The Heritage Group

7.12 THG Acceptabel Computergebruik en Beveiligingsbeleid

Algemene Beleidsverklaring

Het is het beleid van The Heritage Group (THG) en de verantwoordelijkheid van alle gebruikers van haar computermiddelen en informatiemiddelen om:

- Te voldoen aan alle auteursrechten op computersoftware en de voorwaarden na te leven van alle softwarelicenties waarbij THG partij is.
- De vertrouwelijkheid, integriteit en beveiliging te beschermen van de hardware, gegevens, informatie en softwaretoepassingen die door THG worden gebruikt.
- De computermiddelen en informatie op passende en effectieve wijze te gebruiken zoals vereist voor de activiteiten en missie van THG.

Beheer en Handhaving van het Beleid

De THG Corporate IT-groep is belast met het beheer van dit beleid en elke business unitmanager van THG is verantwoordelijk voor de handhaving ervan. Personen worden op de hoogte gebracht van dit beleid tijdens het aanwervings- of contractproces en ondertekende exemplaren worden bewaard in het personeelsdossier van de medewerker of in het contractdossier van de leveranciers.

Straffen en Sancties

Elke gebruiker die dit beleid opzettelijk overtreedt, zal onderworpen worden aan disciplinaire maatregelen in lijn met de bepalingen van het arbeidsreglement.

Toepassingsgebied van het Beleid

Dit beleid geldt voor gebruikers, computermiddelen en informatiemiddelen bestaande uit hardware, software, gegevens, communicatieprocessen en dienstverleners, inclusief (maar niet beperkt tot):

- Gebruikers zijn medewerkers, tijdelijke medewerkers, consultants en dienstverleners die toegang hebben gekregen tot THG-computermiddelen. Elke gebruiker is verplicht dit beleid te lezen, te begrijpen en ermee in te stemmen.
- Hardware omvat servers, desktop- en laptopcomputers, tablets, PDA's, mobiele telefoons, smartphones, draagbare schijven en opslagapparaten, monitoren, printers, routers, modems, switches en multifunctionele kopieermachines en alle andere apparaten die direct of indirect verbinding maken met het THG-netwerk of zijn computermiddelen.
- Software omvat toepassingen die worden geïnstalleerd op de hardware die eigendom is van THG of namens THG wordt beheerd.
- Gegevens of informatie die worden opgeslagen op een bedrijfshardware die eigendom is van THG of namens THG wordt beheerd, waaronder openbare, vertrouwelijke en beschermde zakelijke en persoonlijke gegevens, bedrijfsinformatie, informatie die wordt verstrekt door of gedeeld met klanten en partners.
- Communicatie omvat elektronische communicatiemiddelen zoals e-mail, blogs, discussiefora, berichtendiensten en/of online berichten.
- Dienstverleners kunnen onder meer omvatten: beheerde dienstverleners, systeemanalisten, hardware-reparatie, auditors, contractmedewerkers, bedrijfsanalisten, externe hosting, enz.

Redelijke Zorg

Gebruikers en dienstverleners dienen redelijke zorg te betrachten met betrekking tot de computermiddelen en informatiemidddelen van THG, waaronder, maar niet beperkt tot:

- Het onmiddellijk melden van verloren of gestolen computermiddelen en/of informatiemidddelen aan de THG IT-afdeling.
- Verantwoordelijk omgaan met en beschermen van THG-computermiddelen en/of informatiemidddelen tegen schade en diefstal.
- Het onmiddellijk melden van elke beveiligingsinbreuk, virus, malware of misbruik door andere gebruikers.
- Het onmiddellijk melden van elk misbruik van computermiddelen en/of informatiemidddelen.
- Het onmiddellijk melden van verdacht gedrag van andere werknemers of derden.

Naleving van Licenties en Auteursrechten

Het is het beleid van THG om alle software- en hardwarelicenties en auteursrechten na te leven.

- **Ongeautoriseerde duplicatie van software kan gebruikers en/of THG blootstellen aan zowel civiele als strafrechtelijke sancties. overtredingen kunnen leiden tot burgerlijke en strafrechtelijke sancties conform de Belgische en Europese wetgeving inzake auteursrechten**
- Gebruikers mogen geen gelicentieerde software of bijbehorende documentatie dupliceren voor gebruik op THG-terreinen of elders, tenzij THG daartoe uitdrukkelijk gemachtigd is door een overeenkomst met de licentiegever.
- Gebruikers mogen bedrijfssoftware niet verstrekken aan externe partijen, inclusief medewerkers, contractors, klanten of anderen.
- Gebruikers mogen software alleen gebruiken in overeenstemming met de toepasselijke licentieovereenkomsten.

Eigendom van Gegevens

De volgende normen zijn van toepassing op het eigendom van gegevens:

- Alle gegevens en gegevensbestanden moeten een eigenaar hebben die verantwoordelijk is voor de inhoud, toegangsautorisatie, bescherming en integriteit van de gegevens.
- Eigenaren van gegevens zijn verantwoordelijk voor het bepalen van de bewaar- en archiveringsvereisten van hun gegevens en het communiceren van deze vereisten aan IT.
- THG IT is de bewaarder van bedrijfsunitgegevens, niet de eigenaar van bedrijfsunitgegevens.

Wijzigen van Computer- en LAN/WAN-configuratie

Gebruikers mogen geen enkele software of hardware installeren zonder voorafgaande goedkeuring.

- Gebruikers mogen de hardwareconfiguratie van door het bedrijf verstrekte computerapparatuur of LAN/WAN-netwerkapparaten niet wijzigen. Gebruikers mogen de antivirussoftware of andere systeembeheerservices (firewalls, versleuteling, Windows- of andere updates, anti-spyware, enz.) niet uitschakelen of de configuratie van het besturingssysteem niet wijzigen.
- Gebruikers mogen geen alternatieve ISP- of WAN-datanetworkservices installeren in THG-faciliteiten.

Hardware en Software

Aankoop van hardware en software

- **<u>Alle aankopen van computerhardware en -software moeten worden goedgekeurd door en/of aangeschaft via de IT-afdeling.</u>**
- Om een aankoopverzoek in te dienen, moet een gedetailleerd verzoek worden gestuurd naar de THG IT helpdesk, inclusief de rekening en afdeling waarop de apparatuur moet worden geboekt.
- Medewerkers met aankoopbevoegdheden mogen (met hun kaart) geen computerhardware of -software aanschaffen zonder voorafgaande goedkeuring van de THG IT-afdeling.
- Medewerkers moeten door het bedrijf verstrekte werkstations gebruiken en mogen geen persoonlijke werkstations aansluiten op het THG-netwerk.

Registratie van software, hardware en diensten

- Alle software, hardware en diensten waarvoor licenties vereist zijn of die eigendom impliceren, moeten worden geregistreerd op naam van THG of de betreffende bedrijfsunit. Deze items mogen nooit worden geregistreerd op naam van een individuele gebruiker of een externe dienstverlener.

Verwijderen van computerhardware

- Gebruikers moeten contact opnemen met THG IT of de lokale It support voor het veilig wissen en afvoeren van apparatuur.

Persoonlijke Apparatuur en Software van Gebruikers of Dienstverleners

Zonder voorafgaande goedkeuring van ITSS is het gebruikers en dienstverleners verboden om:

- Software te installeren op computers van THG
- Computerapparatuur (laptops, desktops, routers, draadloze apparaten, enz.) rechtstreeks aan te sluiten op het bedrijfsnetwerk
- Software in eigendom van het bedrijf te installeren op de persoonlijke computer, tablet of smartphone van de gebruiker of dienstverlener. De enige afwijkingen van deze regel betreffen Office 365-installaties, waarmee gebruikers het mogen installeren op maximaal 5 mobiele apparaten en 5 computers.

Beperkingen voor hardware en software

- Het gebruik van niet-geautoriseerde draagbare opslagapparaten is strikt verboden op alle niet-THG externe informatiesystemen.

Audits

- Er zullen periodieke audits worden uitgevoerd op alle THG-computerassets om te waarborgen dat THG en gebruikers voldoen aan alle softwarelicenties en dit beleid; volledige medewerking van elke gebruiker is vereist tijdens een audit.
- THG IT bewaakt het netwerk en IT-assets regelmatig. Als zich gebeurtenissen voordoen die de beschikbaarheid of beveiliging van IT-middelen kunnen bedreigen of THG kunnen blootstellen aan risico op juridische aansprakelijkheid, zal IT het juiste management informeren en dit kan leiden tot disciplinaire maatregelen.
  Audits en monitoring gebeuren conform CAO 81, met respect voor finaliteit, proportionaliteit en transparantie; individualisering van gegevens gebeurt enkel wanneer wettelijk toegestaan en volgens de vastgelegde procedures. Monitoring gebeurt uitsluitend voor één of meer van de wettelijk toegelaten doeleinden zoals bepaald in CAO nr. 81.

E-mailgebruik

- Alle e-mail in, verzonden door en ontvangen in e-mailaccounts van het bedrijf is eigendom van het bedrijf en gebruikers mogen slechts een beperkte verwachting van privacy hebben, rekening houdend met de professionele aard van de middelen en conform de geldende wetgeving..
- Inzage in mailboxen gebeurt enkel indien noodzakelijk, proportioneel en conform privacywetgeving, bij voorkeur met medeweten of deelname van de betrokkene, tenzij wettelijk niet mogelijk."
- E-mailaccounts van het bedrijf zijn uitsluitend bestemd voor zakelijk gebruik en e-mailadressen van het bedrijf moeten in het algemeen niet worden gebruikt om zich te registreren voor persoonlijke e-commerce of privécommunicatie.
- Gebruikers mogen het e-mailsysteem niet gebruiken voor 'spamming', intern of extern. Spamming wordt gedefinieerd als het verzenden van ongevraagde, onnodige of ongewenste e-mails naar andere e-mailgebruikers.
- Alle e-mails moeten professioneel zijn en mogen geen ongepaste of aanstootgevende inhoud bevatten.
- Gebruikers mogen geen bedrijfszaken afhandelen via e-mailaccounts van derden zoals Gmail, Yahoo, enz.
- Gebruikers mogen THG-e-mail niet automatisch doorsturen naar een e-mailsysteem van derden (bijv. Gmail, Yahoo, enz.).
- **E-mail wordt niet gearchiveerd en back-ups worden slechts 30 dagen bewaard.** Gebruikers moeten zelf stappen ondernemen voor archivering indien nodig.
- Gebruikers mogen geen PST-bestanden aanmaken of gebruiken. Als een PST-bestand nodig is, is ondersteuning door ITSS vereist.

Toegang tot computerbronnen

- Toegang tot THG-computerbronnen en -gegevens is beperkt tot geautoriseerde gebruikers. Gebruikers die toegang nodig hebben tot THG-technologie moeten via de standaard HR-onboardingprocessen worden aangevraagd. Gebruikers moeten ook via de standaard HR-offboardingprocessen van toegang tot THG-technologie verwijderd worden.
- Medewerkers mogen, met goedkeuring van hun manager, toegang verlenen tot THG-computerbronnen aan dienstverleners, klanten of tijdelijke medewerkers, maar deze toegang moet noodzakelijk zijn vanwege een duidelijk gedefinieerde zakelijke behoefte.
- Toegang wordt alleen verleend voor de tijd die nodig is om de taak uit te voeren.
- Contract- en ingehuurde medewerkers moeten worden geregistreerd bij de THG HR Shared Services-groep (HRSS). Dit registratieproces leidt vervolgens tot de aanvraag en inrichting van de toegang voor contract- en ingehuurde medewerkers.
- THG kan multi-factor authenticatie (MFA) vereisen om toegang te krijgen tot technologische bedrijfsmiddelen en/of gegevens. De MFA-oplossing van het bedrijf is Microsoft Authenticator, die moet worden geïnstalleerd op een bedrijfs- en/of persoonlijk mobiel apparaat.

Eigendom van opgeslagen documenten en gegevens

- Alle gegevens en informatie, inclusief e-mails, foto's en andere documenten, die zijn opgeslagen op computers, tablets, smartphones en andere apparaten die eigendom zijn van het bedrijf, zijn eigendom van het bedrijf en gebruikers mogen slechts een beperkte verwachting van privacy hebben, rekening houdend met de professionele aard van de middelen en conform de geldende wetgeving..
- Gegevens die worden gecreëerd tijdens iemands functie/rol zijn eigendom van het bedrijf.
- Wanneer een medewerker het bedrijf verlaat, kan IT op verzoek van HR en/of de leidinggevende toegang verlenen tot de gegevens van de voormalige medewerker (bijv. e-mail, OneDrive for Business, enz.). Deze gegevens worden 91 dagen na uitdiensttreding bewaard en daarna verwijderd.
- Persoonlijke gegevens dienen uitsluitend op de lokale computerdrive te worden opgeslagen en mogen de prestaties van de computer niet beïnvloeden.
- Documenten in persoonlijk eigendom die op netwerkopslag zijn opgeslagen, kunnen op elk moment en zonder kennisgeving worden verwijderd.

Integriteit, beveiliging en vertrouwelijkheid van systemen en informatie

Het is de verantwoordelijkheid van elke gebruiker om te helpen de integriteit, beveiliging en vertrouwelijkheid te waarborgen van de informatie en systemen die zij gebruiken of beheren.

- Gebruikers mogen systeemwachtwoorden nooit zichbaar maken en wachtwoorden mogen niet met anderen worden gedeeld. Wachtwoorden mogen niet worden opgeslagen op Post-its of in elektronische bestanden die op de computer van een gebruiker of een andere technologische bedrijfsmiddel van het bedrijf zijn opgeslagen.
- Gebruikers moeten de aan hen toegewezen gebruikersnaam-/wachtwoordgegevens gebruiken en mogen hun toegang niet delen.
- Waar mogelijk in THG-applicaties moeten alle wachtwoorden voor gebruikersaccounts die zijn ingesteld op interne systemen die Heritage-gegevens bevatten, voldoen aan de volgende vereisten voor wachtwoordbeveiliging:
    - Wachtwoordvervaltermijn = 90 dagen
    - Minimale geldigheid = 1 dag
    - Wachtwoordgeschiedenis = 8 wachtwoorden
    - Minimale wachtwoordlengte = 8 tekens
    - Wachtwoordcomplexiteit moet een mix bevatten van letters, cijfers en speciale tekens

- Maximaal aantal mislukte inlogpogingen = 3
- Duur van accountvergrendeling = 15 minuten

- Gebruikers mogen geen software installeren of gebruiken die bedoeld is om beveiligingsmaatregelen te omzeilen.
- Gebruikers mogen bedrijfsgegevens niet moedwillig verwijderen of wijzigen.
- Slechts specifieke opslagapparaten worden door THG IT geback-upt voor hersteldoeleinden. De gebruiker is verantwoordelijk voor alle informatie die is opgeslagen op verwijderbare media of lokale (niet-servergebaseerde) opslagdrives. **Desktops, laptops, tablets en draagbare drives worden niet geback-upt.**
- Gebruikers moeten voldoen aan alle beleidsregels voor het bewaren van elektronische documenten zoals vereist door het management van hun bedrijfsunit of door THG-beleid.
- THG schrijft het gebruik voor van de nieuwste aanvaardbare versleutelingsstandaarden om gegevens tijdens transport te beveiligen.
- Alle gebruikers-endpoints hebben een maximale operationele levensduur van vier jaar; daarna moeten ze worden geëvalueerd en, indien nodig, vervangen om te blijven voldoen aan onze beveiligingsnormen. Op dezelfde manier geldt voor servers en netwerkhardware een maximale operationele levensduur van vijf jaar.
- Om ervoor te zorgen dat beleid en regelgeving met betrekking tot de fysieke bedrijfsomgeving voor organisatie-assets strikt worden nageleefd, houden THG-medewerkers veilige fysieke locaties aan voor onze servers en werkstations, beheersen zij omgevingscondities om de prestaties en levensduur van apparatuur te optimaliseren, en zorgen zij ervoor dat alle fysieke toegang tot deze assets wordt beheerd door onze uitgebreide beveiligingsprotocollen.

Gegevens worden geclassificeerd als Vertrouwelijk, GDPR, Alleen intern gebruik of Openbaar. De definitie van en omgang met deze informatie moet voldoen aan de richtlijnen in de onderstaande tabel:

		Opslagapparaat of -bestemming Laag risico → Hoog risico							
		Netwerk (server/gemapte schijf, SharePoint, OneDrive for Business)	**Desktop** (lokale schijf)	**Draagbare computer** (lokale schijf op laptop, tablet)	**Smartphone** (iPhone, Android)	**E-mail**	**Portaal voor samenwerking met partners** (dataroom, FTP-site)	**Draagbare schijf** (zip drive, thumb drive, USB-drive en vergelijkbaar)	**Publieke cloud** (Cloud drive, Box, OneDrive Personal, Dropbox, Google Drive, enz.)
Informatie- of gegevenstype	**Vertrouwelijke gegevens van Heritage**	**Toegestaan**	**Niet toegestaan**	**Niet toegestaan**	**Niet toegestaan** – tenzij het apparaat is versleuteld, met wachtwoord is beveiligd en het document is geback-upt	**Niet toegestaan** – tenzij het document met een wachtwoord is beveiligd en versleuteld wordt verzonden	**Niet toegestaan** – tenzij goedgekeurd door de manager, het document met een wachtwoord is beveiligd, de site SSL-versleuteld is en het document is geback-upt	**Niet toegestaan**	**Niet toegestaan**
	Gegevens van Heritage – alleen intern gebruik	**Toegestaan**	**Toegestaan**	**Niet toegestaan**	**Niet toegestaan** – tenzij het apparaat met een wachtwoord is beveiligd en het document is geback-upt	**Toegestaan**	**Niet toegestaan** – tenzij goedgekeurd door de manager, het document of portaal met een wachtwoord is beveiligd, de site SSL-versleuteld is en het document is geback-upt	**Toegestaan maar niet aangeraden** – tenzij het apparaat is versleuteld, met wachtwoord is beveiligd en het document is geback-upt	**Niet toegestaan**
	Openbare gegevens van Heritage	**Toegestaan**	**Toegestaan – apparaat moet versleuteld**	**Toegestaan – apparaat moet versleuteld**	**Toegestaan**	**Toegestaan**	**Toegestaan**	**Toegestaan**	**Toegestaan**

			versleuteld en met wachtwoord beveiligd zijn	**en met wachtwoord beveiligd zijn**	**en met wachtwoord beveiligd zijn**				
	Heritage back-upproces	**Dagelijks automatisch met bewaartermijn van 30 dagen**	**Geen automatische back-up of niet beheerd door THG IT**	**Geen automatische back-up of niet beheerd door THG IT**	**Geen automatische back-up of niet beheerd door THG IT**	**Dagelijks automatisch met bewaartermijn van 30 dagen**	**Geen automatische back-up of niet beheerd door THG IT**	**Geen automatische back-up of niet beheerd door THG IT**	**Geen automatische back-up of niet beheerd door THG IT**

Vertrouwelijke gegevens van Heritage

Alle gegevens die persoonlijk identificeerbare informatie (PII) bevatten over een individu en die worden gereguleerd door lokale en Europese GDPR privacyregelgeving. Voorbeelden zijn onder meer het naam met adres, bankgegevens, enz. ***LET OP: Creditcards worden beschouwd als Vertrouwelijke gegevens, maar mogen niet elektronisch worden opgeslagen.***

Gegevens van Heritage – alleen intern gebruik

Alle gegevens die niet zijn geclassificeerd als Vertrouwelijke gegevens van Heritage, maar die Heritage niet aan het algemene publiek zou verspreiden. Voorbeelden zijn financiële gegevens, intellectueel eigendom, informatie die door klanten, leveranciers of partners aan Heritage is verstrekt, als vertrouwelijk aangemerkte gegevens, contracten en overeenkomsten, enz.

Openbare gegevens van Heritage

Alle gegevens die niet zijn geclassificeerd als Vertrouwelijk of Alleen intern gebruik en die al openbaar beschikbaar zijn, of waarvan Heritage het acceptabel vindt om ze openbaar beschikbaar te maken.

Internetgebruik

- Internettoegang kan worden gebruikt in overeenstemming met de lokale afspraken en de behoeften van de functie. Toegang wordt voorzien als werkmiddel en kan, indien nodig, in overleg met de leidinggevende worden afgestemd of aangepast.
- Internetgebruik kan op een transparante en proportionele manier worden gefilterd en opgevolgd om de veiligheid van systemen en de correcte werking van de organisatie te waarborgen, overeenkomstig CAO 81. Controles gebeuren in principe op algemene of geaggregeerde basis. Het bezoeken van duidelijk ongepaste of wettelijk verboden content (zoals pornografie, excessief geweld, drugs- of goksites) is niet toegestaan. Individuele gegevens worden enkel geraadpleegd wanneer dit wettelijk toegelaten is en volgens de procedures van CAO 81, bijvoorbeeld bij vastgestelde onregelmatigheden.
- Gebruikers die internet gebruiken, treden op als vertegenwoordigers van THG. Daarom moeten medewerkers zich zodanig gedragen dat zij de reputatie van het bedrijf niet schaden en de vertrouwelijkheid, integriteit of beveiliging van de computersystemen of informatie van het bedrijf niet schenden.
- Gebruikers mogen geen internet-e-mailaccounts (Google Mail, Yahoo Mail, enz.) aanmaken, URL's registreren, websites of blogs opzetten die geïnterpreteerd kunnen worden als representatief voor het bedrijf of die zouden worden gebruikt om bedrijfsactiviteiten te verrichten zonder voorafgaande goedkeuring van het management.
- Gebruikers mogen op sociale netwerksites, blogs of forums geen content publiceren die schadelijk is voor de reputatie van het bedrijf, henzelf of andere personen binnen het bedrijf.
- De waarheid of nauwkeurigheid van informatie op internet en in e-mail moet als twijfelachtig worden beschouwd totdat deze is bevestigd door een afzonderlijke betrouwbare bron.
- Medewerkers mogen geen materiaal van het bedrijf (auteursrechtelijk beschermde software, interne correspondentie, enz.) plaatsen op een publiek toegankelijke internetsite zonder een duidelijk gedefinieerde zakelijke behoefte en voorafgaande goedkeuring van het management.
- Internet garandeert niet de privacy of vertrouwelijkheid van informatie. Gevoelig materiaal dat via internet wordt verzonden, kan het risico lopen door derden te worden onderschept en moet daarom versleuteld worden verzonden. Medewerkers moeten grote voorzichtigheid en zorgvuldigheid betrachten bij het overdragen van dergelijk materiaal in welke vorm dan ook.
- Tenzij anders vermeld, moet alle software op internet worden beschouwd als auteursrechtelijk beschermd werk. Daarom is het medewerkers verboden software te downloaden en/of dergelijke bestanden te wijzigen zonder toestemming van de auteursrechthebbende en zonder naleving van alle overige licentievereisten.
- 'Shareware' en 'freeware' die via internet kunnen worden gedownload, moeten worden beoordeeld en geïnstalleerd door de THG IT-groep.
- Elke inbreukmakende activiteit op internet door een medewerker kan de verantwoordelijkheid van THG zijn. Bijgevolg **kan THG ervoor kiezen de medewerker aansprakelijk te houden voor zijn/haar handelen.**

Sociale media

Het algemene gebruik van sociale media wordt bepaald door elke bedrijfsunit. Al het gebruik van sociale media vanaf apparatuur van THG en apparaten die met het THG-netwerk zijn verbonden, wordt door THG IT gemonitord en gefilterd om misbruik en ongepaste content te voorkomen. Overmatig gebruik van sociale media kan leiden tot disciplinaire maatregelen in lijn met de bepalingen in het arbeidsreglement.
Het plaatsen van content op door het bedrijf gesponsorde sociale media (bijv. de corporate Facebookpagina) is alleen toegestaan voor de THG HR-afdeling of zoals goedgekeurd door de THG HR-afdeling. Raadpleeg het beleid inzake elektronische media voor verdere richtlijnen.

Ongepaste content op sociale media

Hoewel sociale media legitieme zakelijke en persoonlijke content bevatten, omvatten ze ook content die ongepast is voor de werkplek, waaronder naakt, geweld,

drugsgebruik, seks en gokken. Daarom is hetzelfde beleid inzake ongepaste content dat van toepassing is op het bredere internetgebruik, ook van toepassing op content binnen sociale media. Ongepaste content mag niet door medewerkers worden geraadpleegd tijdens het werk of bij gebruik van bedrijfsbronnen. Medewerkers dienen hun gezonde verstand te gebruiken en rekening te houden met anderen bij het bepalen welke content geschikt is voor de werkplek.

Mobiele apparaten

De volgende standaarden zijn van toepassing op het gebruik van mobiele apparaten voor THG-zakelijk gebruik:

- Alleen ondersteunde mobiele apparaten zijn geautoriseerd voor verbinding met THG-systemen. Uitzonderingen moeten worden goedgekeurd door THG IT.
- Alle mobiele apparaten die verbinding maken met de THG-omgeving moeten worden geregistreerd.
- Alle apparaten moeten de eigendomsinformatie correct op het apparaat opgeslagen hebben (bijv. uw naam en telefoonnummer).
- Mobiele apparaten die THG-documenten of e-mail bevatten, moeten zijn beveiligd met een pincode (PIN) en apparaatversleuteling.
- THG behoudt zich het recht voor om bedrijfsgegevens van elk mobiel apparaat te verwijderen.

Kunstmatige intelligentie en machine learning

THG heeft een beleid vastgesteld voor acceptabel gebruik van kunstmatige intelligentie en machine learning op de werkplek. Raadpleeg het beleid ‘AI-gebruik op de werkplek’.

Kader voor beleidsgovernance

Dit beleid wordt beheerd volgens het NIST en NIS2 Cybersecurity Framework (CSF), dat een gestructureerde aanpak biedt voor het beheersen van cyberbeveiligingsrisico’s. De kernfuncties van het framework—Identificeren, Beschermen, Detecteren, Reageren en Herstellen—sturen de ontwikkeling en implementatie van dit beleid om een uitgebreide en veerkrachtige cyberbeveiligingshouding te waarborgen.
Persoonsgegevens worden verwerkt conform Verordening (EU) 2016/679 (GDPR), met respect voor de beginselen van rechtmatigheid, doelbinding, minimale gegevensverwerking en bewaarbeperking. Voor internationale doorgiften van persoonsgegevens naar de Verenigde Staten wordt gebruikgemaakt van het EU-US Data Privacy Framework, zoals goedgekeurd door de Europese Commissie, en uitsluitend met ontvangers die geldig zijn gecertificeerd onder dit framework. Waar van toepassing worden bijkomende passende technische en organisatorische maatregelen genomen ter bescherming van persoonsgegevens.

Bevestiging

Ik heb het THG-beleid inzake acceptabel computergebruik en beveiliging gelezen en ga ermee akkoord dit na te leven als voorwaarde voor mijn voortgezette dienstverband bij THG. Ik begrijp dat overtreding van dit beleid kan leiden tot disciplinaire maatregelen en/of intrekking of beperken van internet- of systeemtoegang.