - The third line is the Group Internal Audit Department, which independently and regularly evaluates the effectiveness of the ISMS and the proper implementation of applicable security standards. Its recommendations are incorporated into continuous improvement plans.
- Employees are required to comply with security rules and procedures in their daily activities. They are continually made aware of and trained in good practices. Any breach is analyzed, followed and results in appropriate actions (reminders, educational measures or even disciplinary sanctions).
- Partners and service providers must also conform to the Group's security requirements. Regular audits and joint steering committees are conducted to ensure the protection of the data and systems involved.

3.2. Operational Implementation at the Entity Level

- In compliance with the guidelines defined by the Group Cybersecurity Department, each entity operationally implements this Policy according to its own specific context.
- In this framework, each entity is responsible for establishing local governance aligned with the central model, integrating cybersecurity requirements into its activities, conducting risk analyses tailored to its environment, raising security awareness among its employees and participating in the centralized system for security event detection, response and reporting.
- The Group Cybersecurity Department oversees this rollout through methodological support, regular coordination of the security correspondent network and continuous monitoring to ensure the consistency, coherence and effectiveness of the overall ISMS across the Group.

4. Risk Management and Compliance Framework

A cybersecurity program covering all facets required for robust protection is implemented on an ongoing basis. Aligned with leading security frameworks (ISO, NIST, CIS, OWASP, etc.), this program ensures consistent risk treatment and a framework for continuous improvement. The processes implemented include in particular:

4.1. Risk Analysis and Treatment

- Data and associated information systems are inventoried and undergo regular security analyses.
- A risk map is maintained and treatment plans are implemented to mitigate identified risks in line with the risk tolerance defined by the Group.

4.2. Internal Security Framework

- The Policy is implemented through directives and operational procedures covering all key areas including governance, asset classification, access management, data and application security, network protection, security event management, business continuity, compliance, etc.
- These documents provide teams with instructions to follow in order to implement security on a daily basis. Made available to the entities, the internal framework constitutes a shared baseline of elevated security standards.
- The directives and procedures are reviewed at least every three years by the Group Cybersecurity Department in coordination with those entities to take into account potential evolutions in standards, context and security needs. Any updates are approved by the CSSI.

4.3. Regulatory and Standards Compliance

- The cybersecurity program incorporates the applicable regulatory and standards-based requirements relating to information systems security and data protection. It aligns with the aforementioned frameworks and the recommendations issued by the competent authorities.
- The Group demonstrates its compliance with applicable regulations and cooperates with regulators in full transparency.
- In conjunction with this Policy, the security of personal data processing is governed by the Group Personal Data Protection Policy, which notably sets out the purposes and methods of data collection, the categories of recipients, how data subjects may exercise their rights (including access, rectification and erasure, subject to applicable legal limits) and the timeframes for handling such requests.

5. Security Measures and Monitoring

To anticipate and respond effectively to cyber threats, the Group deploys a coherent set of preventive, reactive and corrective security measures, ensuring constant vigilance and a proven ability to safeguard its information and associated assets:

5.1. Preventive Security

- The Group applies the principle of defense-in-depth, combining multi-layered security mechanisms (firewalls, intrusion detection systems, antivirus/EDR, network segmentation, strict access rights management, multi-factor authentication, encryption of sensitive data, etc.).

- Security configurations and parameters are defined according to industry best practices to minimize potential attack surfaces.

5.2. Vulnerability Management

- A vulnerability analysis and monitoring process is in place to identify potential weaknesses affecting the Group's assets.
- Vulnerability scans and penetration tests are performed periodically.
- To keep the infrastructure up to date and protected, security patches are applied diligently according to the criticality of the vulnerabilities.

5.3. Maintaining a Secure State

- Systems are continuously monitored to ensure compliance with security guidelines (secure configuration, hardening, account and access rights reviews, etc.).
- Ongoing controls and self-assessments are carried out by the responsible teams, supplemented by periodic tests conducted by the Risk Management Function to ensure that security measures are operating effectively.

5.4. Incident Detection and Response

- The Group has established a security monitoring capability enabling the detection of unusual or malicious events (SIEM, SOC).
- Dedicated incident response teams and procedures are in place: as soon as a security event is detected, an escalation process allows employees to report it without delay.
- If a security incident were to occur, it would be analyzed and handled according to a defined response plan, including communication to governing bodies and, where applicable, notifications to regulators and affected parties.

5.5. Business Continuity and Operations Recovery

- To guard against any major incident, the Group has developed business continuity and IT recovery plans.
- These plans cover severe security incident scenarios and provide for data backup procedures, failover to backup infrastructures and restoration of systems within controlled timeframes.
- Regular tests of these IT contingency plans are carried out to ensure the effectiveness of measures and the preparedness of teams in the event of an actual crisis.

6. Control, Reporting and Continuous Improvement

To effectively manage cybersecurity and adapt to ever-evolving threats, the Group has established a process of control, regular evaluation and continuous improvement that ensures a high level of maturity and transparency:

6.1. Audits

- The Group undergoes regular independent external audits on organizational and technical aspects of cyber risk management based in particular on frameworks such as ISO/IEC 27001/2, the NIST Cybersecurity Framework (NIST CSF), OWASP, the French General Security Baseline (RGS) and the cybersecurity policy of La Banque Postale, its parent company.
- In addition, internal audits of the IT infrastructure and ISMS are regularly carried out to evaluate their compliance with cybersecurity standards and to identify any potential areas for improvement.
- The conclusions from these audits are incorporated into security action plans and their implementation is monitored by the Group Cybersecurity Department.

6.2. Security Reporting

- A reporting system is in place to track performance and risk indicators, as well as any vulnerabilities.
- Each month, the Group Cybersecurity Department prepares a report for the CSSI, including a summary of the main events over the past period and the progress of security initiatives.
- The Group attaches particular importance to transparency with its governance bodies and, when necessary, externally: in the event of a major incident affecting sensitive data, impacted stakeholders and regulatory authorities would be informed in accordance with the company's obligations and commitments.

6.3. Review and Update of the Policy

- To ensure its continuous improvement, the Policy is reviewed by the Group Cybersecurity Department annually or at any time in case of a significant change in the regulatory, security, organizational or technological context. This review aims to ensure that the Policy remains aligned with applicable requirements, state of the art and evolving cyber threats.
- For its part, the CSSI conducts ISMS reviews incorporating audit results and key security indicators. These reviews make it possible to assess the operational effectiveness of implemented measures, evaluate the adequacy of the resources allocated, identify areas for improvement and, where appropriate, approve a security enhancement roadmap.
- Following these reviews, the Policy is updated when justified by the findings. Any significant change is subject to formal approval by the Group Risk Committee (CRG), thereby ensuring the ongoing relevance and continuous adaptation of the ISMS to the state of cyber risks.

**Insuring
a more
open world**

