Politique en matière de sécurité et de cybersécurité des systèmes d'information

Politiques corporatives 2025

Table des matières

01

Objet

La présente Politique en matière de sécurité et de cybersécurité des systèmes d'information (ci-après dénommée « la Politique »), qui fait partie de la Politique-cadre de conformité, a pour objectif de définir et de divulguer les fondements et les règles générales de Konecta, groupe multinational de sociétés spécialisées dans la fourniture de services et de solutions numériques de gestion de la relation client (ci-après dénommé « Konecta », « l'Entreprise », « la Société » ou « la Compagnie »), afin de garantir l'intégrité, la confidentialité et la sécurité des informations, conformément à la législation en vigueur en la matière, en évaluant les risques et en assurant une utilisation efficace des ressources, le tout sur la base de critères de proportionnalité dans la gestion.

L'utilisation massive des technologies de l'information et des télécommunications (TIC) dans tous les domaines de la société a créé un nouvel espace, le cyberespace, où des conflits et des agressions peuvent se produire, et où il existe des cybermenaces qui peuvent nuire à Konecta et à ses différentes sociétés.

La présente Politique établit un cadre de référence qui pose les principes visant à assurer la protection des systèmes d'information de Konecta contre les accès non autorisés, les pertes ou les dommages lors du traitement des informations et autres types de cybermenaces, garantissant ainsi la disponibilité, l'intégrité et la confidentialité des informations et des données gérées par Konecta.

Cette Politique est conçue pour établir le cadre de référence pour les parties prenantes internes de Konecta (employés, actionnaires, investisseurs, dirigeants) et externes (clients, fournisseurs, auditeurs, gouvernements, organismes de réglementation, médias, concurrents et institutions financières), de sorte à renforcer la confiance dans les systèmes d'information de l'Entreprise tout en veillant au respect scrupuleux de la réglementation en vigueur dans tous les pays, des exigences propres et des normes internationales.

Cette Politique sera affichée sur le site web de l'entreprise (Konecta.com) de sorte à ce toutes les parties prenantes puissent la consulter.

02

Champ d'application

La présente Politique s'inscrit dans le champ d'application de la Politique-cadre de conformité. Elle s’applique à toutes les entités de Konecta et elle est soutenue par la direction générale de l'Entreprise.

Par conséquent, cette Politique est à respecter par tous les employés de Konecta, indépendamment du poste ou des fonctions qu’ils exercent au sein de l'organisation ou de leur situation géographique.

Sans préjudice de ce qui précède, son champ d'application peut être élargi, si cela s’avère nécessaire et possible eu égard à la nature de la relation, à toutes les personnes physiques et/ou morales liées à Konecta sur le plan commercial ou professionnel, par une relation autre que celle relevant du droit du travail : fournisseurs, sous-traitants et travailleurs de la chaîne d'approvisionnement, et partenaires commerciaux.

Étant donné que de nombreuses sociétés de Konecta ont leur siège social en dehors de l'Union européenne, la réglementation interne sera adaptée à la réglementation propre à chaque État, tout en respectant et en garantissant les principes fondamentaux énoncés ici.

03

Principes généraux d'action

La Politique en matière de sécurité et de cybersécurité des systèmes d'information traduit l'engagement explicite de l'Entreprise à définir et à établir les lignes directrices et le soutien appropriés pour la gestion de la sécurité des informations qu'elle traite, conformément à ses propres exigences et aux lois et réglementations en vigueur.

Konecta veille à garantir « une utilisation sûre des réseaux et des systèmes d'information en renforçant nos capacités de prévention, de défense, de détection, d'analyse, d'enquête, de récupération et de réponse face aux cyberattaques » qui pourraient se produire.

Konecta mise sur une utilisation sécurisée des systèmes d'information et des télécommunications, tout en restant en phase avec la stratégie et les objectifs de l'Entreprise. Dans cette optique, elle s'est fixée les objectifs spécifiques suivants, cohérents par rapport au contexte dans lequel l'Entreprise mène ses activités:

- Promouvoir la sécurité et la résilience des réseaux et des systèmes d'information utilisés.
- Sensibiliser l'ensemble du personnel de l'Entreprise aux risques liés au cyberespace.
- Former et maintenir les connaissances, les compétences, l'expérience et les capacités technologiques nécessaires pour soutenir les objectifs de Konecta en matière de cybersécurité.

À cet égard, Konecta s'engage à atteindre les objectifs suivants:

- Considérer les informations et les systèmes qui les supportent comme des actifs stratégiques. Konecta exprime ainsi sa détermination à atteindre les niveaux de sécurité requis pour garantir les exigences de confidentialité, d'intégrité et de disponibilité des informations traitées au sein de l'organisation et des ressources des systèmes d'information qui les traitent, les stockent ou les distribuent.
- Veiller à la divulgation de la réglementation définie au soutien de cette Politique, de sorte à inculquer au personnel de Konecta un niveau de sensibilisation et de formation en matière de sécurité de l'information qui garantisse l'application de pratiques appropriées dans ce domaine, en tant qu'élément essentiel à l'exercice de leurs fonctions.
- Promouvoir la mise en place des niveaux de sécurité de l'information requis, dans le cadre d'un processus permanent d'amélioration et de progrès constants, fondé sur la définition des objectifs et des exigences à respecter, la mise en œuvre des processus et mesures appropriés, la vérification de leur efficacité, de leur efficience et de leur performance, et l'adoption des corrections et modifications jugées appropriées.
- La présente Politique doit être le principal outil permettant de garantir de manière adéquate la sécurité de l'information, notamment en encourageant et en assurant son respect au sein des différents services.
- Veiller à l'opérationnalité des mécanismes nécessaires pour assurer la continuité des activités critiques de l'entreprise qui reposent sur les systèmes d'information afin de garantir leur récupération dans un délai acceptable.
- Maximiser la qualité des services fournis.
- Réduire ou éliminer autant que possible les dangers et les risques liés aux actifs, aux processus et aux services fournis par Konecta.

- Édicter les mesures essentielles de sécurité de l'information que Konecta doit adopter pour se protéger de manière appropriée contre les menaces susceptibles de nuire à un degré ou un autre à la confidentialité, à l'intégrité et à la disponibilité de l'information.

Les objectifs de la présente Politique sont mis en œuvre sur la base d'une stratégie à long terme. Les activités visant à atteindre ces objectifs doivent être maintenues dans le temps.

En ce qui concerne les risques liés à la sécurité, les plans d'action doivent être définis et ajustés chaque année (contrôles de sécurité, définition des projets de sécurité, surveillance continue, etc.).

Les plans de transition nécessaires sont mis en place afin de réduire tout impact sur les activités et/ou les ressources de Konecta. En outre, celle-ci veille à ce que les employés:

- ... connaissent et appliquent les procédures internes et les protocoles en matière de sécurité de l'information de Konecta.
- ... disposent d'outils leur permettant d'accéder facilement aux procédures opérationnelles internes (Intranet). De plus, des canaux de communication alternatifs seront mis en place pour communiquer certains processus, mesures spéciales ou mises à jour des procédures.
- ... soient conscients qu'ils ne doivent traiter que les informations pour lesquelles ils ont été autorisés et utiliser les actifs de Konecta uniquement dans le cadre de l'exercice de leurs fonctions professionnelles. Les employés doivent se conformer aux règles de base d'accès aux applications et/ou aux équipements donnant accès aux données à caractère personnel.
- ... connaissent les procédures existantes dans l'entreprise afin de savoir comment agir face à toutes actions ou menaces susceptibles de mettre en péril la sécurité des informations, et sachent qu'ils doivent informer de celles-ci au service Technologie et au Directeur de la sécurité (CISO).

Dans le constat que chacun des pays dans lesquels l'entreprise opère présente un contexte social et des besoins spécifiques, la présente Politique se conjugue sous forme de plans et d'actions conformes aux principes y énoncés et adaptés à la réalité de chacun de ces territoires.

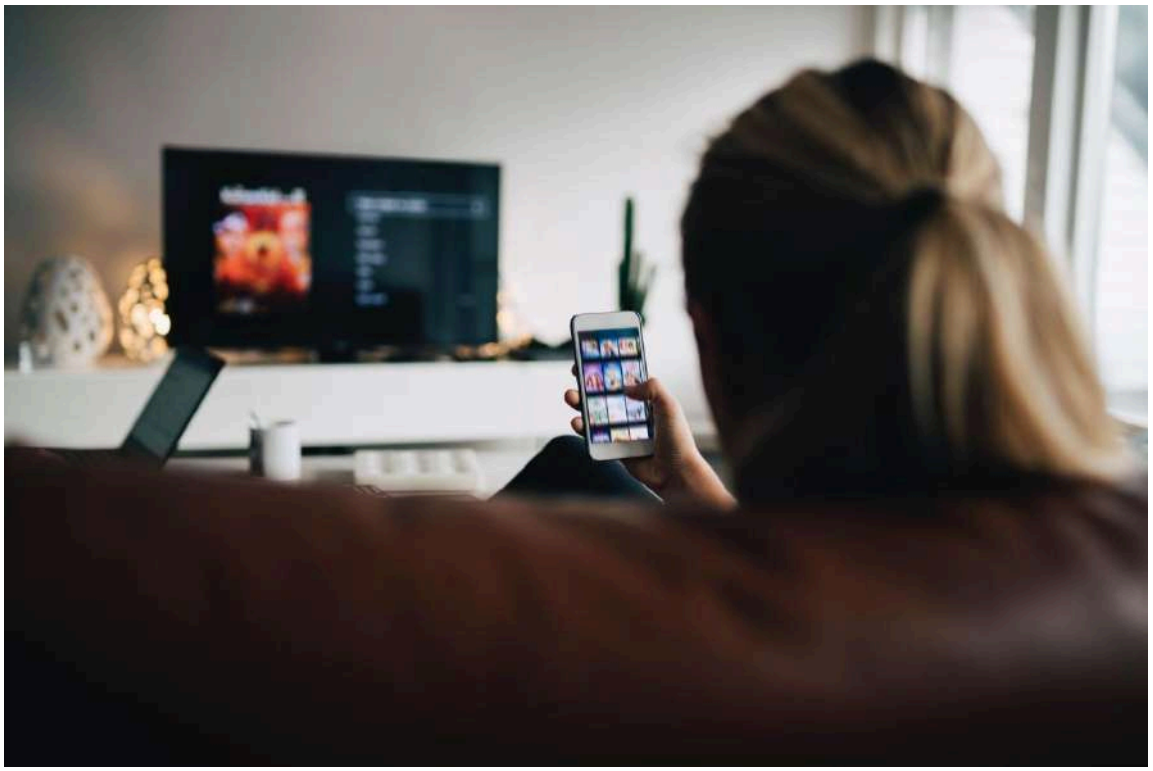
Ces principes d'action répondent aux impacts, risques et opportunités (IRO) découlant des thématiques matérielles concernées : sécurité de l'information, transformation numérique, conformité et éthique d'entreprise, et gestion des fournisseurs.

Les travailleurs et les tiers qui soupçonnent ou ont connaissance d'un éventuel manquement, quel qu'il soit, à la présente Politique ou au Code d'éthique, peuvent transmettre leurs informations, leurs doutes ou leurs craintes à cet égard, de manière confidentielle et sans crainte de représailles, par le biais des Canaux d'information disponibles sur le site web de Konecta (https://Konecta.integrityline.com), conformément à la procédure PG COR 26 Canaux d'information, disponible sur le même site, qui précise les différents canaux disponibles et la nature des communications qui peuvent être effectuées par leur intermédiaire.

Ce canal est disponible 24 heures sur 24, 7 jours sur 7. Aucune mesure de représailles ne sera tolérée à l'encontre de quiconque ayant signalé, de bonne foi, des faits susceptibles de constituer une violation de la présente Politique, et les garanties et

protections prévues par la réglementation et la loi applicables seront appliquées aux auteurs de ces communications.

Les mesures disciplinaires pertinentes seront prononcées en cas de violation de la présente Politique, conformément aux règlements internes, sans préjudice des sanctions administratives ou pénales qui, le cas échéant, seraient prononcées par l'autorité compétente au motif d’une telle violation.



04

Mise à jour et révision

La présente Politique établit les bases de la conformité aux normes suivantes:

- ISO/IEC 27001:2022 Technologies de l'information - Techniques de sécurité - Systèmes de management de la sécurité de l'information - Exigences.
- ISO/IEC 27701 - Extension de la norme ISO 27001 en matière de management de la sécurité de la vie privée.
- ISO/IEC 27002:2022 Technologies de l'information - Techniques de sécurité - Code de bonnes pratiques pour les contrôles de sécurité de l'information.
- Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (Règlement général sur la protection des données) (Texte pertinent aux fins de l'EEE).
- Lois en matière de protection des données à caractère personnel applicables dans chaque pays.

La Politique en matière de sécurité et de cybersécurité des systèmes d'information est révisée et mise à jour périodiquement ainsi que toutes fois que nécessaire, afin de l'adapter aux changements du modèle d'entreprise, ou susceptibles de se produire dans le domaine d'activité de Konecta ou à la suite de l'adoption de réglementations directement applicables, afin d'en garantir l'efficacité et la conformité.

REMARQUE: la présente Politique a été révisée et approuvée le 16 décembre 2025 par la plus haute instance dirigeante et remplace toute version antérieure de celle-ci, le présent document étant le seul valable à compter de ladite date.

Contrôle des versions

Version	Date de révision	Révisé	Validé	Approuvé	Motif de la modification
2	22/06/2021	IT_Sécurité de l'information Organisation et Procédures	Direction Juridique	Conseil d'administration	Révision générale de la politique
3	19/12/2022	IT_Sécurité de l'information Organisation et Procédures	Direction Juridique	Conseil d'administration	Révision générale de la politique
4	16/12/2025	IT_Sécurité de l'information Organisation et Procédures	Direction Juridique	Conseil d'administration	Adaptation aux exigences légales Adaptation au nouveau format et à l'image de marque