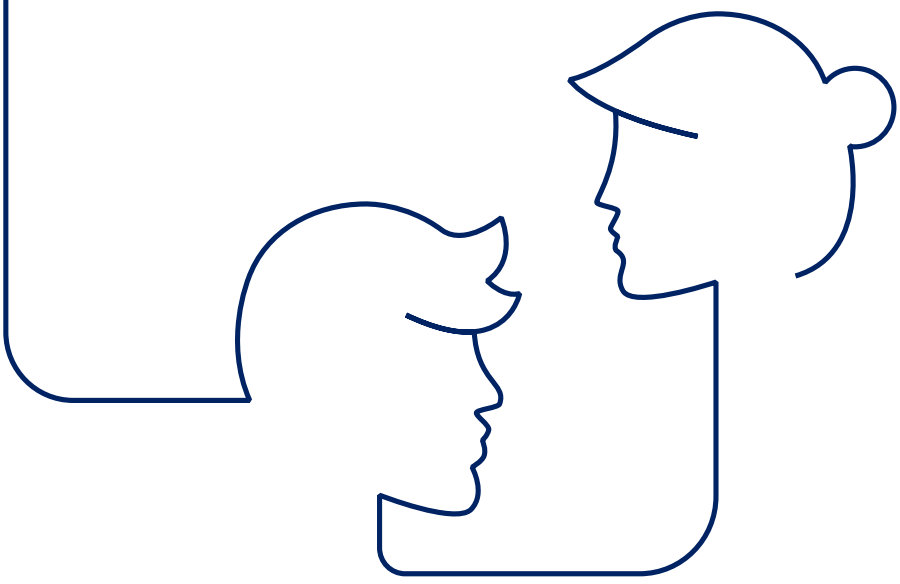
Assurons
un monde
plus ouvert

CNP
assurances

CNP Assurances

Synthèse politique Groupe Cybersécurité

Mai 2026



Version 2

Note introductive

Ce document constitue une version condensée de la politique de cybersécurité du groupe CNP Assurances - GR/DCSG/POL001 (la **« Politique »**). Il s'adresse principalement aux parties prenantes externes et offre un aperçu synthétique des modalités de sécurisation de l'information au sein de chaque entité du groupe CNP Assurances, composé de CNP Assurances Holding et de l'ensemble de ses filiales directes et indirectes (le **« Groupe »**).

1. Objet et portée de la Politique

- Le Groupe accorde une importance stratégique à la cybersécurité afin d'assurer la résilience numérique de ses activités, de se conformer à ses obligations et de conforter la confiance de ses parties prenantes.
- La Politique définit les orientations fondamentales en matière de sécurité de l'information. Elle s'applique à toutes les entités du Groupe, ainsi qu'à son personnel, ses partenaires et prestataires disposant d'un accès à ses données ou systèmes d'information (« SI »).
- Dans le respect des exigences légales et réglementaires applicables, elle vise à garantir la confidentialité, l'intégrité et la disponibilité des informations traitées en s'alignant sur l'état de l'art de la cybersécurité.
- Approuvée lors de sa création par le Comité exécutif (COMEX) et lors de tout changement significatif par le Comité des Risques Groupe (CRG), la Politique est le reflet de la stratégie de cybersécurité supervisée par le Conseil d'administration du Groupe. Elle est revue annuellement pour prendre en compte les évolutions technologiques, normatives, réglementaires et la dynamique constante des menaces cyber.

2. Principes directeurs

La cybersécurité du Groupe repose sur les principes directeurs suivants. Alignés sur les grands standards internationaux, ces principes orientent l'ensemble des actions de protection et assurent une gestion dynamique des risques cyber :

2.1. Approche par les risques et amélioration continue

- Le Groupe s'engage dans une démarche sécuritaire proactive consacrée par la norme ISO/IEC 27001 : « Planifier - Déployer - Contrôler - Agir » (PDCA).
- Des analyses de risques sont continuellement réalisées afin d'identifier, d'évaluer et de traiter efficacement les menaces pesant sur les actifs informationnels et associés.
- Cette approche alimente un processus structuré d'amélioration continue, incluant des contrôles fréquents et des actions de sécurité correctives ou de renforcement tenant compte de l'appétence au risque définie par le Groupe.

2.2. Protection de l'information et des actifs associés

- Le Groupe protège son patrimoine informationnel, ainsi que les systèmes, applications et infrastructures qui le supportent, afin de prévenir toute fuite, altération, indisponibilité ou accès non autorisé aux données.
- Cette protection repose sur des mesures adaptées aux enjeux et aux risques, destinées à garantir la confidentialité, l'intégrité, la disponibilité et la traçabilité des informations tout au long de leur cycle de vie.
- Les principes de *Security by design* et de *Privacy by design* sont intégrés dès les phases de cadrage et de conception des projets. Ils se traduisent par l'identification des besoins de sécurité, la réalisation d'analyses de risques, leur documentation dans les dossiers projet, leur déclinaison en mesures adaptées, ainsi que par la validation des traitements de données à caractère personnel avant leur mise en œuvre, notamment par la conduite d'analyses d'impact relatives à la vie privée lorsque la réglementation l'exige.

2.3. Surveillance et réponse aux menaces

- Une surveillance continue de la sécurité des systèmes et des menaces émergentes est assurée.
- Des mécanismes de détection et d'alerte permettent d'identifier rapidement les évènements, les tentatives d'intrusion ou les activités suspectes.
- Le Groupe dispose d'une capacité de réponse aux incidents de sécurité éprouvée, avec des procédures d'escalade qui permettent de traiter efficacement tout incident cyber et d'en limiter l'impact sur ses activités et sa clientèle.

2.4. Responsabilité partagée et culture de sécurité

- Au sein du Groupe, la sécurité de l'information est l'affaire de tous. Fortement engagés en faveur de la cybersécurité, le Conseil d'administration et le COMEX veillent à ce que chaque collaborateur soit sensibilisé aux règles de protection et à la nécessité de les appliquer au quotidien.
- Un programme continu de sensibilisation et de formation est mis en place afin de développer une véritable culture de sécurité. Tous les collaborateurs suivent obligatoirement une formation annuelle pour connaître les bonnes pratiques et les obligations liées à la sécurité de l'information.

2.5. Gestion du risque tiers

- Le Groupe exige de ses partenaires et intervenants externes un niveau de sécurité adapté aux risques associés à leurs activités, aligné sur ses propres standards lorsqu'ils accèdent à ses systèmes, services ou données.
- Cette exigence s'appuie sur un processus de due diligence, des clauses contractuelles, des plans d'assurance sécurité et des campagnes d'audit de cybersécurité. Par là-même, le Groupe veille notamment à ce que les intervenants externes disposent d'une sensibilisation adaptée aux risques de sécurité des SI, selon une approche proportionnée à la nature de leurs prestations et à leurs conditions d'intervention.

3. Gouvernance, rôle et responsabilités

Une gouvernance claire et structurée constitue le socle d'un dispositif de cybersécurité robuste et efficace. A cet effet, le Groupe s'est doté d'un modèle de gouvernance articulé entre les organes centraux et les entités opérationnelles pour garantir la mise en œuvre homogène de la Politique à tous les niveaux de l'organisation.

3.1. Structure centrale de gouvernance

- Le Conseil d'administration, sur avis de son Comité spécialisé, le Comité d'Audit et des Risques (CAR), valide l'appétence aux risques et la stratégie de cybersécurité du Groupe. Le CAR assure une supervision régulière des enjeux de sécurité des SI et des données. Dans ce cadre, il examine les orientations, les risques majeurs, les incidents éventuels, les indicateurs clés et les plans d'action associés afin d'éclairer le Conseil d'administration dans l'exercice de ses responsabilités.
- Le COMEX porte la responsabilité ultime de la sécurité des SI. Il veille à l'application effective de la Politique et à son intégration dans la stratégie globale du Groupe.
- La RSSI Groupe, en qualité de Responsable de la Direction cybersécurité Groupe, élabore la Politique, pilote la mise en œuvre du dispositif sécuritaire, mesure sa performance et rend compte régulièrement au COMEX et aux Comités spécialisés : Comité de Sécurité des Systèmes d'Information (CSSI), Comité des Risques Groupe (CRG) et Comité d'Audit et des Risques (CAR).
- Afin de garantir le pilotage transverse du dispositif sécuritaire et son adaptation continue, cette gouvernance s'appuie sur des Comités de Sécurité des Systèmes d'Information (CSSI) mensuels, composés notamment des Fonctions clé risques, IT, DPO et de membres du COMEX.
- L'organisation s'inscrit dans un modèle à trois lignes de défense, garantissant la séparation des responsabilités entre mise en œuvre et opérations (1), pilotage et contrôle de second niveau (2), audit indépendant (3) :

    - Regroupant les équipes informatiques et métiers, la première ligne applique les mesures de sécurité dans les activités opérationnelles de l'entreprise. Assurant des fonctions de détection, protection et continuité, l'équipe IT conçoit, déploie et opère des solutions sécuritaires. Garante des dispositifs techniques et de leur maintien en conditions opérationnelles, elle réalise des contrôles de 1er niveau et accompagne les projets en matière de sécurité.
    - Constituée par la Fonction clé risques (incluant la Direction cybersécurité Groupe), la deuxième ligne assure la définition du dispositif, son pilotage et son contrôle. Elle identifie et suit les risques cyber, s'assure du respect des réglementations en lien avec la Direction conformité et réalise des contrôles réguliers sur les dispositifs en place.
    - La troisième ligne correspond à la Direction de l'Audit interne Groupe, qui évalue de manière indépendante et régulière l'efficacité du dispositif de cybersécurité et la bonne implémentation des standards de sécurité applicables. Ses recommandations sont intégrées aux plans d'amélioration continue.

- Les collaborateurs sont tenus de respecter les règles et procédures de sécurité dans leurs activités quotidiennes. Ils sont continuellement sensibilisés et formés aux bonnes pratiques. Tout manquement est analysé, suivi et donne lieu aux actions appropriées (rappel, actions pédagogiques, voire sanction disciplinaire).
- Les partenaires et prestataires doivent se conformer aux exigences de sécurité du Groupe. Des audits et des comités de pilotage de la relation sont menés régulièrement afin de garantir la protection des données et des systèmes concernés.

3.2. Déclinaison opérationnelle au niveau des entités

- Dans le respect des orientations définies par la Direction cybersécurité Groupe, chaque entité décline opérationnellement la présente Politique selon ses propres spécificités.
- Dans ce cadre, toute entité est responsable d'établir une gouvernance locale alignée sur le modèle central, d'intégrer les exigences de cybersécurité dans ses activités, de conduire des analyses de risques adaptées à son contexte, de sensibiliser ses collaborateurs et de participer au dispositif centralisé de détection, réponse et reporting des évènements sécuritaires.
- La Direction cybersécurité Groupe supervise cette déclinaison par un accompagnement méthodologique, une animation régulière du réseau des correspondants sécurité, ainsi qu'un contrôle continu pour garantir l'homogénéité, la cohérence et l'efficacité du dispositif de cybersécurité dans son ensemble.

4. Cadre de gestion des risques et conformité

Un programme de cybersécurité, couvrant l'ensemble des dimensions nécessaires à une protection robuste, est mis en œuvre de façon continue. Aligné sur les grands référentiels de sécurité (ISO, NIST, CIS, OWASP, etc. …), ce programme garantit un traitement cohérent des risques et un cadre d'amélioration permanente. Les processus implémentés incluent notamment :

4.1. Analyse et traitement des risques

- Les données et les SI associés sont inventoriés et font l'objet d'analyses régulières de sécurité.
- Une cartographie des risques est maintenue et des plans de traitement sont mis en œuvre pour atténuer les risques identifiés conformément à la tolérance définie par le Groupe.

4.2. Référentiel interne de sécurité

- La Politique est déclinée en directives et procédures opérationnelles couvrant l'ensemble des domaines clés : gouvernance, classification des actifs, gestion des accès, sécurité des données et des applications, protection des réseaux, gestion des évènements sécuritaires, continuité d'activité, conformité, etc.
- Ces documents fournissent aux équipes des instructions à suivre pour mettre en œuvre la sécurité au quotidien. Mis à la disposition des entités, le référentiel interne constitue un socle commun de sécurité élevé.
- Les directives et procédures sont revues a minima tous les 3 ans par la Direction cybersécurité Groupe en lien avec lesdites entités pour prendre en compte l'évolution potentielle des normes, contextes et besoins de sécurité. Leur mise à jour est approuvée par le CSSI.

4.3. Conformité réglementaire et normative

- Le programme de cybersécurité intègre les exigences réglementaires et normatives applicables en matière de sécurité des SI et de protection des données. Il s'aligne sur les référentiels précités et les recommandations des autorités compétentes.
- Le Groupe démontre sa conformité aux lois et règlements en vigueur et collabore avec les régulateurs en toute transparence.
- En articulation avec la présente Politique, les modalités de sécurisation des traitements de données personnelles sont régies par la politique de protection des données à caractère personnel du Groupe, qui décrit notamment les finalités et les moyens de collecte, les catégories de destinataires, les conditions d'exercice des droits des personnes concernées (dont l'accès, la rectification et l'effacement dans les limites prévues par la réglementation), ainsi que les délais de traitement des demandes.

5. Mesures de sécurité et surveillance

Pour anticiper et répondre efficacement aux cybermenaces, le Groupe déploie un ensemble cohérent de mesures de sécurité préventives, réactives et correctives, assurant une vigilance permanente et une capacité démontrée à préserver ses actifs informationnels et associés :

5.1. Sécurité préventive

- Le Groupe applique le principe de défense en profondeur, combinant des mécanismes de sécurité à plusieurs niveaux (pare-feu, systèmes de détection d'intrusion, antivirus/EDR, segmentation réseau, gestion de droits d'accès stricts, authentification multi-facteurs, chiffrement des données sensibles, etc.).
- Les configurations et paramètres de sécurité sont définis selon l'état de l'art afin de réduire au maximum les éventuelles surfaces d'attaque.

5.2. Gestion des vulnérabilités

- Un processus d'analyse et de veille de vulnérabilités est en place pour identifier les failles potentielles affectant les actifs du Groupe.
- Des scans de vulnérabilités et des tests d'intrusion sont réalisés périodiquement.
- Afin de maintenir l'infrastructure à jour et protégée, les correctifs de sécurité sont appliqués de manière diligente en fonction de la criticité des vulnérabilités en présence.

5.3. Maintien en conditions de sécurité

- Les systèmes font l'objet d'un suivi continu pour vérifier le respect des directives de sécurité (configuration sécurisée, durcissement, revues de comptes et de droits, etc.).
- Des contrôles permanents et auto-évaluations sont effectués par les équipes en charge, complétés par des tests périodiques menés par la Fonction clé risques pour s'assurer que les mesures de sécurité fonctionnent efficacement.

5.4. Détection et réponse aux incidents

- Le Groupe s'est doté d'une capacité de supervision de la sécurité permettant de détecter les événements inhabituels ou malveillants (SIEM, SOC).
- Des équipes et procédures dédiées de réponse à incident sont en place : dès qu'un évènement de sécurité est détecté, un processus d'escalade permet aux collaborateurs de le signaler sans délai.
- Dans le cas où un incident de sécurité se produirait, il serait analysé et traité selon un plan de réponse défini, incluant la communication aux instances dirigeantes et, le cas échéant, la notification aux régulateurs et personnes concernées.

5.5. Continuité d'activité et reprise des opérations

- Afin de se prémunir contre tout sinistre majeur, le Groupe a développé des plans de continuité d'activité et de reprise informatique.
- Ces plans couvrent des scénarios d'incident grave de sécurité et prévoient des procédures de sauvegarde des données, de bascule sur des infrastructures de secours et de rétablissement des systèmes dans des délais maîtrisés.
- Des tests réguliers de ces plans de secours informatiques sont réalisés afin de garantir l'efficacité des mesures et la préparation des équipes pour le cas où une crise réelle se produirait.

6. Contrôle, reporting et amélioration continue

Pour piloter efficacement la cybersécurité et s'adapter aux menaces en perpétuelle évolution, le Groupe a établi un processus de contrôle, d'évaluation régulière et d'amélioration continue garantissant un haut niveau de maturité et de transparence :

6.1. Audits

- Le Groupe fait continuellement l'objet d'audits externes indépendants sur des aspects organisationnels et techniques de gestion des risques cyber, fondés notamment sur des référentiels tels que ISO/IEC 27001/2, NIST CSF, OWASP, le référentiel général français de sécurité (RGS) ou encore la politique cyber de La Banque Postale, sa société mère.
- En complément, des audits internes de l'infrastructure IT et du dispositif de sécurité sont régulièrement accomplis, afin d'en évaluer la conformité aux standards de cybersécurité et d'identifier d'éventuels axes de renforcement.
- Les conclusions de ces audits sont intégrées aux plans d'actions sécuritaires et leur mise en œuvre est suivie par la Direction cybersécurité Groupe.

6.2. Reporting de sécurité

- Un dispositif de reporting permet de suivre des indicateurs de performance et de risques, ainsi que d'éventuelles vulnérabilités.
- La Direction cybersécurité Groupe établit mensuellement un rapport à destination du CSSI incluant un bilan des principaux évènements sur la période écoulée et l'avancement des initiatives de sécurité.
- Le Groupe attache une importance particulière à la transparence vis-à-vis des instances de gouvernance et, lorsque nécessaire, vis-à-vis de l'externe : en cas d'incident majeur affectant des données sensibles, les parties prenantes impactées et les autorités réglementaires seraient informées conformément aux obligations et aux engagements de l'entreprise.

6.3. Revue et mise à jour de la Politique

- Afin d'assurer son amélioration continue, la Politique est revue par la Direction cybersécurité Groupe annuellement ou à tout moment en cas d'évolution significative du contexte réglementaire, sécuritaire, organisationnel ou technologique. Cette revue vise à s'assurer que la Politique demeure alignée avec les exigences applicables, l'état de l'art et l'évolution des menaces cyber.

- Pour sa part, le CSSI réalise des revues du dispositif intégrant notamment les résultats des audits et les indicateurs clés de sécurité. Ces revues permettent d'évaluer l'efficacité opérationnelle des mesures implémentées, d'apprécier l'adéquation des moyens alloués, d'identifier des axes d'amélioration et le cas échéant d'approuver une feuille de route de renforcement sécuritaire.
- A l'issue de ces revues, la Politique est mise à jour lorsque les constats réalisés le justifient. Tout changement significatif fait l'objet d'une approbation formelle par le Comité des Risques Groupe (CRG), garantissant ainsi la pertinence et l'adaptation permanente du dispositif à l'état des risques cyber.

Assurons
un monde
plus ouvert

CNP Assurances – Siège social : 4 promenade Cœur de Ville 92130 Issy-les-Moulineaux – 01 42 18 88 88 – www.cnp.fr
Société anonyme au capital de 686 618 477 euros entièrement libéré – 341 737 062 RCS Nanterre
Entreprise régie par le code des assurances – IDU EMP FR231782_01ZWUC