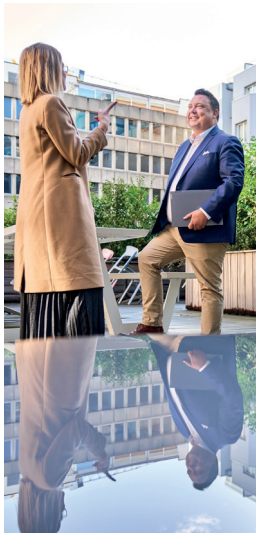
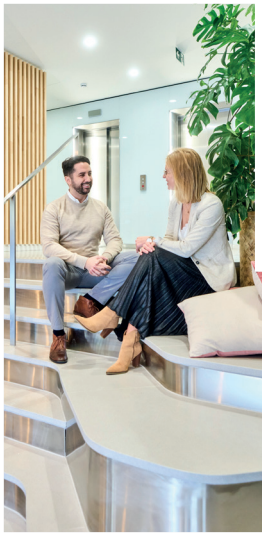
Cofinimmo

together in real estate

POLITIQUE EN MATIÈRE DE CYBERSECURITÉ





Document finalisé le 18.12.2025

Dernière mise à jour le 15.12.2025

Rédigé à l'origine en anglais

POLITIQUE EN MATIÈRE DE CYBERSECURITÉ

CONTENU

I. COMPÉTENCE, DIFFUSION ET ÉVALUATION

1 Diffusion et disponibilité

Ce document est public et sera diffusé auprès de toutes les parties prenantes concernées.

2 Contrôle et maintenance

Cette politique, ainsi que tous les documents et procédures connexes, sont révisés chaque année ou lorsque des changements importants interviennent dans la structure organisationnelle, la technologie ou les exigences légales. Des mises à jour et des améliorations sont apportées afin de garantir que la politique reste conforme aux meilleures pratiques et aux exigences légales.

II. OBJECTIF ET CHAMP D'APPLICATION

1 Objectif

L'organisation (voir paragraphe 4 ci-dessous) reconnaît l'importance cruciale de la protection des sources d'information dans la poursuite de ses objectifs d'entreprise. Dans un environnement où les systèmes d'information sont de plus en plus interconnectés et disponibles, le risque d'attaques hostiles, de perte ou d'exposition des données n'a jamais été aussi élevé. La présente politique de cybersécurité définit les exigences minimales en matière de gouvernance pour tous les départements et entités de l'organisation, afin de garantir la protection de la propriété intellectuelle, de l'avantage commercial et de notre personnel contre les conséquences d'une sécurité de l'information insuffisante et des cyberattaques.

Une attention particulière est également accordée au respect des lois et réglementations.

Ce document fait partie d'une série de documents stratégiques qui aident l'organisation à élaborer une stratégie solide en matière de cybersécurité.

2 Champ d'application

Cette politique s'applique à toutes les informations et à tous les systèmes d'information gérés par l'organisation, y compris, mais sans s'y limiter :

- Les systèmes et sources d'information fournis ou entretenus par l'organisation ;
- Les personnes internes et externes qui traitent les informations organisationnelles ;
- Tous les appareils et terminaux utilisés pour le traitement de l'information ;
- Les procédures et processus soutenant la gestion de l'information ;
- Les sites physiques et virtuels où sont menées les activités organisationnelles ;
- Tous les autres éléments susceptibles de présenter un risque pour la cybersécurité.

Les informations ou systèmes critiques et confidentiels sont des informations ou des systèmes dont la confidentialité, l'intégrité ou la disponibilité causeraient un préjudice considérable à l'organisation si elles étaient compromises.

> *Dans un environnement où les systèmes d'information sont de plus en plus interconnectés et disponibles, le risque d'attaques hostiles, de perte ou d'exposition des données n'a jamais été aussi élevé.*

III. DEFINITIONS

Termes spécifiques et abréviations utilisés dans le présent document

Terme	Description
L'Organisation	Toutes les sociétés et filiales du groupe Cofinimmo
Information Security Manager	Head of IT ou equivalent désigné (supportit@cofinimmo.be)
Sous-traitants	Personnes ou entités externes engagées par l'organisation pour traiter des informations organisationnelles ou avoir accès à des systèmes d'information et qui doivent se conformer aux mêmes mesures, formations et programmes de sensibilisation en matière de cybersécurité que les employés.
Confidentialité	Propriété selon laquelle les informations ne sont pas mises à la disposition ou divulguées à des personnes, entités ou processus non autorisés[1].
Intégrité	Caractéristique d'exactitude et d'exhaustivité, ce qui signifie que les données n'ont pas été modifiées, détruites ou perdues de manière non autorisée ou accidentelle[1].
Beschikbaarheid	Caractéristique selon laquelle les informations sont accessibles et utilisables à la demande d'une entité autorisée[1].

IV. DÉCLARATIONS POLITIQUES

1 Gouvernance et responsabilités

Les rôles et responsabilités en matière de cybersécurité sont clairement définis et communiqués à toutes les parties prenantes internes et externes. Le Information Security Manager est chargé de faire respecter cette politique, de donner des conseils et de garantir sa mise en œuvre dans l'ensemble de l'organisation. La direction générale approuve et soutient cette politique, tous les cadres supérieurs et responsables étant chargés de veiller à son respect au sein de leurs départements respectifs. Des évaluations et des mises à jour sont effectuées régulièrement, au moins une fois par an ou plus souvent si nécessaire.

2 Principes politiques

- Des directives et procédures efficaces sont mises en place et appliquées, avec une prise de conscience claire des risques liés à la sécurité de l'information au sein de l'organisation.
- L'organisation tient à jour un inventaire de tous les équipements physiques, systèmes et logiciels afin de garantir leur disponibilité et leur intégrité continues.
- Des mesures de sécurité, telles que des solutions antivirus et anti-malware, sont mises en œuvre et maintenues sur tous les systèmes et terminaux concernés ;
- Le réseau de l'entreprise est protégé conformé-

1 Source: ISO27000:2018 Overview and Vocabulary (https://standards.iso.org/ittf/PubliclyAvailableStandards/c073906_ISO_IEC_27000_2018_E.zip)

ment à la politique de sécurité du réseau, grâce à des correctifs réguliers et à la gestion des vulnérabilités ;
- La gestion des accès respecte les principes d'accès minimal et d'authentification multiple, tels que décrits dans la politique d'accès et de mot de passe ;
- Des formations et des programmes de sensibilisation sont régulièrement proposés aux employés et aux sous-traitants, notamment une communication sur les 10 règles d'or de l'organisation en matière de cybersécurité[2];
- Des processus de sauvegarde, de reprise après sinistre et de réponse aux incidents sont en place pour garantir la continuité des activités et le respect des obligations légales et réglementaires ;
- Tous les incidents de sécurité réels ou présumés doivent être immédiatement signalés au Information Security Manager afin qu'il puisse mener une enquête approfondie et prendre les mesures qui s'imposent.

Toutes les directives, procédures et contrôles font l'objet d'un processus d'amélioration continue, au cours duquel ils sont adaptés aux changements intervenant dans l'organisation et son environnement de risque.

3 Exigences légales et réglementaires

L'organisation s'engage à identifier, évaluer et mettre en œuvre toutes les exigences légales et réglementaires applicables en matière d'information et de cybersécurité. Ce processus comprend la tenue d'un registre à jour des lois, obligations légales et réglementations sectorielles pertinentes qui s'appliquent au traitement, au stockage et à la gestion des sources d'information.

Des évaluations sont régulièrement effectuées afin de rester en conformité avec les cadres juridiques en constante évolution, tels que la législation en matière de protection des données, de confidentialité et de cybersécurité. Le Information Security Manager est chargé de suivre l'évolution de la réglementation et de veiller à ce que les contrôles, procédures et documents nécessaires soient immédiatement mis à jour en réponse à des exigences nouvelles ou modifiées. En ce qui concerne la réglementation RGPD, l'équipe chargée de la confidentialité est responsable du suivi des modifications réglementaires et de la mise en œuvre des mises à jour pertinentes dans les contrôles et la documentation de l'organisation. Si nécessaire, l'organisation sollicite de manière proactive des conseils juridiques spécialisés afin d'interpréter et de respecter les obligations complexes, tout en garantissant que tous les employés reçoivent des conseils appropriés grâce à des formations et des communications ciblées.

« Des évaluations sont régulièrement effectuées afin de rester en conformité avec les cadres juridiques en constante évolution, tels que la législation en matière de protection des données, de confidentialité et de cybersécurité.

2 Partie intégrante du programme de sensibilisation à la cybersécurité : ensemble complet de directives et de bonnes pratiques visant à améliorer les pratiques de cybersécurité pour les personnes au sein de l'organisation.