30-09-2021
Versie 1.2

Privacy & Securitybeleid 2021-2025

G.A. Douma (CISO)
M. Cornelissen (FG)

Hanzehogeschool Groningen
University of Applied Sciences

Inhoudsopgave

Samenvatting

Het succes van een organisatie hangt steeds meer af van informatie, nieuwe technologieën en computersystemen. Die informatie moet goed worden beveiligd, zeker als er persoonsgegevens worden opgeslagen. In dit document is verwoord op welke manier de Hanzehogeschool (Hanze) voorziet in adequate informatiebeveiliging en daarmee voldoet aan de relevante wet- en regelgeving.
Met het Privacy- en Securitybeleid wil de Hanzehogeschool ook bijdragen aan een betere kwaliteit van de informatievoorziening en zorgen voor een juiste balans tussen functionaliteit, veiligheid en privacy.

Beschreven wordt op wie, op welke onderdelen van de instelling en op welke apparaten en applicaties het beleid van toepassing is. Informatiebeveiliging werkt door in alle lagen van de organisatie. Naast de reikwijdte van het beleid worden de verantwoordelijkheden van de betrokken functionarissen beschreven. Het lijnmanagement is verantwoordelijk voor haar eigen processen, de directie zorgt ervoor dat beveiligingsmaatregelen daadwerkelijk worden geïmplementeerd. Eindverantwoordelijkheid ligt bij het College van Bestuur (CvB) van de Hanzehogeschool.

Vijf beleidsprincipes zijn leidend, namelijk:

1. *Risico-gebaseerd*
   We baseren de maatregelen op de mogelijke veiligheidsrisico's van onze informatie, processen en IT-faciliteiten.
2. *Iedereen*
   Iedereen is en voelt zich verantwoordelijk voor een juist en veilig gebruik van middelen en bevoegdheden.
3. *Altijd*
   Informatiebeveiliging zit in het DNA van al onze werkzaamheden.
4. *Security & Privacy by Design*
   Informatiebeveiliging is vanaf de start een integraal onderdeel van ieder project of iedere verandering m.b.t. informatie, processen en IT-faciliteiten.
5. *Security & Privacy by Default*
   Gebruikers hebben alleen toegang tot informatie en IT-faciliteiten die zij nodig hebben voor hun werkzaamheden. Het openstellen van informatie is een bewuste keuze.

Beleid en maatregelen zijn niet voldoende om risico's op het terrein van informatiebeveiliging uit te sluiten. De mens zelf creëert de grootste risico's. Bij de Hanzehogeschool werken we daarom voortdurend aan het vergroten van het beveiligingsbewustzijn van medewerkers om kennis van risico's te verhogen en veilig en verantwoord gedrag aan te moedigen.

Informatiebeveiliging is een continu proces, waarbij we steeds kijken naar mogelijke verbeteringen. Dit gebeurt onder andere door jaarplannen, controles en bijsturing. Naast Security Officers kunnen de Functionaris Gegevensbescherming en de interne auditor hier bijvoorbeeld adviezen voor geven.

In de bijlagen is aandacht voor de managementcyclus voor periodieke bijstelling inclusief de documenten die hiervoor van belang zijn op het gebied van informatiebeveiliging. De vijf beleidsprincipes voor informatiebeveiliging zijn in de bijlage volledig uitgewerkt. Daarnaast is een overzicht gegeven van de belangrijkste wet- en regelgeving rondom informatiebeveiliging en worden de rollen van betrokken functionarissen verhelderd.

1. Inleiding

Het succes van de Hanzehogeschool hangt steeds meer af van informatie, nieuwe technologieën en computersystemen. We kunnen niet meer zonder het digitaal verzamelen, vastleggen en delen van informatie met zowel interne als externe partners, collega's en studenten. Het nieuwe strategisch beleid van de Hanzehogeschool benoemt Digitale Transformatie en Flexibilisering als belangrijke speerpunten.

De Hanzehogeschool is een instelling met een open karakter. De Hanze stelt zich risicomijdend op. Vanuit het onderwijs- en onderzoeksperspectief is de insteek "*Open waar mogelijk, gesloten waar nodig*". Dat past ook bij de FAIR[1] doelstellingen in het onderzoekdomein. Adequate beveiliging van informatie is steeds een randvoorwaarde en het openstellen van informatie moet een bewuste keuze zijn.

De digitale werkelijkheid is constant in beweging en dat brengt steeds nieuwe en andere risico's met zich mee voor de Informatieveiligheid[2]. De risico's vormen een bedreiging voor de kwaliteit en continuïteit van processen en voor het behalen van de strategische doelen. De bedreigingen kunnen de beschikbaarheid, integriteit en vertrouwelijkheid van informatie beïnvloeden. Voorbeelden van bedreigingen zijn kwetsbaarheden in systemen of ongeautoriseerde toegang tot informatie. Dit kan de waarde van een Hanzehogeschool-diploma(certificaat), behaalde cijfers of de legitimiteit van onderzoekconclusies ondermijnen.
Ook de privacy van studenten, medewerkers en gasten en de reputatie van de Hanzehogeschool kunnen worden geschaad. De Hanze stelt zich risicomijdend op. Informatiebeveiliging is daarom van cruciaal belang.

Informatiebeveiliging vraagt steeds om bijstelling zodat er een passend beveiligingsniveau blijft. Dat komt onder andere door de technologische ontwikkelingen, de aangescherpte eisen om te voldoen aan de wet- en regelgeving rondom gegevensbescherming en privacy (AVG), en de afspraken met onderzoek- en onderwijspartners.

Het verkleinen en beheersen van de risico's vraagt om inspanningen op organisatorisch, procesmatig en technologisch vlak. Daarnaast moeten bestuurders, studenten en gasten van de Hanze zich ook bewust worden van de risico's en hun handelen daarop afstemmen.

Informatieveiligheid is niet te bereiken door alleen een aantal technische en organisatorische maatregelen vast te stellen. Door de veranderende wereld is het een dynamisch proces. In dit document zijn om die reden vijf hoofdprincipes leidend voor informatiebeveiliging binnen de Hanzehogeschool. De vast te stellen maatregelen, procedures en richtlijnen kunnen getoetst worden aan de vijf hoofdprincipes die in hoofdstuk 3 zijn beschreven.

Er is een belangrijke relatie tussen informatiebeveiligingsrisico's en risico's op andere gebieden, zoals privacy, safety[3] (arbowetgeving), veiligheid in onderwijs en onderzoek, fysieke beveiliging en business-continuïteit. Soms overlappen ze elkaar gedeeltelijk.

2. Wet- en regelgeving & Aanverwante documenten

De Hanzehogeschool streeft ernaar om in al haar processen en procedures te voldoen aan de relevante wet- en regelgeving. Dit doet zij op basis van het principe "Pas toe of leg uit", waardoor de Hanzehogeschool

[1] Findable – Accessible – Interoperable – Reusable (zie https://nl.wikipedia.org/wiki/FAIR-principes)
[2] Zie toelichting paragraaf 3.1 over verschillen in de definities 'informatieveiligheid' en 'informatiebeveiliging'
[3] *Safety* wordt als verzamelterm gebruikt voor de verschillende aspecten van personele veiligheid: Arbo en milieu, sociale veiligheid, bedrijfshulpverlening e.d.

altijd kan verantwoorden waarom zij wel of niet voldoet.
Bijgaand overzicht van de belangrijkste aan informatieveiligheid gerelateerde wet- en regelgeving met specifieke aandachtspunten voor Hanzehogeschool. Ook documenten van de Hanzehogeschool zelf dienen als belangrijke input. De komende beleidsperiode zal integrale veiligheid een belangrijk onderdeel uitmaken van het verder uitwerken van dit beleid.
De volgende regelgeving stelt o.a. eisen aan informatieveiligheid:

- Wet Hoger Onderwijs en Wetenschappelijk Onderzoek
- Wet Computercriminaliteit
- AVG
- UAVG
- Wet Meldplicht Datalekken (per 1 januari 2016)
- Archiefwet
- Auteurswet
- Gedragscode Onderzoek
- Governance Code Hoger Onderwijs

Normenkader:

- Het Normenkader SurfAudit (o.b.v. NEN ISO27001/2:2017).
- PDCA
- Het Cloud Juridisch Normenkader (voor SAAS/Cloud diensten)
- De Surf Baseline informatiebeveiliging
- De Surf Informatiebeveiligingsarchitectuur
- De Surf model-classificatierichtlijn
- De HORA, de Hogeschool Referentie Architectuur
- HG Model DPIA
- Surf verwerkersovereenkomst
- Databeleid Hanzehogeschool
- Landelijke Dreigingsbeeld

Hanzehogeschool documenten & beleid

- Regeling Gebruik ICT-voorzieningen
- Beleidsplan Veilige Hogeschool
- Strategisch Beleid Hanzehogeschool
- Crisisdocumentatie Hanzehogeschool

Bronnen:

- Surf-SCIPR model voor Informatiebeveiliging
- Landelijk platform integraal veilig hoger onderwijs
- Dreigingenanalyse Onderwijs Deloitte
- Dreigingenanalyse NCSC
- BIR/BIG
- CISA handboek training ISACA
- OWASP
- Informatiebeveiliging onder controle, Paul Overbeek et al., Pearson Education Uitgeverij BV
- Praktijkgids Code voor informatiebeveiliging, Standaard voor informatiebeveiliging met succes invoeren bij uw organisatie, Ernst J. Oud, Academic Service
- Cybersaveyourself.nl
- NCSC.nl

3. Definitie, doelstelling, doelgroep en reikwijdte

3.1 Informatieveiligheid en Informatiebeveiliging

De begrippen informatieveiligheid en informatiebeveiliging worden vaak door elkaar gebruikt, maar ze hebben niet dezelfde betekenis. Informatieveiligheid richt zich op het beschikbaar, integer en vertrouwelijk houden van informatie. Hiervoor moeten informatie en informatiesystemen beschermd worden tegen mogelijke bedreigingen. Dit wordt gedaan door het nemen, onderhouden en controleren van beveiligingsmaatregelen, ook wel informatiebeveiliging genoemd.

De eindverantwoordelijkheid voor informatieveiligheid ligt bij het College van Bestuur.

3.2 Doelstelling, randvoorwaarden en uitgangspunten

Informatiebeveiliging heeft de volgende doelen:

- Het waarborgen van de beschikbaarheid van informatie van het onderwijs, onderzoek en de bedrijfsvoering.
- Het waarborgen dat informatie juist, volledig en actueel is (integriteit) en alleen toegankelijk is voor personen die vanuit hun rol/functie daar toegang tot mogen hebben (beschikbaarheid, integriteit en vertrouwelijkheid).
- Het voorkomen van beveiligings- en privacy-incidenten (vertrouwelijkheid) en de eventuele gevolgen hiervan verminderen.

Met het Privacy en Securitybeleid wil de Hanzehogeschool bijdragen aan een betere kwaliteit van de informatievoorziening en zorgen voor een juiste balans tussen functionaliteit, veiligheid en privacy en uiteraard de daarmee samenhangende kosten. Het Privacy en Securitybeleid sluit daarmee aan bij de missie van de instelling.

De Hanzehogeschool heeft de ambitie om met behulp van dit beleidsdocument de informatieveiligheid structureel naar een hoog niveau te brengen en daar te houden. Dit doet zij door het beschrijven van verantwoordelijkheden, taken en bevoegdheden en wet- en regelgeving.

Het Privacy en Securitybeleid, en de opvolging daarvan, moet Hanzehogeschool in staat stellen ‘in control’ en compliant te zijn. Op basis daarvan kunnen de betrokken Deans en directeuren verantwoording afleggen aan het College van Bestuur en het CvB aan de Raad van Toezicht (RvT). De uitvoering van het beleid is ook de basis om te voldoen aan wettelijke voorschriften.

Randvoorwaarden

Om deze doelstellingen te kunnen bereiken zijn de volgende randvoorwaarden voor de Hanzehogeschool van belang:

- *Beveiligingsorganisatie*
  De verantwoordelijkheden, taken en bevoegdheden van de informatiebeveiligingsfunctie zijn expliciet vastgelegd en worden gedragen door het bestuur, en afgeleid daarvan, door de hele instelling.
- *Procesbenadering*
  Informatiebeveiliging is een continu proces. Periodiek worden er risicoanalyses en audits uitgevoerd. De resultaten hiervan worden opgenomen in vastgestelde jaarplannen met duidelijke keuzes in beveiligingsmaatregelen. De uitvoering van deze beveiligingsmaatregelen wordt periodiek gecontroleerd.

Uitgangspunten

Uit de doelstelling en de randvoorwaarden komen de volgende uitgangspunten voort:

- *Kader*
  Het beleid biedt een kader om (toekomstige) maatregelen in de informatiebeveiliging te toetsen aan de vastgestelde beveiligingsprincipes (hoofdstuk 4), best practices en normen. Daarnaast biedt het een kader om de taken, bevoegdheden en verantwoordelijkheden in de instelling te beleggen.
- *Normen*
  Specifiek voor de SURF gemeenschap[4] is het 'SURF Normenkader Informatie Beveiliging Hoger Onderwijs' (IBHO) vastgesteld. Het IBHO is gebaseerd op de normen die zijn vastgelegd in de ISO-27000-serie. Het IBHO vormt samen met dit beleidsdocument de basis voor een informatie-beveiligingsmanagementsysteem (ISMS[5], zie bijlage A) van de Hanzehogeschool. Het ISMS is ingericht op basis van de internationale standaard ISO 27001. Formele certificering, bijvoorbeeld volgens de norm ISO 27001, wordt niet als noodzakelijk gezien voor de Hanzehogeschool.
- *Volwassenheid*
  IBHO omschrijft een norm voor de volwassenheid van de Informatiebeveiliging volgens het Capability Maturity Model (CMM)[6]. De Hanzehogeschool streeft naar een volwassenheidsniveau 3 volgens de SURF-richtlijnen. 2-jaarlijks doen we mee met de Surfaudit benchmark volgens het NBA maturity model van de beroepsvereniging van IT-auditors. We zorgen binnen de Hanze dat dit aantoonbaar is.
- *Maatregelen*
  De Hanzehogeschool neemt maatregelen op basis van de internationaal vastgestelde ISO-27002-standaard. Hierbij worden de 'SURF Baseline Informatie Beveiliging Hoger Onderwijs' en overige best practices in de SURF-gemeenschap als uitgangspunt genomen.

3.3. Doelgroep

Het beleid is bestemd voor iedereen die – intern of extern – te maken heeft met de bedrijfsprocessen van Hanzehogeschool. Het beleid richt zich in eerste instantie op het bestuur, hoger management, de Contactpersonen Verantwoorde Informatiehuishouding (CVI's), de beveiligingsorganisatie en de leidinggevenden. Zij dragen uit dat het beleid van toepassing is op alle medewerkers, studenten, bestuurders, gasten, bezoekers en externe relaties.

3.4. Reikwijdte van het beleid

Bij de Hanzehogeschool wordt informatieveiligheid breed geïnterpreteerd. Het gaat over alle vormen van formeel vastgelegde informatie (dus niet alleen digitale informatie), die de instelling of haar relaties verwerken. Daarnaast heeft het beleid betrekking op niet-formeel vastgelegde informatie, zoals uitspraken van studenten en medewerkers in discussies, op webpagina's en persoonlijke websites, waarop men de Hanze kan aanspreken.

Het beleid heeft betrekking op alle instellingsonderdelen en-dienstverlening. Het gaat over alle door de Hanzehogeschool beheerde apparaten en applicaties waarmee geautoriseerde toegang tot (diensten van) het Hanze-netwerk kan worden verkregen en/of waarmee data van de instelling wordt verwerkt.

[4] De actuele documenten zijn te vinden op https://www.surf.nl/informatiebeveiliging en https://www.surf.nl/surfaudit-inzicht-in-je-informatiebeveiliging-en-privacy en voor SCIPR-leden op de ondersteunende wiki's https://wiki.surfnet.nl/display/SCIPR/SCIPR+Home en https://wiki.surfnet.nl/display/SA/SURFaudit+Home
[5] ISMS: Information Security Management System.
[6] https://nl.wikipedia.org/wiki/Capability_Maturity_Model

Onder apparaten en applicaties vallen:

- Alle fysiek op het netwerk aangesloten apparaten zoals servers, werkstations, laptops, gebouwbeheerssystemen.
- Door de Hanze aangeboden applicatie (on-premise, cloud).
- Alle draadloos op het netwerk aangesloten mobiele apparaten, zoals notebooks, tablets, smartphones, smartwatches.
- IoT[7]-devices, zoals bewakingscamera's en sensoren.
- Alle op deze apparaten beschikbare (web/cloud)services en applicaties ('apps').
  Het toepassen van AI.

De Hanzehogeschool faciliteert het gebruik van privéapparaten (BYOD[8]) in beperkt mate. Het gebruik van BYOD op het HG-netwerk voor toegang tot applicaties of informatie van de instelling valt onder dit beleid.

Het beleid is locatie-onafhankelijk: het geldt ook als men op een andere locatie dan op het terrein van de Hanze met informatie of informatievoorzieningen van de Hanze werkt (zoals thuis, in de trein of bij een andere onderwijsinstelling).

4. Beleidsprincipes informatiebeveiliging

4.1. Inleiding

De Hanzehogeschool is een instelling met een open karakter. De Hanze stelt zich risicomijdend op. Vanuit het onderwijs- en onderzoeksperspectief is de insteek "*Open waar mogelijk, gesloten waar nodig*". Dat past ook bij de FAIR[9] doelstellingen in het onderzoekdomein. Adequate beveiliging van informatie is steeds een randvoorwaarde en het openstellen van informatie moet een bewuste keuze zijn.

De Hanzehogeschool heeft vijf beleidsprincipes voor informatiebeveiliging vastgesteld. Deze helpen om te bepalen welke beveiligingsmaatregelen er nodig zijn.

Een korte introductie van de vijf beleidsprincipes volgt in paragraaf 4.2. Een gedetailleerde uitwerking van de principes is opgenomen in bijlage B.

4.2. Beleidsprincipes

De vijf hierna vermelde beleidsprincipes helpen bij de implementatie van het beleid.
Op basis van deze vijf beleidsprincipes kunnen maatregelen worden geformuleerd die relevant zijn voor de bescherming van processen van de Hanzehogeschool. De beleidsprincipes vormen de basis voor de communicatie rondom het beleid van de Hanzehogeschool.

De vijf door de Hanzehogeschool vastgestelde beleidsprincipes zijn:
1. Risico-gebaseerd
2. Iedereen
3. Altijd
4. Security & Privacy by Design
5. Security & Privacy by Default

[7] Internet of Things
[8] Bring Your Own Device
[9] Findable – Accessible – Interoperable – Reusable (zie https://nl.wikipedia.org/wiki/FAIR-principes)

1	**Risico-gebaseerd** Informatiebeveiliging is risico-gebaseerd. De HG stelt zich risicomijdend op. 
Kern	We baseren de maatregelen op de mogelijke veiligheidsrisico's van onze informatie, processen en IT-faciliteiten. Concreet: Data, processen, systemen.
Achtergrond	Het delen van kennis (openheid) is een belangrijke kernwaarde van het onderwijs- en onderzoekproces van Hanzehogeschool. Voor een goede risicoafweging bij het beschermen van informatie en het treffen van de juiste maatregelen, is het van belang om de waarde van informatie vast te stellen. Als de waarde van informatie bekend is, kan ook de juiste mate van beveiliging worden bepaald, één die past bij de risico's. Proportionaliteit daarin is gewenst, ook om de beschikbare financiële middelen efficiënt te gebruiken.
Implicaties	Denk aan het inrichten van een risicomanagementproces (classificatie), het vastleggen van verantwoordelijkheden, het borgen van risico's in contracten. Zie bijlage A voor een overzicht van alle implicaties.

2	**Iedereen** Informatiebeveiliging is een verantwoordelijkheid van iedereen. 
Kern	Iedereen is en voelt zich verantwoordelijk voor een juist en veilig gebruik van middelen en bevoegdheden.
Achtergrond	Iedereen is zich bewust van de waarde van informatie en handelt daarnaar. Deze waarde wordt bepaald door de mogelijke schade als gevolg van verlies van beschikbaarheid, integriteit of vertrouwelijkheid. Van zowel medewerkers, studenten als derden wordt verwacht dat ze bewust omgaan met informatie in welke vorm dan ook en dat ze actief bijdragen aan de veiligheid van de geautomatiseerde systemen en de daarin opgeslagen informatie. Het succes van beveiliging staat of valt met goede communicatie.
Implicaties	Denk hierbij aan het vastleggen van afspraken in arbeidsvoorwaarden, omgangsvormen, gedragscodes en huisregels etc. Zie bijlage A voor een overzicht van alle implicaties. Concreet voor de Hanze betekent dit vaststelling én conformering van medewerkers aan de ICT-regeling via AFAS.

3	**Altijd** Informatiebeveiliging is een continu proces. 
Kern	Informatiebeveiliging zit in het DNA van al onze werkzaamheden.
Achtergrond	De omgeving verandert continu; cyberdreigingen nemen toe en af; processen veranderen, medewerkers en studenten veranderen etc. Eenmalig de maatregelen bepalen en implementeren is onvoldoende om een veilig klimaat te behouden. Informatiebeveiliging heeft alleen zin als dit een continu proces is van het nemen van maatregelen, bewustzijn en controles.
Implicaties	Denk hierbij aan het houden van HG-brede awareness campagnes, het inrichten van een audit-proces. Zie bijlage A voor een overzicht van alle implicaties.

4	**Security & privacy by Design** Integrale aanpak informatiebeveiliging. 
Kern	Informatiebeveiliging is vanaf de start een integraal onderdeel van ieder project of iedere verandering m.b.t. informatie, processen en IT-faciliteiten.
Achtergrond	Security & privacy by design betekent dat al tijdens de start van een project, het ontwerp van een nieuwe applicatie of ICT-omgeving en bij technische of functionele veranderingen rekening wordt gehouden met de beveiliging van gegevens en de continuïteit van de processen. Dit voorkomt (vaak dure) herstel-werkzaamheden achteraf.
Implicaties	Denk hierbij aan het vaststellen en toetsen van beveiligingseisen in projecten en het inregelen van autorisatieschema's. Zie bijlage A voor een overzicht van alle implicaties.

5	**Security & privacy by Default** Standaard beperkte toegang en veilige instellingen 
Kern	Gebruikers hebben alleen toegang tot informatie en IT-faciliteiten die zij nodig hebben voor hun werkzaamheden. Het openstellen van informatie is een

	bewuste keuze.
Achtergrond	Security & privacy by default betekent dat in elke configuratie die wordt geïmplementeerd de aanwezige security & privacy opties standaard aan staan. Dit voorkomt ongewenste en ongecontroleerde toegang tot (persoons)gegevens. Openstellen van informatie is daarmee altijd een bewuste keuze na een zorgvuldige afweging.
Implicaties	Denk hierbij aan het definiëren van standaard rollen en het standaard beperken van autorisaties en het standaard beschermen van alle externe communicatie met SSL-technologie. Zie Bijlage A voor een overzicht van alle implicaties.

5. Governance Privacy en Security

5.1. Verantwoordelijkheid

Privacy en Security valt onder verantwoordelijkheid van de Directeur Informatisering/CIO en deze wordt hierin ondersteund door de Chief Information Security Officer (CISO) en de Functionaris Gegevensbescherming (FG). Informatisering faciliteert, geeft beleidsadviezen, handhaaft en heeft ook een toezichthoudende rol. De eindverantwoordelijkheid is belegd bij het College van Bestuur. De FG heeft een zelfstandige positie binnen de HG.

5.2. Rollen en hun inpassing

College van Bestuur

Het College van Bestuur is verantwoordelijk voor de informatiebeveiliging binnen de Hanzehogeschool en stelt het beleid en de governance op het gebied van informatieveiligheid vast. Informatieveiligheid komt zo vaak als nodig en minimaal 2x per jaar op de agenda van het bestuur. Het bestuur wijst een van haar leden aan als portefeuillehouder informatieveiligheid.

Directeur Informatisering / CIO[10] (Chief Information Officer)

De Directeur Informatisering/CIO is verantwoordelijk voor de portefeuille privacy & security. Hij legt hierover verantwoording af aan het CvB.

Functionaris Gegevensbescherming (FG)

De FG houdt binnen de Hanzehogeschool toezicht op de toepassing en naleving van de AVG zoals beschreven in het Bestuursreglement[11]. De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie in de instelling. De FG rapporteert aan de directeur informatisering/CIO en beschikt tevens over een rechtstreekse lijn met het CvB.

Chief Information Security Officer (CISO)

De CISO is een rol op strategisch (en tactisch) niveau. De CISO stelt het Securitybeleid op, helpt bij een juiste vertaling daarvan naar instellingsonderdelen, ziet toe op de (uniforme) naleving ervan en rapporteert over de effectiviteit van maatregelen en mogelijke afwijkingen. De CISO kan zowel gevraagd als ongevraagd advies geven. De Manager Vernieuwing is de hiërarchisch leidinggevende van de CISO. De rol van CISO is belegd bij één persoon.

[10] Chief Information Officer (CIO) is de benaming van de functie die gegeven wordt aan de persoon in een onderneming die verantwoordelijk is voor de informatie technologie en computer systemen.

[11] BESTUURSREGLEMENT (hanze.nl)

Dean/Directeur
De dean of directeur is eindverantwoordelijk (accountable) voor privacy & security binnen de *school*, kenniscentra of stafbureaus.

Contactpersoon Verantwoorde Informatiehuishouding (CVI)
De portefeuille privacy & security is in het MT belegd. De rol van Contactpersoon Verantwoorde Informatiehuishouding (CVI) is ingevuld door een MT-lid binnen het organisatieonderdeel.
De CVI legt verantwoording af (responsible) aan de dean/directeur(accountable).

Privacy Officer (PO)
De PO houdt zich binnen de Hanzehogeschool centraal of decentraal bezig met de toepassing en naleving van de AVG. Bijvoorbeeld bij het analyseren van (mogelijke) datalekken, het uitvoeren van een DPIA[12], het geven van advies op privacy vragen of bij het afsluiten van verwerkersovereenkomsten.

Teamleider (inclusief onderwijsverantwoordelijken)
Naleving van het Privacy en Securitybeleid is onderdeel van het integrale bedrijfsproces. Iedere leidinggevende heeft de taak om:

- Ervoor te zorgen dat hun medewerkers c.q. studenten op de hoogte zijn van (de voor hen relevante aspecten van) het beveiligingsbeleid;
- Toe te zien op de naleving van het beveiligingsbeleid door medewerkers en studenten;
- Periodiek het onderwerp informatiebeveiliging onder de aandacht te brengen in werkoverleggen;
- Als aanspreekpunt beschikbaar te zijn voor alle personeel gerelateerde informatiebeveiligingszaken.

Security Officer / Functionaris Informatiebeveiliging (SO/FIB)
De SO/FIB is een rol op tactisch (en indien nodig operationeel) niveau en is verantwoordelijk voor het actueel houden van het IT-Continuïteit Plan (ICP), het vertalen van securitybeleid naar operatie en uitvoeringsrichtlijnen en ziet toe op de realisatie hiervan. De SO/FIB voert technische audits uit op de IT-infrastructuur en geeft opdracht tot het verrichten van interne onderzoeken en audits en ziet toe op de implementatie van aanbevelingen. De SO/FIB adviseert bij besluitvorming met gevolgen voor informatiebeveiliging en voert risicoanalyses uit binnen zijn competentiegebied als vertegenwoordiger van de ICT-organisatie. De SO/FIB beoordeelt relevante rapportages en de afhandeling van security incidenten en zet acties uit op basis van bevindingen.

Een specifieke rol op het gebied van informatiebeveiliging die de SO/FIB heeft, is de CSIRT-coördinator[13] . De CSIRT-coördinator is verantwoordelijk voor information security incident management binnen de instelling, en het opstellen en bijhouden van het RFC-2350 document. In dat kader is de CSIRT-coördinator ook bevoegd om bijvoorbeeld tijdelijk computersystemen of netwerksegmenten te laten isoleren en kwaadaardige e-mailberichten uit mailboxen te verwijderen. Voor het uitvoeren van deze taken stuurt de CSIRT-coördinator het Hanze-CSIRT team aan bestaande uit, formeel benoemde, CSIRT-leden. Deze CSIRT leden voldoen aan het opgestelde profiel[14]

Proces- en systeemeigenaar
De systeemeigenaar en proceseigenaar zijn gezamenlijk verantwoordelijk voor het actief consulteren van de beveiligingsorganisatie in het geval van nieuwe systemen en processen en/of de uitbreiding hiervan.

[12] Data Privacy Impact Assessment of Gegevenbeschermingseffectbeoordeling

[13] Computer(/Cyber) Security Incident Response Team (ook wel CERT: Computer Emergency Response Team genoemd).

[14] Zie document Profiel Hanze-CSIRT medewerker.

Proceseigenaar

De proceseigenaar heeft een cruciale rol in het borgen dat de systemen de functionaliteit leveren die het proces nodig heeft.
De proceseigenaar:
• bepaalt hoe het proces moet lopen rekening houdend met de keten
• geeft aan welke (geautomatiseerde) functionaliteit er nodig is om het proces goed te bedienen
• bepaalt en bewaakt de proceseisen
• bepaalt welke delen al dan niet geautomatiseerd dienen te verlopen
• bewaakt de keten brede procesgang
• is eigenaar van primaire gegevens die in het proces verrijkt of vervaardigd worden
• bepaalt de benodigde brongegevens
• is verantwoordelijk voor datamanagement
• is inhoudelijk verantwoordelijk voor uit te voeren DPIA's op het betreffende proces
• stemt eisen m.b.t. informatievoorziening af met de domeineigenaar, de systeemeigena(a)r(en) en de demandmanagers.

Systeemeigenaar

Deze functionaris moet ervoor zorgen dat het systeem de benodigde functionaliteit levert voor alle processen die er gebruik van maken.
Verder moet de systeemeigenaar borgen dat:
• er voldaan wordt aan de centrale architectuurrichtlijnen zodat de doorontwikkeling van het systeem duurzaam en toekomstvast geschiedt (richtlijnen m.b.t. beveiliging, gegevensbeheer, integratie, infrastructuur…)
• hij eigenaarschap neemt van contracten met leveranciers en daarmee opdrachtgever is voor de contractmanager ten aanzien van aanschaf, exploitatie, beheer en onderhoud
• er releasebeleid (welke versie, wanneer) is rekening houdende met de impact ervan op gebruikers, systemen en infrastructuur en architectuurrichtlijnen
• er besloten wordt over nieuwe of uitbreiding van functionaliteiten zodat alle proceseigenaren worden bediend
• er bewaking is van de lifecycle van het systeem
• de benodigde middelen (exploitatiebudget en onderhoudsbudget) worden afgestemd met de Directeur informatisering/CIO.
• het exploitatie- en onderhoudsbudget bewaakt wordt.

5.3 Eindverantwoordelijkheid

Juridisch gezien is het CvB eindverantwoordelijk voor informatieveiligheid en daarmee ook voor Informatiebeveiliging van de instelling. Specifieke onderdelen van deze verantwoordelijkheid worden via de mandaatregeling bij de decanen/directeuren binnen de instelling verder belegd.

5.4 Taken, bevoegdheden, verantwoordelijkheden

De diverse taken, bevoegdheden en verantwoordelijkheden zijn onderverdeeld in Strategisch, Tactisch en Operationeel niveau.

In de volgende tabel zijn de taken, bevoegdheden en verantwoordelijkheden per niveau samengevat, aangevuld met de onderliggende documenten.

Niveau	Wat?	Wie?	Overleg	Documenten (rapportages, beleid)
Richtinggevend (strategisch)	• Bepalen strategie • Organisatie van informatiebeveiliging • IB-Jaarplan • Communicatie naar management en organisatie (awareness)	CvB (de portefeuillehouder Informatieveiligheid) op basis van advies CISO, FG en directeur informatisering/CIO	CvB stelt vast	• Privacy & Security beleid • Regeling ICT-voorziening • Jaarverslag Privacy & Security CvB & RvT
Sturend (tactisch)	Planning & Control IB: • Voorbereiden normen en wijze van toetsen • Evalueren beleid en maatregelen, ook van externe partijen bij contracten • Begeleiding interne assessments en externe audits • Communicatie naar proces- en systeem-eigenaren en IT-ondersteuning	• Proceseigenaren • Systeemeigenaren • FG • CISO • SO/FIB	Informatie-Beveiligings-overleg (IBO) (MT-INF+ FG, CISO, SO/FIB)	• Classificaties/Risicoanalyses en audits, inclusief DPIA's en SURFaudit • Jaarplan en-verslag P&S • ICT-richtlijnen
Uitvoerend (operationeel)	• Implementeren IB-maatregelen • Registreren en evalueren incidenten, inclusief datalekken • Communicatie eindgebruikers	• IT in samenwerking met proces- en systeemeigenaren • Functioneel beheer • SOC[15] • CSIRT[16] • PO • SO/FIB • CISO • FG	Operationeel IB-overleg CSIRT-overleg	• SLA's (security-paragraaf) • Incidentregistratie inclusief evaluatie • Procesrapportage

5.5. Bewustwording en training

Beleid en maatregelen zijn niet voldoende om risico's op het terrein van informatiebeveiliging uit te sluiten. De mens zelf creëert de grootste risico's. Bij de Hanzehogeschool werken we daarom voortdurend aan de vergroting van het beveiligingsbewustzijn van medewerkers om kennis van risico's te verhogen en veilig en verantwoord gedrag aan te moedigen. Onderdeel van het beleid zijn regelmatig terugkerende bewustwordingscampagnes voor alle medewerkers, studenten, derden en met name operationele beheerders. Verhoging van het beveiligingsbewustzijn is een verantwoordelijkheid van zowel de leidinggevenden, de CISO en de FG. Bewustwording is een onderdeel van het introductieprogramma voor nieuwe medewerkers en studenten.

[15] [SOC staat voor "Security Operations Center", meestal geleid door de CISM en inhoudelijk aangestuurd door CISO.]

[16] <Computer Security Incident Response Team / Computer Emergency Response Team>

5.6. Controle, oefenen, naleving en sancties

Bij de Hanzehogeschool zijn de CISO & FG verantwoordelijk voor de (planning van) privacy & security audits. De PO en SO ondersteunen hierbij.

De Hanzehogeschool neemt deel aan de SURFaudit selfassessment cyclus en de bijbehorende tweejaarlijkse benchmark. Daarnaast nemen we jaarlijks deel aan de OZON/NOZON oefening.

De bevindingen van de interne en externe controles en mogelijke externe eisen met betrekking tot beveiliging, zijn input voor de nieuwe jaarplannen van de Hanzehogeschool. Deze kunnen ook tot wijziging van het beleid leiden.

Controle op de naleving vindt plaats door toezicht te houden op hoe in de dagelijkse praktijk met informatiebeveiliging wordt omgegaan. Hierbij is het van belang dat CVI's samen met leidinggevenden (inclusief onderwijsverantwoordelijken) de medewerkers en studenten bewust maken op gebied van privacy & security. Voor het toezicht op de naleving van de AVG is de FG verantwoordelijk.

Als uit de controles blijkt dat de naleving ernstig tekortschiet, dan kan de Hanzehogeschool de betrokken verantwoordelijke medewerkers of studenten een sanctie opleggen. De sanctie wordt opgelegd binnen de kaders van de cao, arbeidsovereenkomsten, regeling ICT-voorzieningen en de wettelijke mogelijkheden in bijvoorbeeld de Wet op het hoger onderwijs en wetenschappelijk onderzoek (WHW). Primair is dit een verantwoordelijkheid van het College van Bestuur, maar dit kan in sommige gevallen worden gemandateerd aan de verantwoordelijke leidinggevenden (dean/directeur).

5.7. Financiering

Financiële middelen voor privacy & security worden structureel opgenomen in de diverse (project)begrotingen. De financiering van privacy & security wordt bij de Hanzehogeschool centraal geregeld.

Centraal

Algemene zaken, zoals het opstellen van een privacy & securityplan voor de instelling of een externe audit, worden uit de algemene middelen betaald via begroting INF. Instelling brede bewustwordingscampagnes en trainingen worden ook uit deze middelen betaald.

Decentraal

Alle decentrale aanvragen worden separaat beoordeeld en decentraal bekostigd.

6. Melding en afhandeling van incidenten

Een incident is een gebeurtenis die de bedrijfsvoering negatief kan beïnvloeden. Incidentbeheer en-registratie gaat over het detecteren, vastleggen en afhandelen van incidenten. Belangrijk hierbij is dat medewerkers, studenten en derden herkennen wanneer er sprake is van een incident of inbreuk op de informatiebeveiliging en dit ook melden.

Van incidenten kan worden geleerd. Incidentregistratie en periodieke rapportage over opgetreden incidenten horen dan ook thuis in een volwassen informatiebeveiligingsomgeving.

Security incidenten en (potentiële) datalekken kan men bij de Hanzehogeschool melden bij het Support Center (ict.supportcenter@org.hanze.nl). De Hanzehogeschool heeft de contactgegevens van dit meldpunt duidelijk gecommuniceerd naar haar medewerkers, studenten en derden.

Aan het privacy & security team kunnen vragen gesteld worden door deze te mailen naar ict-security@org.hanze.nl. *Dit betreft vragen die geen spoed hebben*.

Security incidenten dienen door het Support Center direct gemeld te worden aan het CSIRT-meldpunt (csirt@org.hanze.nl) en de CSIRT-beheerder van de dag.

Bij calamiteiten op gebied van privacy & security wordt het IT-Continuïteit Plan (ICP) gehanteerd.

Er is een vastgesteld beleid voor Responsible Disclosure. Daarmee geeft de Hanzehogeschool mogelijke melders van kwetsbaarheden in de informatiesystemen een garantie dat de Hanzehogeschool, onder voorwaarden, geen juridische stappen tegen hen onderneemt.

7. Vaststelling & wijziging

Het College van Bestuur stelt het privacy & security beleid vast dat de CISO & FG voorstelt. Het privacy & security beleid volgt de kaders van het instellingsbeleid. Het wordt 1x per 2 jaar geëvalueerd en zo nodig bijgesteld. Minimaal 1 keer per 4 jaar, of na een substantiële verandering van het instellingsbeleid of belangrijke ontwikkelingen op cyberveiligheidsgebied, wordt het beleid herzien en opnieuw vastgesteld.

Bijlage A – Informatiebeveiligingsprincipes

1	**Risico-gebaseerd** Informatiebeveiliging is risico-gebaseerd. 
Kern	We baseren de maatregelen op de mogelijke veiligheidsrisico's van onze informatie, processen en IT-faciliteiten.
Achtergrond	Het delen van kennis (openheid) is een belangrijke kernwaarde van het onderwijs- en onderzoekproces van de Hanzehogeschool. Voor een goede risicoafweging bij het beschermen van informatie en het treffen van de juiste maatregelen, is het van belang om de waarde van informatie vast te stellen. Als de waarde van informatie bekend is, kan ook de juiste mate van beveiliging worden bepaald, één die past bij de risico's. Proportionaliteit daarin is gewenst, ook om de beschikbare financiële middelen efficiënt te gebruiken ('Fit for purpose').
Implicaties	• De risico's worden ingeschat en vastgesteld op basis van een risicoclassificatie. • De Hanzehogeschool stelt een Classificatie Richtlijn vast. • Een gegevensbeschermingseffectbeoordeling (DPIA – Data Protection Impact Assessment) in het kader van de AVG maakt waar nodig onderdeel uit van de risicoanalyse. • Waar nodig worden maatregelen getroffen om het vastgestelde risico op beschikbaarheid, integriteit en vertrouwelijkheid te brengen naar het geaccepteerde niveau. • Informatie heeft één eigenaar. • Eigenaren van informatie, informatiesystemen, applicaties en processen zijn verantwoordelijk voor de implementatie en operationele handhaving van maatregelen onder het principe van "Pas toe of leg uit". • Afwijkingen kunnen worden geaccepteerd binnen de risicobereidheid (risk-appetite) van de Hanzehogeschool, uiteindelijk te bepalen door het CvB. • Voor afwijkingen moet het risico-acceptatieproces worden gevolgd, met acceptatie door de informatie-, proces- of applicatie-eigenaar. • De informatie-eigenaar (of eventueel ook de proces- of applicatie-eigenaar) tekent voor acceptatie van de risico's. • Maatregelen moeten zo worden ingericht dat hun effect controleerbaar is. • De hoogste risico's worden als eerste gemitigeerd. • Op basis van de risicoanalyse kan informatiebeveiliging voor gebruiksgemak kiezen. • Maatregelen moeten (qua kosten) in balans zijn met de vermindering van risico's (proportionaliteitsprincipe). • Informatie heeft één bron, waardoor eigenaarschap en "single point of truth" goed te duiden is. Hierdoor ontstaat ook een extra ketenverantwoordelijkheid voor de consequenties van wijzigingen bij de bron. • De Hanzehogeschool blijft verantwoordelijk voor adequate bescherming van informatie bij gebruik van externe diensten voor informatieverwerking.

	• Waar van toepassing bevatten contracten de veiligheidseisen en de levering van externe toetsing (assurance) die laat zien dat maatregelen effectief zijn.

2	**Iedereen** Informatiebeveiliging is een verantwoordelijkheid van iedereen. 
Kern	Iedereen is en voelt zich verantwoordelijk voor een juist en veilig gebruik van middelen en bevoegdheden.
Achtergrond	Iedereen is zich bewust van de waarde van informatie en handelt daarnaar. Deze waarde wordt bepaald door de mogelijke schade als gevolg van verlies van beschikbaarheid, integriteit of vertrouwelijkheid. Van zowel medewerkers, studenten als derden wordt verwacht dat ze bewust omgaan met informatie in welke vorm dan ook en dat ze actief bijdragen aan de veiligheid van de geautomatiseerde systemen en de daarin opgeslagen informatie. Het succes van beveiliging staat of valt met goede communicatie. Goede communicatie wordt daarom actief bevorderd, op en tussen alle niveaus in de instelling.
Implicaties	• Voor alle gebruikers van digitale informatievoorzieningen van Hanzehogeschool is een zogenaamde Acceptabel Use Policy (AUP) beschikbaar die is gepubliceerd via de website van Hanzehogeschool. Deze AUP is van toepassing op zowel studenten, medewerkers als derden. • Het veilig omgaan met informatie en informatiedragers is een onderdeel van de arbeidsovereenkomst van alle medewerkers. • Informatiebeveiliging krijgt aandacht bij indiensttreding van medewerkers en bij periodieke overleggen. • Informatiebeveiliging krijgt aandacht in reguliere overleggen bij onderwijs, onderzoek en afdelingen. • Medewerkers en studenten spreken elkaar aan op onveilige omgang met informatie en systemen. • Medewerkers en studenten melden (vermoedens van) kwetsbaarheden bij het CSIRT. • Schending van wetgeving, voorschriften en regels op gebied van informatiebeveiliging kan leiden tot sanctionerende maatregelen, door of namens het CvB, zoals vastgelegd in de gedragscodes.

3	**Altijd** Informatiebeveiliging is een continu proces. 
Kern	Informatiebeveiliging zit in het DNA van al onze werkzaamheden.

Achtergrond	De omgeving verandert continu; cyberdreigingen nemen toe en af; processen veranderen, medewerkers en studenten veranderen etc. Eenmalig de maatregelen bepalen en implementeren is onvoldoende om een veilig klimaat te behouden. Informatiebeveiliging heeft alleen zin als dit een continu proces is van het nemen van maatregelen, bewustzijn en controles.
Implicaties	• Periodiek worden audits en assessments uitgevoerd die het mogelijk maken het beleid en de genomen maatregelen te controleren op effectiviteit (controleerbaarheid). • Bij instroom van nieuwe medewerkers en studenten is er aandacht voor de bewustwording van de risico's en de beveiligingsprocedures van de Hanzehogeschool rond toegang en gebruik van IT-middelen. • Periodiek worden accounts met hoge privileges gevalideerd. • De Hanzehogeschool organiseert regelmatig cybersecurity-awareness activiteiten voor de diverse doelgroepen: studenten, medewerkers, leidinggevenden en partners van de Hanzehogeschool. • Bij aanpassingen in rollen, taken, en verantwoordelijkheden van een persoon worden ook de autorisaties daarmee in overeenstemming gebracht en aangepast. • Er wordt een proces ingericht om het dreigingsbeeld voor de Hanzehogeschool te bepalen en periodiek bij te stellen. Nieuwe dreigingen leiden waar nodig tot aanpassing van maatregelen.

4	**Security & Privacy by Design** Integrale aanpak informatiebeveiliging. 
Kern	Informatiebeveiliging is vanaf de start een integraal onderdeel van ieder project of iedere verandering m.b.t. informatie, processen en IT-faciliteiten.
Achtergrond	Security by design betekent dat al tijdens de start van een project, het ontwerp van een nieuwe applicatie of ICT-omgeving en bij technische of functionele veranderingen rekening wordt gehouden met de beveiliging van gegevens en de continuïteit van de processen. Dit voorkomt (vaak dure) herstelwerkzaamheden achteraf.
Implicaties	• Voor elk nieuw project/software-inkoop/innovatie worden de security-eisen (non-functional requirements) vanaf de start meegenomen. • Voor de livegang wordt de toepassing van de security-eisen getoetst en/of getest. • Bij elk IT-systeem of inrichting wordt ter bevordering van informatiebeveiliging het principe van 'minste rechten' gehanteerd. Dat betekent dat ernaar wordt gestreefd om niet meer rechten te verlenen dan nodig zijn voor adequate functie- en bedrijfsuitoefening. • Toegang tot systemen is gebaseerd op autorisatieschema's. • Scheiding van verantwoordelijkheden wordt toegepast in processen en procedures.

	• In het ontwerp wordt meegenomen dat het gebruik van informatie en IT-voorzieningen herleidbaar is tot een verantwoordelijke gebruiker. • Er wordt een richtlijn “security in projecten” vastgesteld, gebaseerd op de maatregelen die voortkomen uit de risicoclassificatie en maatregelen die mogelijk voortvloeien uit de gegevensbeschermingseffectbeoordeling (DPIA) in het kader van de AVG. • Bij procesontwerp worden maatregelen meegenomen die de continuïteit van het proces afdoende kunnen waarborgen.

5	**Security & Privacy by Default** Standaard beperkte toegang en veilige instellingen. 
Kern	Gebruikers hebben alleen toegang tot informatie en IT-faciliteiten die zij nodig hebben voor hun werkzaamheden. Het openstellen van informatie is een bewuste keuze.
Achtergrond	Security by default betekent dat in elke configuratie die wordt geïmplementeerd de aanwezige security opties standaard aan staan. Dit voorkomt ongewenste en ongecontroleerde toegang tot (persoons)gegevens. Openstellen van informatie is daarmee altijd een bewuste keuze na een zorgvuldige afweging.
Implicaties	• De beveiligingsbaseline van de standaardconfiguratie moet worden vastgelegd. (bv. het standaard beschermen van alle externe communicatie met SSL-technologie) • Het principe bij initiële inrichting van een informatiesysteem of een infrastructuur is “*gesloten, tenzij*”. • Afwijking van de initiële inrichting volgt het principe “Pas toe of leg uit.” • Security wordt geborgd in een changemanagementproces. • Toegang tot informatie is rol-gebaseerd, waardoor gebruikers alleen toegang hebben tot informatie en IT-faciliteiten die zij nodig hebben voor hun werkzaamheden (vastgelegd in een autorisatieschema). • Er worden enkele hoofdrollen geïdentificeerd op basis waarvan baseline-autorisaties worden toegekend. Te denken valt aan de hoofdrol student, medewerker, leverancier etc. Gebruikers krijgen standaard alleen deze rollen. • Logging- en auditprocessen worden zodanig ingeregeld dat toegang tot informatie en IT-faciliteiten herleidbaar is tot een verantwoordelijke gebruiker.

Bijlage B – BIV-Classificatie van data en systemen

De Hanzehogeschool volgt een risico gestuurde aanpak. Voor alle data die verwerkt wordt, wordt het risico bepaald door impact die een incident kan hebben en de kans dat een incident zich voordoet.

De impact wordt bepaald door de schade die een bepaalde dataset kan veroorzaken, door bijvoorbeeld de data te verliezen. De schade wordt vastgesteld door de data-eigenaar die de data in een bepaalde categorie indeelt. De risicobereidheid en de schade zijn een gegeven. De kans wordt bepaald door de maatregelen die genomen zijn om de data te beschermen. Aanvullende maatregelen verkleinen de kans. De CISO bepaald welke maatregelen geïmplementeerd moeten zijn zodat de kans en daarmee het restrisico naar een acceptabel laag niveau kan worden gebracht. Dit doen we aan de hand van de BIV-classificatie van data, processen en systemen.

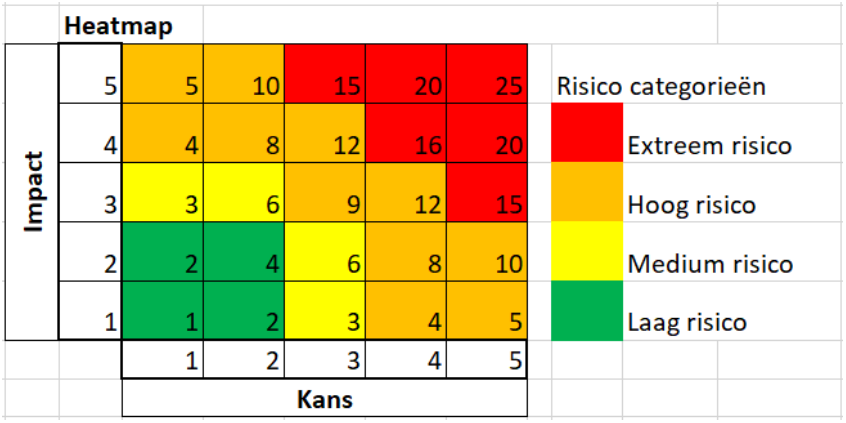
Bepalen schade / waarde

De eigenaar van de data heeft de eindverantwoordelijkheid voor de uitvoering van het inschatten van de waarde/schade en het selecteren van een gepast systeem om de data te verwerken. Schade kan worden veroorzaakt door de data kwijt te raken, maar ook door dat de data onbetrouwbaar is geworden of boetes vanwege onzorgvuldige omgang. De waarde van de data is het financiële gewin voor een derde als ongeautoriseerde toegang tot de data kan krijgen.
De eigenaar bepaalt de schade categorie op basis van de maximale schade/waarde van de data.
De eigenaar houdt bij het bepalen rekening met drie hoofdscenario's:

- Beschikbaarheid: De data is weg door een fout, storing of kwaadwillende.
- Integriteit: We kunnen niet meer garanderen dat de data niet is aangepast.
- Vertrouwelijkheid: De data is in handen van derden en deze kunnen er mee doen wat ze willen.

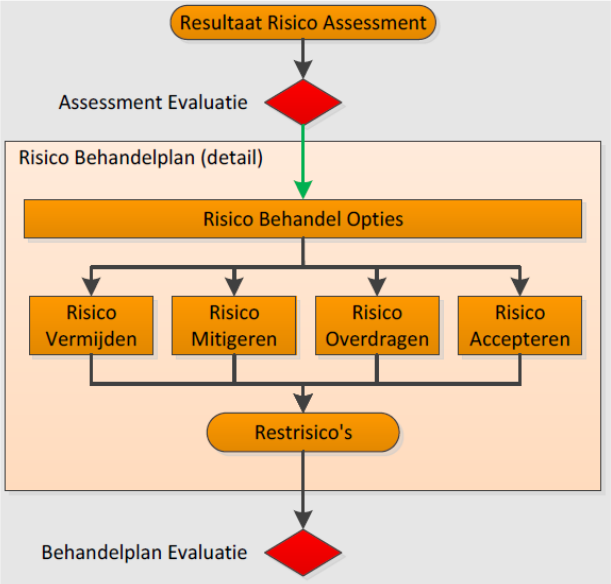
Risicoanalyse

Risicoanalyse wordt uitgevoerd via DPIA's op privacy gebied. De HG hanteert hierin het standaard format DPIA dat ontwikkeld is.
Op gebied van security risico's maken we gebruiken we onderstaande heatmap en wordt prioriteit bepaald op basis van Kans x Impact



	Kans
1	Onwaarschijnlijk - OF - eens per jaar
2	Zeldzaam - OF - eens per half jaar
3	Mogelijk - OF - per kwartaal tot maandelijks
4	Hoogstwaarschijnlijk - OF maandelijks tot wekelijks
5	Vrijwel zeker - OF Wekelijks tot dagelijks
	Impact
1	Onbelangrijk - OF - schade € 1 - € 1.000 - OF - 1 medewerker
2	Gering - OF - schade € 1.000 - € 10.000 - OF - <30 medewerkers
3	Groot - OF - schade € 10.000 - € 100.000 - OF - een afdeling
4	Aanzienlijks - OF - schade € 100.000 - € 1.000.000 - OF - meerdere afdelingen
5	Catastrofaal - OF - schade > € 1.000.000 - OF - Iedereen

Voor het behandelen van een risico kunnen we kiezen uit een 4 tal mogelijkheden:



Accepteren: Het risico kan geaccepteerd worden indien de (financiële) impact van een geëffectueerde bedreiging minimaal is en de kosten van het mitigeren van het risico hoger zijn dan de potentiële impact. Risico's die geaccepteerd worden geregistreerd in het risicoregister.

Overdragen/verzekeren: Dit is iets voor met name financiële risico's met een lage waarschijnlijkheid en een hoge (financiële) impact. De financiële gevolgen kunnen mogelijk verzekerd worden. Daar waar mogelijk zullen mitigerende maatregelen worden genomen om de impact te beperken.

Mitigeren: Dit betreft met name risico's uit de hiervoor bedoelde categorieën medium en hoog. Mitigatie van het risico naar een geaccepteerd niveau kan plaats vinden door het nemen van preventieve en corrigerende maatregelen.

Vermijden: Dit betreft uitsluitend risico's waarbij de (financiële) impact zo hoog is dat de continuïteit van het bedrijf in gevaar komt en waarbij één van de voorgaande behandel opties niet mogelijk is of kosten met zich meebrengt die hoger zijn dan het bijbehorende potentiële (financiële/commerciële) voordeel. Vermijden betekent in de praktijk het stoppen met de betreffende activiteiten.

Bijlage C - Documenten informatiebeveiliging

Voor informatiebeveiliging wordt bij de Hanzehogeschool dezelfde (PDCA-)managementcyclus gevolgd, die ook voor andere onderwerpen geldt. De (PDCA-)managementcyclus bestaat uit visie/idee, beleid, analyse, plan implementatie, uitvoering, controles en evaluatie.

In het kader van informatiebeveiliging hanteert de Hanzehogeschool de volgende documenten:

1. *Het Privacy & Security-beleid*
   Het beleid ligt ten grondslag aan de aanpak van (digitale) informatiebeveiliging binnen Hanzehogeschool. Het beleid wordt opgesteld door de CISO en FG en vastgesteld door het CvB.

2. *DPIA-format, werkinstructies.*

3. *Projectbrief Privacy & Security*
   Deze wordt jaarlijks opgesteld met hierin de belangrijkste projecten waarvoor financiering wordt aangevraagd. Projecten worden opgesteld n.a.v. de beleidsprincipes uit het overkoepelende beleid en landelijke ontwikkelingen op gebied van privacy & security.

4. *Jaarplan/verslag*
   De CISO en FG leveren, in lijn met de PDCA-cyclus, jaarlijks een verslag over het afgelopen jaar en een jaarplan voor het volgende jaar op aan het CvB en de RvT. Het jaarverslag is mede gebaseerd op de resultaten van de periodieke controles/audits. Er wordt o.a. ingegaan op incidenten, resultaten van risicoanalyses (inclusief genomen maatregelen) en andere initiatieven die het afgelopen jaar hebben plaatsgevonden. Waar nodig wordt apart aandacht besteed aan specifieke systemen/applicaties.
   Het jaarplan moet getoetst worden op de beschikbaarheid van resources (mensen en middelen), afgezet tegen de risico's die gemitigeerd moeten worden.

5. *Policies*
   Gedragscodes en richtlijnen op het gebied van informatiebeveiliging voor medewerkers, studenten en derden (al dan niet voor specifieke doelgroepen), zoals:
   - Acceptable Use Policy, voor het veilig gebruik van IT-voorzieningen, e-mail en internetgebruik door medewerkers, studenten en derden (Regeling ICT voorzieningen)
   - ICP
   - Publieksversie Privacy & Security Beleid 2021-2025
   - En andere gepubliceerde beleidsdocumenten op Hanze.nl

Daarnaast is informatiebeveiliging een vast onderdeel van de volgende documenten:

6. *Dienstenovereenkomsten (DVO's, SLA's), inhuur- en uitbestedingscontracten en eventueel bijbehorende verwerkersovereenkomsten*
   Bij de inhuur van personeel en bij de inkoop van middelen (met name hardware, software, applicatie/cloud platforms en diensten), wordt expliciet aandacht aan informatiebeveiliging besteed. Dit wordt gedaan door o.a. het Privacy en Securitybeleid toe te passen op externen en door beveiliging standaardonderdeel van de inkoopvoorwaarden te maken. Afspraken worden in een contract(en) met de leverancier vastgelegd. Het contract bevat standaard een informatiebeveiligingsparagraaf waarin de verantwoordelijkheden van de leverancier zijn opgenomen. De basis hiervoor is het SURF Juridisch Normenkader Cloudservices Hoger Onderwijs[17] die een informatiebeveiliging bijlage bevat.

17 https://www.surf.nl/binaries/content/assets/surf/nl/kennisbank/2013/juridisch-normenkader-cloudservices-hoger-onderwijs.pdf