Cofinimmo

together in real estate

CYBERSECURITY BELEID

Document gefinaliseerd op 18.12.2025.
Laatst bijgewerkt op 15.12.2025.
Oorspronkelijk geschreven in het Engels.

CYBERSECURITY BELEID

INHOUD

I. BEVOEGDHEID, VERSPREIDING EN BEOORDELING

1 Verspreiding en beschikbaarheid

Dit document is openbaar en wordt verspreid onder alle relevante stakeholders.

2 Controle en onderhoud

Dit beleid, samen met alle ondersteunende documenten en procedures, wordt jaarlijks herzien of wanneer er belangrijke veranderingen plaatsvinden in de organisatiestructuur, technologie of wettelijke vereisten. Er worden updates en verbeteringen doorgevoerd om ervoor te zorgen dat het beleid blijft aansluiten bij de best practice en wettelijke vereisten.

II. DOEL EN TOEPASSINGSVELD

1 Doel

De organisatie (zie paragraaf 4 hieronder) erkent het cruciale belang van het beschermen van informatiebronnen bij het nastreven van haar bedrijfsdoelstellingen. In een omgeving waarin informatiesystemen steeds meer met elkaar verbonden en beschikbaar zijn, is het risico op vijandige aanvallen, gegevensverlies of blootstelling nog nooit zo groot geweest. Dit cybersecuritybeleid stelt de minimale governancevereisten vast voor alle afdelingen en entiteiten binnen de organisatie, om de bescherming van intellectuele eigendom, commercieel voordeel en van onze mensen te waarborgen tegen de gevolgen van een zwakke informatiebeveiliging en cyberaanvallen.

Er wordt ook voldoende aandacht besteed aan de naleving van wet- en regelgeving.

Dit beleidsdocument maakt deel uit van een reeks beleidsdocumenten die de organisatie ondersteunen bij het opstellen van een gedegen cybersecuritystrategie.

2 Toepassingsveld

Dit beleid is van toepassing op alle informatie en informatiesystemen die door de organisatie worden beheerd, met inbegrip van maar niet beperkt tot:

- Informatiesystemen en -bronnen die door de organisatie worden geleverd of onderhouden;
- Interne en externe personen die organisatorische informatie verwerken;
- Alle toestellen en eindpunten die worden gebruikt voor informatieverwerking;
- Procedures en processen ter ondersteuning van informatiebeheer;
- Fysieke en virtuele locaties waar organisatorische activiteiten worden uitgevoerd;
- Alle overige elementen die een cybersecurityrisico kunnen vertonen.

Kritieke en vertrouwelijke informatie of systemen zijn informatie of systemen waarvan de vertrouwelijkheid, integriteit of beschikbaarheid, indien aangetast, de organisatie aanzienlijke schade zou berokkenen.

> *In een omgeving waarin informatiesystemen steeds meer met elkaar verbonden en beschikbaar zijn, is het risico op vijandige aanvallen, gegevensverlies of blootstelling nog nooit zo groot geweest.*

III. DEFINITIES

Specifieke termen en afkortingen die in dit document worden gebruikt

Term	Beschrijving
De organisatie	Alle vennootschappen en dochtervennootschappen van de Cofinimmo-groep
Information Security Manager	Head of IT of aangesteld equivalent (supportit@cofinimmo.be)
Onderaannemers	Externe personen of entiteiten die door de organisatie worden ingeschakeld om organisatorische informatie te verwerken of toegang hebben tot informatiesystemen en die zich moeten houden aan dezelfde cybersecuritymaatregelen, -opleidingen en -bewustmakingsprogramma's als de werknemers.
Vertrouwelijkheid	Eigenschap dat informatie niet beschikbaar wordt gesteld of bekendgemaakt wordt aan onbevoegde personen, entiteiten of processen[1].
Integriteit	Eigenschap van nauwkeurigheid en volledigheid, wat betekent dat gegevens niet op ongeoorloofde of onopzettelijke wijze gewijzigd of vernietigd werden of verloren gingen[1].
Beschikbaarheid	Eigenschap dat informatie op verzoek toegankelijk en bruikbaar is voor een bevoegde entiteit[1].

IV. BELEIDSVERKLARINGEN

1 Bestuur en verantwoordelijkheden

De rollen en verantwoordelijkheden op het vlak van cybersecurity zijn duidelijk omschreven en worden aan alle interne en externe stakeholders meegedeeld. De Information Security Manager is verantwoordelijk voor het handhaven van dit beleid, het geven van advies en het waarborgen van de uitvoering ervan binnen de hele organisatie. Het senior management onderschrijft en ondersteunt dit beleid, waarbij alle C-levels en managers verantwoordelijk zijn voor de naleving ervan binnen hun respectieve afdelingen. Er worden regelmatig evaluaties en updates uitgevoerd, minimaal eenmaal per jaar of vaker indien nodig.

2 Beleidsprincipes

- Er worden effectieve richtlijnen en procedures opgesteld en gehandhaafd, waarbij men zich duidelijk bewust is van de risico's op het vlak van informatiebeveiliging binnen de organisatie;
- De organisatie houdt een geüpdatete inventaris bij van alle fysieke toestellen, systemen en software, om de voortdurende beschikbaarheid en integriteit ervan te waarborgen;
- Beveiligingsmaatregelen, zoals antivirus- en antimalwareoplossingen, worden op alle relevante systemen en eindpunten geïmplementeerd en onderhouden;
- Het bedrijfsnetwerk wordt in overeenstemming

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

met het netwerkbeveiligingsbeleid beschermd met regelmatige patching en kwetsbaarheidsbeheer;
- Toegangsbeheer handhaaft de principes van minimale toegang en meervoudige authenticatie, zoals beschreven in het toegangs- en wachtwoordbeleid;
- Er worden regelmatig trainingen en bewustwordingsprogramma's aan medewerkers en onderaannemers aangeboden, waaronder communicatie over de 10 gouden regels van de organisatie voor cybersecurity[2];
- Er zijn processen voor back-up, noodherstel en incidentrespons, die de bedrijfscontinuïteit en naleving van wettelijke en regelgevende verplichtingen waarborgen;
- Alle daadwerkelijke of vermoedelijke beveiligingsincidenten moeten onmiddellijk worden gemeld aan de Information Security Manager voor grondig onderzoek en respons.

Alle richtlijnen, procedures en controles zijn onderhevig aan een proces van voortdurende verbetering, waarbij ze worden aangepast aan veranderingen in de organisatie en haar risico-omgeving.

3 Wettelijke en regelgevende vereisten

De organisatie zet zich in voor het identificeren, beoordelen en implementeren van alle toepasselijke wettelijke en regelgevende vereisten met betrekking tot informatie en cybersecurity. Dit proces omvat het bijhouden van een actueel register van relevante wetten, wettelijke verplichtingen en sectorspecifieke voorschriften die van toepassing zijn op de omgang met en de opslag en verwerking van informatiebronnen.

Er worden regelmatig beoordelingen uitgevoerd om te blijven voldoen aan veranderende wettelijke kaders, zoals wetgeving op het vlak van gegevensbescherming, privacy en cybersecurity. De Information Security Manager heeft tot taak de ontwikkelingen inzake regelgeving te volgen en ervoor te zorgen dat de nodige controles, procedures en documentatie onmiddellijk worden bijgewerkt in reactie op nieuwe of gewijzigde vereisten. Met betrekking tot de AVG-regelgeving is het privacy team verantwoordelijk voor het monitoren van wijzigingen in de regelgeving en het doorvoeren van relevante updates in de controles en documentatie van de organisatie. Indien nodig zoekt de organisatie proactief deskundig juridisch advies om complexe verplichtingen te interpreteren en na te komen, waarbij wordt gegarandeerd dat alle medewerkers passende begeleiding krijgen door middel van gerichte trainingen en communicatie.

"Er worden regelmatig beoordelingen uitgevoerd om te blijven voldoen aan veranderende wettelijke kaders, zoals wetgeving op het vlak van gegevensbescherming, privacy en cybersecurity.

2 Onderdeel van het programma voor cybersecuritybewustzijn: uitgebreide reeks richtlijnen en best practices gericht op het verbeteren van cybersecuritypraktijken voor personen binnen de organisatie.