hogeschool Windesheim

Informatiebeveiligingsbeleid



Datum: 2 november 2021
Vastgesteld door CvB dd. 7 december 2021
Revisiedatum: voor 1 november 2025

Het informatiebeveiligingsbeleid van Windesheim is gebaseerd op het model informatiebeveiligingsbeleid dat onderdeel is van het SCIPR framework voor informatiebeveiliging.

Meer informatie over SCIPR staat op https://www.scipr.nl

Het Model Informatiebeveiligingsbeleid is opgesteld door SCIPR en is gepubliceerd onder de licentie Creative Commons) NonCommercial, ShareAlike (CC BY-NC-SA 4.0)



Inhoud

Informatiebeveiligingsbeleid 1
Samenvatting 4
1. Inleiding 5
2. Wet- en regelgeving 6
3. Definitie, doelstelling, doelgroep en reikwijdte 6
3.1 Informatieveiligheid en Informatiebeveiliging 6
3.2 Doelstelling, randvoorwaarden en uitgangspunten 6
3.3. Doelgroep 8
3.4. Reikwijdte van het beleid 8
4. Beleidsprincipes informatiebeveiliging 8
4.1. Inleiding 8
4.2. Beleidsprincipes 9
5. Governance Informatiebeveiliging 12
5.1. Afstemming met samenhangende risico's 12
5.2. IB-Governance 12
5.2.1 Eerste en tweede lijn 12
5.2.2 De derde lijn 12
5.2.3 Eindverantwoordelijkheid 13
5.2.4 Taken, bevoegdheden, verantwoordelijkheden 13
5.3. Bewustwording en training 15
5.4. Controle, oefenen, naleving en sancties 16
6. Melding en afhandeling van incidenten en kwetsbaarheden 17
7. Vaststelling & wijziging 18
Bijlage A – Informatiebeveiligingsprincipes 19
Bijlage B - Wet- en regelgeving 24
Bijlage C - Documenten informatiebeveiliging 26
Bijlage D - Inrichting van CSIRT 28

Samenvatting

Het succes en de continuïteit van een organisatie hangt steeds meer af van informatie, nieuwe technologieën en geautomatiseerde procesketens. Die informatie moet goed worden beveiligd, zeker als er persoonsgegevens worden opgeslagen. In dit document is verwoord op welke manier Windesheim voorziet in adequate informatiebeveiliging en daarmee voldoet aan de relevante wet- en regelgeving.
Met het informatiebeveiligingsbeleid (IB-beleid) wil Windesheim 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.

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 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 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 Windesheim 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 de security werkgroep kunnen de Functionaris Gegevensbescherming en de interne auditor hier bijvoorbeeld adviezen voor geven.

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 is de Integrale Veiligheid (IV) governance van Windesheim weergegeven, waar de IB governance op aansluit. In de bijlagen ook een opsomming van documenten die van belang zijn op het gebied van informatiebeveiliging.

1. Inleiding

Het succes en de continuïteit van Windesheim hangen 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.

De digitale werkelijkheid is constant in beweging en dat brengt steeds nieuwe en andere risico's met zich mee voor de Informatieveiligheid. 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 Windesheim-diploma(certificaat), behaalde cijfers of de legitimiteit van onderzoekconclusies ondermijnen. Ook de privacy[1] van studenten, medewerkers en gasten en de reputatie van Windesheim kunnen worden geschaad. Informatiebeveiliging is daarom van cruciaal belang. Informatieveiligheid is niet vanzelfsprekend. Het vraagt om discipline, geld, inspanning en keuzes. Risicomanagement gaat immers niet over het compleet wegwerken van de risico's maar om het terugbrengen van risico's tot een voor de organisatie acceptabel niveau (Risk appetite). Dit beleidskader helpt daarbij.

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, medewerkers, studenten en gasten van Windesheim 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 beleid zijn om die reden vijf hoofdprincipes, leidend voor informatiebeveiliging binnen Windesheim, geformuleerd. De vast te stellen maatregelen, procedures en richtlijnen kunnen getoetst worden aan de vijf hoofdprincipes die in hoofdstuk 4 zijn beschreven.

Er is een belangrijke relatie tussen informatiebeveiligingsrisico's en risico's op andere gebieden, zoals privacy, safety[2] (arbowetgeving), veiligheid in onderwijs en onderzoek, fysieke beveiliging en business-continuïteit. Soms overlappen ze elkaar gedeeltelijk. Afstemming daarover vindt plaats in het integrale veiligheid overleg.

Windesheim heeft ervoor gekozen het beleid verwerking persoonsgegevens (privacy beleid) en het informatiebeveiligingsbeleid niet in één beleidsdocument te verenigingen. Goede informatiebeveiliging is weliswaar een voorwaarde om te kunnen voldoen aan de AVG (artikel 32) maar privacy beleid gaat ook in op zaken als informatieplicht, grondslagen voor verwerking, proportionaliteit en subsidiariteit, verantwoordingplicht (noodzaak tot verzamelen) en het waarborgen van rechten van betrokkenen.

[1] Voor het specifieke Privacy beleid van Windesheim zie https://liveadminwindesheim.sharepoint.com/:b:/r/sites/InfositeAlgemeen/CVB%20besluiten/Beleid%20Verwerking%20persoonsgegevens%20Windesheim%20(besluit%202017-047).pdf?csf=1&web=1&e=qCd5gE

[2] *Safety* wordt als verzamelterm gebruikt voor de verschillende aspecten van personele veiligheid: Arbo en milieu, sociale veiligheid, bedrijfshulpverlening e.d.

2. Wet- en regelgeving

Windesheim streeft ernaar om in al haar processen en procedures te voldoen aan de relevante wet- en regelgeving. Bepaalde wetgeving is heel direct te vertalen in uitvoering en moet gevolgd worden. Er is ook wet- en regelgeving waarbij de uitvoering niet direct uit de wet volgt. Dit wordt ook wel een “open norm” genoemd. De AVG is zo’n “open norm”. Het stelt wel regels maar de exacte invulling van de regels volgt niet altijd direct uit de wet. Zo begint artikel 32.1 van de AVG: *Rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen, treffen de verwerkingsverantwoordelijke en de verwerker passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen, die, waar passend, onder meer het volgende omvatten:*.
Bij de invulling van dit soort open normen is Windesheim in staat zich te verantwoorden voor de keuzes die ze maakt..

3. Definitie, doelstelling, doelgroep en reikwijdte

3.1 Informatieveiligheid en Informatiebeveiliging

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.

Informatiebeveiliging richt zich op drie kwaliteitsaspecten:

- Beschikbaarheid: de mate waarin gegevens of functionaliteit op de juiste momenten beschikbaar zijn voor gebruikers;
- Integriteit: de mate waarin gegevens of functionaliteit juist, volledig en actueel zijn;
- Vertrouwelijkheid: de mate waarin de toegang tot gegevens of functionaliteit beperkt is tot degenen die daartoe bevoegd zijn.

Hierbij gaat het ook om de controleerbaarheid (bijvoorbeeld via logging) van de maatregelen die genomen zijn om deze kwaliteitsaspecten te borgen.

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)
- Het waarborgen dat informatie alleen toegankelijk is voor personen die vanuit hun rol/functie daar toegang tot mogen hebben (vertrouwelijkheid).
- Het voorkomen van beveiligings- en privacy-incidenten en het beperken van de impact van mogelijke incidenten.

Met het informatiebeveiligingsbeleid (IB-beleid) wil Windesheim 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 IB-beleid sluit daarmee aan bij de missie en waarden

van de instelling[3].

Het IB-beleid, en de opvolging daarvan, moet Windesheim in staat stellen aantoonbaar 'in control' en compliant te zijn. Op basis daarvan kunnen de betrokken directeuren samen met het College van Bestuur verantwoording afleggen 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 Windesheim 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.
- *Risk based en Procesbenadering*
  Informatiebeveiliging is een continu proces inclusief PDCA cyclus. Periodiek worden er risicoanalyses en audits uitgevoerd. De resultaten hiervan worden opgenomen in vastgestelde IVT 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' (Surf Normenkader) vastgesteld. Het Surf Normenkader is gebaseerd op de normen die zijn vastgelegd in de ISO-27000-serie[5]. Windesheim hanteert het Surf Normenkader als basis voor haar informatiebeveiliging. Formele certificering, bijvoorbeeld volgens de norm ISO 27001, wordt niet als noodzakelijk gezien voor Windesheim. Dit is een intensief en kostbaar traject en er is geen externe noodzaak om als hoger onderwijsinstelling hieraan te voldoen.
- *Volwassenheid*
  Het SURF Normenkader omschrijft een norm voor de volwassenheid van de Informatiebeveiliging volgens het Capability Maturity Model (CMM)[6]. Windesheim streeft naar een volwassenheidsniveau volgens de SURF-richtlijnen (gemiddeld niveau 3).
- *Maatregelen*
  Windesheim 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] Alles over de Strategische Koers - Introductiepagina (sharepoint.com)

[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] ISO/IEC 27000-series - Wikipedia

[6] Capability Maturity Model- Wikipedia

3.3. Doelgroep

Het IB-beleid is bestemd voor iedereen die – intern of extern – te maken heeft met de bedrijfsprocessen van Windesheim. Het beleid richt zich in eerste instantie op het bestuur, hoger management, proceseigenaren, product owners en leidinggevenden. Zij dragen uit dat het beleid van toepassing is op alle medewerkers, docenten, studenten, bestuurders, gasten, bezoekers en externe relaties.

3.4. Reikwijdte van het beleid

Bij Windesheim wordt informatieveiligheid breed geïnterpreteerd. Het gaat over alle vormen van formeel vastgelegde informatie (dus niet alleen digitale informatie), die de instelling of haar relaties genereren en beheren. 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 Windesheim kan aanspreken.

Het IB-beleid heeft betrekking op alle medewerkers, studenten, gasten en externe relaties alsmede alle organisatieonderdelen.
Het gaat over alle door Windesheim beheerde apparaten en applicaties waarmee geautoriseerde toegang tot (diensten van) het Windesheim-netwerk kan worden verkregen en/of waarmee data van de instelling wordt verwerkt. Het heeft betrekking op zowel processen, applicaties/functionaliteit, data als de infrastructuur.

Windesheim faciliteert in beperkte mate het gebruik van privéapparaten (BYOD[7]). Het gebruik van BYOD op het Windesheim-netwerk voor toegang tot applicaties of informatie van de instelling valt onder dit IB-beleid.

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

4. Beleidsprincipes informatiebeveiliging

4.1. Inleiding

Windesheim is een instelling met een open karakter. Vanuit het onderwijs- en onderzoeksperspectief is de insteek "*Open waar mogelijk, gesloten waar nodig*". Adequate beveiliging van informatie is steeds een randvoorwaarde en het openstellen van informatie moet een bewuste keuze zijn.

Windesheim heeft vijf beleidsprincipes voor informatiebeveiliging vastgesteld. Deze helpen om te bepalen welke beveiligingsmaatregelen er nodig zijn. Een beleidsprincipe bestaat uit:

- Een titel (vaak verklarend).
- Een korte uitleg (de achtergrond).
- De implicaties die uit het beleidsprincipe volgen als basis voor de te nemen maatregelen.

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

De uiteindelijk door de instelling vastgestelde maatregelen zijn niet altijd 1-op-1 toepasbaar in alle situaties. Soms zijn er bijvoorbeeld processen die afwijken of bestaan er technische of organisatorische beperkingen. In die gevallen moeten er vervangende maatregelen worden genomen waarmee het achterliggende principe

[7] Bring Your Own Device

tot zijn recht komt en de risico's voldoende worden afgedekt, volgens het uitgangspunt "Pas toe of leg uit"[8].

Om tot een goede afweging te komen of vervangende maatregelen inderdaad tot een acceptabel restrisico leiden, moeten ze aan het IB-beleid van Windesheim worden getoetst. Met de beleidsprincipes en hun implicaties voor informatiebeveiliging uit dit hoofdstuk kan die toetsing plaatsvinden, ook al zijn vervangende maatregelen niet uitputtend in het beleid of in baselines vastgelegd.

4.2. Beleidsprincipes

De vijf hierna vermelde beleidsprincipes helpen bij de implementatie van het IB-beleid.
Op basis van deze vijf beleidsprincipes kunnen maatregelen worden geformuleerd die relevant zijn voor de bescherming van processen van Windesheim. De beleidsprincipes vormen de basis voor de communicatie rondom het IB-beleid van Windesheim. In bijlage C zijn deze verder in detail uitgewerkt.

Allerlei onderdelen die uit het IB-beleid volgen, kunnen ter toetsing langs de beleidsprincipes worden gehouden. Denk daarbij aan:

- Richtlijnen voor projectmatig werken, werkinstructies en awareness-programma's.
- Classificatie waarmee een risicoanalyse kan worden uitgevoerd als basis voor technische en organisatorische maatregelen.

Ook zijn de beleidsprincipes bedoeld om als basis te gebruiken voor de toetsing van uitzonderingen of keuzes bij onvoorziene omstandigheden.

De vijf door Windesheim vastgestelde beleidsprincipes zijn:

1. Risico-gebaseerd
2. Iedereen
3. Altijd
4. Security by Design
5. Security by Default

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 Windesheim. Voor een goede risicoafweging bij het beschermen van informatie (en kennis) 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

[8] "pas toe" gaat over de specifieke maatregelen, voor "leg uit" dienen de principes als referentie.

	financiële middelen efficiënt te gebruiken (‘Fit for purpose’).
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 het veiligheid houden daarvan. Medewerkers en studenten durven elkaar aan te spreken op onveilig gedrag en helpen elkaar veilig te werken.
Implicaties	Denk hierbij aan het vastleggen van afspraken in arbeidsvoorwaarden, omgangsvormen, gedragscodes en huisregels, etc. Leidinggevende heeft een voorbeeld functie. Hij instrueert, stimuleert, motiveert, coacht, monitort en sanctioneert. Zie bijlage A voor een overzicht van alle implicaties.

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, creëren van bewustzijn en uitvoeren van controles.
Implicaties	Denk hierbij aan het houden van awareness campagnes en het inrichten van een audit-proces. Zie bijlage A voor een overzicht van alle implicaties.

4	**Security by Design** Integrale aanpak informatiebeveiliging 
Kern	Informatiebeveiliging is vanaf de start een integraal onderdeel van ieder project of iedere verandering in informatie, processen en IT.
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	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 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	Denk hierbij aan het definiëren van standaard rollen en het standaard beperken van autorisaties en het standaard beschermen van alle externe communicatie middels versleuteling. Zie bijlage A voor een overzicht van alle implicaties.

5. Governance Informatiebeveiliging

5.1. Afstemming met samenhangende risico's

Binnen Windesheim is aandacht voor alle soorten risico's en hun onderlinge samenhang. Om die reden besteedt Windesheim op strategisch niveau veel aandacht aan afstemming van informatiebeveiliging, Arbo veiligheid, fysieke beveiliging, business-continuïteit en privacybescherming (integrale veiligheid). Waar mogelijk en nodig vertaalt deze afstemming zich ook naar het tactische en operationele niveau. De governance rondom informatiebeveiliging wordt daarom binnen Integrale Veiligheid (IV) in gezamenlijkheid opgepakt. De governance ten aanzien van Integrale veiligheid is vastgelegd in het document "20180601 Visie en governance integrale veiligheid versie 2018".

Dit hoofdstuk gaat in op de governance van de informatieveiligheid en informatiebeveiliging (hierna IB-Governance genoemd) als onderdeel van de IV-Governance van Windesheim.

5.2. IB-Governance

De IB-Governance bij Windesheim is ingericht volgens het zogenaamde Three Lines of Defence model[9] (ook wel '3LoD'). Dit model wordt algemeen toegepast als model om Governance, Risk en Compliance (GRC) te borgen in een operationele organisatie. Het beschrijft niet alleen de rollen binnen de organisatiestructuur, maar ook hun onderlinge samenwerking.

5.2.1 Eerste en tweede lijn

Het 3LoD-model heeft als uitgangspunt dat het lijnmanagement (de business) verantwoordelijk is voor haar eigen processen. De directeuren zorgen ervoor dat beveiligingsmaatregelen ook werkelijk worden geïmplementeerd, dat awareness-programma's worden uitgevoerd, dat personeel wordt opgeleid, etc. Dit is de eerste lijn.

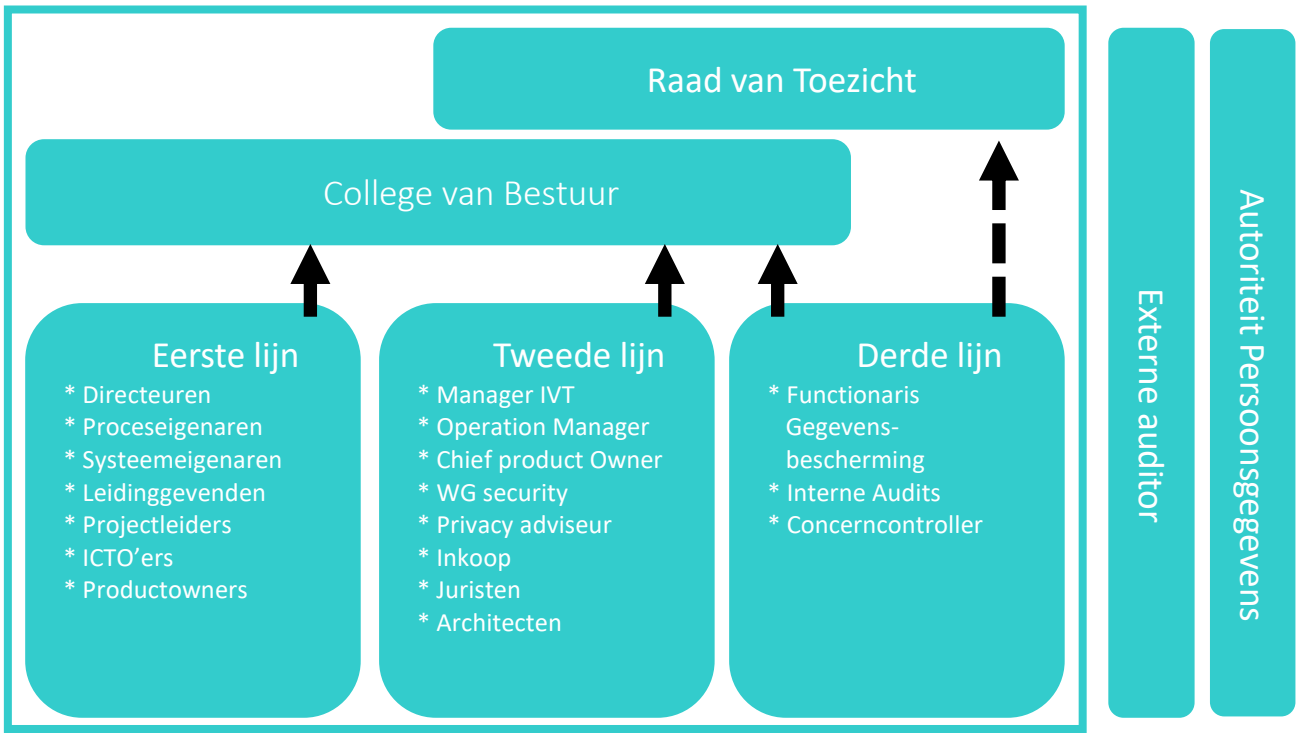
Daarnaast moet er een functie zijn die de eerste lijn ondersteunt, adviseert, coördineert en die bewaakt of het management zijn verantwoordelijkheden ook daadwerkelijk neemt. Dit is de tweede lijn. Ook bepaalde beleidsvoorbereidende taken, het organiseren van de PDCA-cyclus, van integrale risicoanalyses en self-assessments en het opstellen van jaarplannen en rapportages zijn taken van de tweede lijn.

5.2.2 De derde lijn

Het is wenselijk dat er binnen de organisatie een functie bestaat die controleert of het samenspel tussen de eerste en tweede lijn soepel functioneert en daarover een objectief, onafhankelijk oordeel velt met mogelijkheden tot verbetering. Daarbij kijkt men ook of er geen overlapping is en of er blinde vlekken bestaan. Deze functie is de derde lijn.

De binnen de AVG verplichte Functionaris Gegevensbescherming (FG), de afdeling Interne Audits en de concerncontroller behoren tot de derde lijn. Beiden opereren volledig los van alle andere organisatieonderdelen en rapporteren niet alleen aan het College van Bestuur, maar informeren ook de Raad van Toezicht.

[9] https://www.icas.com/ca-today-news/internal-audit-three-lines-of-defence-model-explained



Schema: Three Lines of Defence, vertaald naar Windesheim

5.2.3 Eindverantwoordelijkheid

Het CvB is eindverantwoordelijk voor informatieveiligheid en daarmee ook voor Informatiebeveiliging van de instelling. De directeur Bedrijfsvoering heeft een gedelegeerde verantwoordelijkheid voor de Integrale Veiligheid en is daarmee ook voor informatiebeveiliging.
De rol van Chief information security officer is gedelegeerd aan de manager IVT. De CISO is verantwoordelijk voor het IB-beleid, helpt bij een juiste vertaling daarvan naar instellingsonderdelen en ziet toe op de (uniforme) naleving ervan. In kader daarvan kan hij audit (laten) uitvoeren.

5.2.4 Taken, bevoegdheden, verantwoordelijkheden

In deze paragraaf wordt alleen de specifiek IB Governance aanvulling op de Governance Integrale Veiligheid beschreven.

Binnen de afdeling IVT zijn een tweetal overlegstructuren geïntroduceerd die zich primair met Informatiebeveiliging bezig houden:

- IVT security overleg (Identity en Access Management deskundige, Product owner Infrastructuur, Security Architect, Adviseur Security & Privacy)
- Security overleg (leden van IVT security overleg, Manager IVT/CISO, Operations manager, afhankelijk van agenda ook anderen vanuit IVT)

De security architect is tevens coördinator van het CSIRT (Computer security incident respons team, bestaande uit infra medewerkers en indien nodig aangevuld met andere disciplines) en de manager IVT is tevens voorzitter van het crisis ondersteuningsteam IVT (bestaande uit manager IVT en de Operationsmanagers) en heeft ten tijde van crisis zitting in het CMT.

De twee hierboven genoemde overleggen bevinden zich op strategisch/tactisch niveau.

Doel van het IVT security overleg (wekelijks):

- Zichthouden op marktontwikkelingen en dreigingslandschap
- Signaleren en analyseren bedreigingen/ zorgen dat onderwerpen op de agenda komen
- Formuleren verbetervoorstellen
- Formuleren beleidsvoorstellen/richtlijnen vanuit IB-beleid
- Toezicht naleving IB beleid (signaal functie richting Security Overleg)
- PDCA cyclus rondom incidenten borgen (zie hoofdstuk 6)

Doel van het Security Overleg (6 wekelijks):

- Bespreken incidenten
- Beoordelen analyses
- Prioritering activiteiten
- Vaststellen richtlijnen
- Goedkeuren van beleid dat ter vaststelling naar CvB moet

Beleid wordt voorbereid vanuit IVT en wordt via de directeur dienst Bedrijfsvoering met de portefeuillehouder IV besproken en ter vaststelling voorgelegd aan het CvB na besproken te zijn in het directeuren overleg (strategisch). De vertaling hiervan naar richtlijnen en architectuur wordt binnen IVT gerealiseerd.

(Chief) Product owners, systeemeigenaren en proceseigenaren zijn er samen voor verantwoordelijke dat beveiligingsmaatregelen genomen worden binnen de kaders die architectuur hiervoor heeft gesteld. Zij dienen er ook voor te zorgen dat classificaties/risico analyses en eventueel DPIA's worden uitgevoerd. Voor de centrale systemen is IVT de systeemeigenaar.

Niveau	Wat?	Wie?	Documenten
Richtinggevend (strategisch)	• Bepalen IB-strategie • Organisatie voor IB inrichten • IB planning en control vaststellen • Business continuity management • Communicatie naar management en organisatie	Bestuur (de portefeuillehouder Informatieveiligheid) op basis van advies IVT Security Overleg	• IB beleid • Privacybeleid • Gedrag- en Integriteitscode • Classificatierichtlijn
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 • Chief Product Owners • IVT security overleg	• Classificaties/Risicoanalyses en audits, inclusief DPIA's en SURFaudit • IB baselines (basismaatregelen) • Jaarplan en-verslag • Noodscenario's
Uitvoerend (operationeel)	• Implementeren IB-maatregelen. • Registreren en evalueren incidenten, inclusief datalekken • Communicatie eindgebruikers	• IVT in samenwerking met proces- en systeemeigenaren • Functioneel beheer • Product owners • CSIRT[10]	• SLA's (security-paragraaf) • Incidentregistratie inclusief evaluatie •

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

Documenten

Voor informatiebeveiliging wordt bij Windesheim dezelfde (PDCA-)managementcyclus gevolgd, die ook voor andere onderwerpen geldt: visie/idee, beleid, analyse, plan implementatie, uitvoering, controles en evaluatie. Die cyclus wordt op de verschillende niveaus ondersteund door een aantal formeel vastgestelde documenten. In bovenstaande tabel staan een aantal daarvan benoemd.
De security rapportage aan het CvB is opgenomen in de 4-maands rapportage Integrale veiligheid.
In bijlage C is een uitgebreider overzicht opgenomen van de documenten die Windesheim voor informatiebeveiliging hanteert.

5.3. 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 en is daardoor een wezenlijk onderdeel van de beveiliging. Bij Windesheim 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.
Om tot daadwerkelijk gedragsverandering te komen is het niet alleen van belang dat mensen weten wat er van hen verwacht wordt maar ook dat ze gemotiveerd zijn en gefaciliteerd worden om het gewenste gedrag te vertonen.
Naast kennis en kunde is voorbeeldgedrag van hoger management en direct leidinggevende belangrijk voor het realiseren van een gedragsverandering. Er is een sterke relatie tussen de sociale norm en het gedrag dat vertoond wordt. Het onderling bespreekbaar maken van en elkaar kunnen aanspreken op onveilig handelen draagt bij aan een cultuur waarin Windesheimers zich gezamenlijk verantwoordelijk voelen en "veilig handelen" de sociale norm wordt. Ook handhaving, waarderen van goed gedrag en bestraffen van ongewenst gedrag, is van belang. Hoe beter de handhaving, hoe meer mensen geneigd zijn te doen wat wordt beloond.

Leidinggevenden hebben dus een belangrijke rol in het tot stand brengen van gedragsverandering. Zij zijn er voor verantwoordelijk in werkoverleggen en PE-gesprekken ook onderwerpen als veiligheid en privacy te bespreken. Zij dienen voorbeeldgedrag te vertonen en medewerkers aan te zetten tot het volgen van trainingen op dit gebied. De eLearning "Digitaal Brevet voor medewerkers" van Surf is daar een goed middel toe.

Binnen de afdeling IVT en onze organisatie dienen security trainingen niet alleen gericht te zijn op de medewerker als gebruiker maar ook op professionalisering binnen de specifieke functie die de medewerker vervult (ontwikkelaar, functioneel beheerder, infrastructuurbeheerder, docent, onderzoeker, bedrijfsbureaumedewerker, etc.).

Organiseren van bewustwording onder studenten is in beginsel de verantwoordelijkheid van de Domeinen. Ook hiervoor is centraal materiaal beschikbaar in de vorm van een eLearning "Digitaal Brevet voor studenten".

Onderdeel van het beleid zijn regelmatig terugkerende bewustwordingscampagnes voor alle medewerkers, studenten, derden en met name operationele beheerders. In oktober, de maand van de veiligheid, zal elk jaar vanuit de werkgroep IV centraal bewustwordingscampagnes geïnitieerd worden.
Gedurende het jaar zullen bewustwordingsactiviteiten ook aansluiten op de actualiteit en indien nodig op specifieke doelgroepen gericht zijn (onderzoekers, docenten, medewerkers financiën of bedrijfsbureaus, e.a.).

Verhoging van het beveiligingsbewustzijn is een verantwoordelijkheid van zowel de leidinggevenden, de MT leden met portefeuille risicomanagement en integrale veiligheid als de werkgroep IV. Bewustwording is een onderdeel van het introductieprogramma voor nieuwe medewerkers en studenten.

5.4. Controle, oefenen, naleving en sancties

Bij Windesheim is de manager IVT in de rol van CISO verantwoordelijk voor de (planning van) interne IT audits en voor de controle op de uitvoering van de informatiebeveiligingsplannen. Het IVT security Overleg ondersteunt daarbij.

De interne controles vinden jaarlijks plaats en worden naast de reguliere formele audits aangevuld met diverse incidentele activiteiten, zoals het nemen van steekproeven, het uitvoeren van penetratietesten en het controleren van de feitelijke werking van de vastgestelde beveiligingsmaatregelen. Daarnaast worden vaardigheden en operationele procedures regelmatig getest in brainstormsessies of oefeningen. Voorbeelden hiervan zijn informatiebeveiligings-/CSIRT-firedrills[11]. Hiertoe wordt jaarlijks een OTO plan (OTO=Ontwikkelen, trainen, oefenen) opgesteld (CISO verantwoordelijk).

De informatiesystemen (of-processen) van Windesheim worden intern geaudit. De audit richt zich op (1) de classificatie van de in het informatiesysteem vastgelegde gegevens (2), de inventarisatie van de risico's (3), de genomen beveiligingsmaatregelen en (4) de samenhang tussen 1, 2 en 3. Voor elk informatiesysteem wordt een audit frequentie vastgesteld aan de hand van de risicoclassificatie. Als een informatiesysteem wordt vervangen of als er belangrijke wijzingen plaatsvinden in de beveiliging, wordt er een audit uitgevoerd op basis van een nieuwe businessimpact en risicoanalyse.

Het normenkader IBHO (zie hoofdstuk 3) wordt gebruikt als uitgangspunt voor interne en externe controles. Voor de audits van specifieke onderdelen of van informatiesystemen kunnen aanvullende, meer gedetailleerde, normen worden vastgesteld.

Windesheim neemt deel aan de SURFaudit selfassessment cyclus en de bijbehorende tweejaarlijkse benchmark. Minimaal eens per 4 jaar wordt een SURF Peerreview aangevraagd.

De bevindingen van de interne en externe controles en mogelijke externe eisen met betrekking tot beveiliging, zijn input voor de nieuwe jaarplannen van Windesheim. Deze kunnen ook tot wijziging van het IB-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 leidinggevenden (inclusief onderwijsverantwoordelijken) de medewerkers en studenten aanspreken op tekortkomingen. Voor het toezicht op de naleving van de AVG is de 'Functionaris voor Gegevensbescherming' (FG) verantwoordelijk.

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

[11] Als voorbeeld gelden de (N)OZON oefening die jaarlijks door SURF worden gecoördineerd.

6. Melding en afhandeling van incidenten en kwetsbaarheden

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. De PDCA cyclus rondom incidentbeheer is geborgd in het wekelijkse IVT Security Overleg en de 4 maandelijkse rapportage aan het CvB.

Incidenten kan men bij Windesheim melden bij het CSIRT@windesheim.nl of bij de Servicedesk . Windesheim heeft de contactgegevens van dit meldpunt duidelijk gecommuniceerd naar haar medewerkers, studenten en derden.

Een kwetsbaarheid is een fout in een digitaal systeem die het mogelijk maakt voor hackers om een aanval te plegen. Kwetsbaarheden die door leveranciers gemeld worden zijn vaak voorzien van een CVSS score[12]. Bij een hoge CVSS score wordt door CSIRT direct actie ondernomen.

Een datalek is een inbreuk op de beveiliging van persoonsgegevens die per ongeluk of op onrechtmatige wijze leidt tot vernietiging, verlies, wijziging of ongeoorloofde toegang tot die persoonsgegevens.

Iedere medewerker, student en derde kan kwetsbaarheden, incidenten en inbreuken op de informatiebeveiliging, inclusief datalekken melden en wordt dit ook geacht te doen. Melden kan bij CSIRT@windesheim.nl of de Servicedesk.

De incidenten worden afgehandeld volgens het door Windesheim vastgestelde Incident managementproces, waar de afhandeling van datalekken een onderdeel van is. Security incidenten worden behandeld door het Computer Security Incident Respons Team (CSIRT, zie bijlage D). De taken en bevoegdheden van dit team staan beschreven in de “RFC-2350 voor Windesheim CSIRT” en is gepubliceerd op de website.

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

[12] Common Vulnerability Scoring System SIG (first.org)

7. Vaststelling & wijziging

Het College van Bestuur stelt het IB-beleid vast. Het wordt 1x per 4 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.

Dit beleid, is vastgesteld door het bestuur van Windesheim op 7 december 2021 en kan worden aangehaald als “Informatiebeveiligingsbeleid van Windesheim”.

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 Windesheim. 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	• Voor alle processen worden een risico analyses uitgevoerd of de risico's worden ingeschat en vastgesteld op basis van een risicoclassificatie • Windesheim 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 Windesheim, uiteindelijk te bepalen door het bestuur. • De informatie-eigenaar (of eventueel ook de proces- of applicatie-eigenaar) tekent voor acceptatie van de risico's. Privacy risico's dienen op het niveau van CvB te worden geaccepteerd. • 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. • Windesheim 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 Windesheim is een zogenaamde ICT reglement beschikbaar dat is gepubliceerd via het intranet van Windesheim. Deze ICT reglementen zijn van toepassing op zowel studenten, medewerkers als derden. • Het veilig omgaan met informatie en informatiedragers is een onderdeel van de <aanstelling/arbeidsovereenkomst> van alle medewerkers. • Informatiebeveiliging krijgt aandacht bij indiensttreding van medewerkers en bij <Jaargesprekken/Periodieke overleggen> • Informatiebeveiliging krijgt aandacht in reguliere overleggen in afdelingen en projecten. • Medewerkers en studenten spreken elkaar aan op onveilige omgang met informatie en systemen. • Medewerkers en studenten melden (vermoedens van) kwetsbaarheden bij het CSIRT • Er is een door het bestuur vastgesteld Responsible Disclosure beleid. • 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	• Er wordt een Information Security management Systeem ingericht waarmee door middel van een PDCA-cyclus alle aspecten van het IB-beleid adequaat worden opgevolgd. • 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 Windesheim rond toegang en gebruik van IT-middelen. • Periodiek worden accounts met hoge privileges gevalideerd. • Windesheim organiseert regelmatig cybersecurity-awareness activiteiten voor de diverse doelgroepen: studenten, medewerkers, leidinggevenden en partners van Windesheim. • 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 Windesheim te bepalen en periodiek bij te stellen. Nieuwe dreigingen leiden waar nodig tot aanpassing van maatregelen.

4	Security by Design Integrale aanpak informatiebeveiliging 
Kern	Informatiebeveiliging is vanaf de start een integraal onderdeel van ieder project of iedere verandering mbt 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. • Software ontwikkeling verloopt via het CI/CD concept waar security testen een integraal onderdeel van uitmaakt. • 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. • Bij procesontwerp worden maatregelen meegenomen die de continuïteit van het proces afdoende kunnen waarborgen.

5	Security 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 - Wet- en regelgeving

Deze bijlage geeft een overzicht van de belangrijkste aan informatieveiligheid gerelateerde wet- en regelgeving met specifieke aandachtspunten voor Windesheim.

1. Wet op het Hoger onderwijs en Wetenschappelijk onderzoek (WHW)
   Windesheim heeft een kwaliteitszorgsysteem conform de Instelling Toets Kwaliteitszorg (ITK). Hierin is (onder meer) het zorgvuldig omgaan met gegevens in de studentenadministratie en met de studieresultaten gewaarborgd. Daarnaast worden integriteitscodes voor wetenschappelijk onderzoek nageleefd en toegepast.

2. Algemene Verordening Gegevensbescherming (AVG)
   De instelling heeft een separaat beleid voor verwerking van persoonsgegevens vastgesteld waarin naleving van de AVG wordt geborgd. Naleving van het informatiebeveiligingsbeleid en het beleid voor verwerking van persoonsgegevens inclusief de daarin vermelde technische en organisatorische maatregelen zorgen samen voor het voldoen aan de AVG.

3. Wettelijke Bewaartermijnen/Archiefwet
   Windesheim houdt zich aan de wettelijke voorschriften ten aanzien van bewaartermijnen, zoals die zijn vastgelegd in specifieke wetgeving (zoals de Belastingwet en in het arbeidsrecht) en in de Archiefwet en het Archiefbesluit. Windesheim hanteert daarbij de Selectielijst Hogescholen zoals vastgesteld door de Vereniging Hogescholen.

4. Auteurswet
   Windesheim respecteert auteursrechten en handelt daarnaar.

5. Telecommunicatiewet (wordt straks ePrivacy verordening)
   Omdat de doelgroep van Windesheim voldoende afgebakend is worden de netwerkvoorzieningen van Windesheim niet aangemerkt als een openbaar netwerk in de zin van de Telecommunicatiewet. Het onderdeel ten aanzien van het gebruik van cookies, spamwetgeving en telemarketing is wel van toepassing op het handelen van Windesheim.

6. Wet Computercriminaliteit III
   De Wet Computercriminaliteit richt zich op de strafrechtelijke probleemgebieden in relatie tot het computergebruik. De wet bestaat uit artikelen die op diverse plekken zijn toegevoegd aan het Wetboek van Strafrecht. De extra artikelen houden zich bezig met:
   - Vernieling en onbruikbaar maken.
   - Aftappen van gegevens.
   - Denial of service, verstikkingsaanval.
   - Computervredebreuk.
   - Diensten afnemen zonder betalen.
   - Malware, kwaadaardige software.

   Naleving van dit Informatiebeveiligingsbeleid, met name van de beveiligingsmaatregelen en het te verwachten gedrag zorgen ervoor dat Windesheim een adequaat basisniveau van beveiliging heeft tegen deze dreigingen. Indien er aanvallen op Windesheim plaatsvinden die de beveiliging significant doorbreken en die vallen onder de Wet Computercriminaliteit, zal het bestuur van Windesheim aangifte doen.

7. Overige codes en landelijke afspraken

Het informatiebeveiligingsbeleid bij Windesheim is gebaseerd op het SURF Normenkader en de instelling is deelnemer in de VH . Windesheim is in dit kader gehouden aan de volgende codes en landelijke afspraken:

- Branchecode goed bestuur Hogescholen.
- Nederlandse gedragscode wetenschappelijke integriteit.
- Juridisch Normenkader Hoger Onderwijs.
- Selectielijst Hogescholen
- Gedragscode praktijkgericht Onderzoek HBO

Bijlage C - Documenten informatiebeveiliging

In het kader van informatiebeveiliging hanteert Windesheim de volgende documenten:

1. *Het IB-beleid*
   Het IB-beleid (dit document) ligt ten grondslag aan de aanpak van (digitale) informatiebeveiliging binnen Windesheim. Het beleid wordt opgesteld door het Security Overleg en vastgesteld door het bestuur. De directeur dienst Bedrijfsvoering agendeert.

2. *Classificatie Richtlijn, DPIA, regelingen en werkinstructies*

3. *Jaarplan/verslag*
   Iedere vier maanden wordt er over informatiebeveiliging gerapporteerd als onderdeel van de Integrale veiligheidsrapportage waarin o.a. ook onderwerpen als privacy, arbo, BHV en sociale veiligheid aan de orde komen. Er wordt ingegaan op incidenten, resultaten van risicoanalyses, audits en trends.

4. *Baseline van informatiebeveiligingsmaatregelen*
   Deze baseline beschrijft de maatregelen die minimaal nodig zijn om het voor Windesheim vastgestelde minimale niveau van informatiebeveiliging te kunnen waarborgen. Dit vloeit voort uit het beleid of uit aanvullende besluiten die door het bestuur genomen zijn. Deze basismaatregelen moeten overal in de instelling worden genomen. Wanneer er processen of systemen zijn die na een classificatie of andere risicoanalyse (bijvoorbeeld een DPIA) hogere beveiligingseisen nodig hebben, dan worden er aanvullende maatregelen genomen.

5. *Policies*
   Gedragscodes en richtlijnen op het gebied van informatiebeveiliging voor medewerkers, studenten en derden (al dan niet voor specifieke doelgroepen), zoals:
   - ICT reglementen voor medewerkers, bezoekers en studenten, voor het veilig gebruik van IT-voorzieningen, e-mail en internetgebruik door medewerkers, studenten en derden.
   - RFC-2350 voor de lokale CSIRT, gepubliceerd op de website.
   - Beleid verwerking Persoonsgegevens.
   - Uitwerking beleid verwerking persoonsgegevens
   - Richtlijn Authenticatie (inclusief wachtwoordbeleid).
   - Richtlijn Autorisatie.
   - [Toepassing van cryptografische hulpmiddelen].
   - Beleid responsible disclosure.
   - [IT Lifecycle management[13]].
   - Integriteits-/gedragscode voor ICT-functionarissen.

[13] Bijvoorbeeld: bij de aanschaf van hard/software dient beveiliging tijdens de hele *lifecycle* van aanbesteding, via testen en implementatie, en wijzigingsbeheer tot aan afvoer en vernietiging meegenomen te worden.

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 IB-beleid 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[14] welke een checklist security en model verwerkersovereenkomst omvat die bij aanbestedingen gebruikt worden.

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

Bijlage D - Inrichting van CSIRT

Het doel van het Computer Security Incident Response Team (CSIRT) is het voorkomen van informatie-beveiligingsincidenten en ze te bestrijden als ze zich toch voordoen. Het doel is de continuïteit van Windesheim te ondersteunen en haar reputatie te beschermen. Het CSIRT houdt zich ook bezig met beveiligingsincidenten buiten Windesheim als daar eigen medewerkers in enige rol bij betrokken zijn. In zulke gevallen wordt als dat mogelijk is, gebruikgemaakt van de diensten van SURFcert, die wereldwijd in verbinding staat met andere CSIRT's.

Het CSIRT team van Windesheim wordt gevormd door de afdeling infrastructuur. Zij zijn tevens verantwoordelijke voor operationele monitoring van netwerk activiteiten.

Het CSIRT heeft een handvest opgesteld waarin doelgroep, opdracht, bevoegdheden, escalaties, werkwijze (inclusief omgang met vertrouwelijkheid) en samenstelling zijn uitgewerkt. Ook worden directe escalaties naar het bestuursniveau (via de manager IVT) vastgelegd. Dit is past binnen het algemene calamiteitenprotocol van Windesheim. Ook worden directe contacten vastgelegd met de afdelingen c.q. personen die binnen Windesheim zorg dragen voor juridische kwesties en contacten met de pers.

Het CSIRT is gerechtigd om tijdelijk computersystemen of netwerksegmenten te laten isoleren om haar taak goed te kunnen uitvoeren.

Incidentbeheer en-registratie hebben betrekking op de wijze waarop medewerkers, studenten en derden inbreuken op de informatiebeveiliging melden en de wijze waarop deze worden afgehandeld. Van incidenten kan worden geleerd. Incidentregistratie en periodieke rapportage over opgetreden incidenten horen dan ook thuis in een volwassen informatiebeveiligingsomgeving. Incidenten kunnen bij Windesheim worden gemeld bij het Servicedesk-meldpunt: servicedesk@windesheim.nl (tel 9070) of csirt@windesheim.nl. Windesheim heeft de contactgegevens van dit meldpunt duidelijk gecommuniceerd naar haar medewerkers, studenten en derden.

Elke medewerker, student en derde is zelf verantwoordelijk voor het signaleren en melden van incidenten en inbreuken op informatiebeveiliging, inclusief datalekken. Incidenten en inbreuken dienen direct gemeld te worden aan het CSIRT-meldpunt.

Het bestuur heeft beleid vastgesteld voor Responsible Disclosure. Daarmee geeft Windesheim mogelijke melders van veiligheidsgaten in de informatiesystemen een garantie dat Windesheim, onder voorwaarden, geen juridische stappen tegen onderneemt.

Om incidenten op de juiste manier te kunnen afhandelen, worden ze in het relevante operationeel overleg besproken. In het geval het bedrijfsproces, financiën of de goede naam van Windesheim in gevaar zijn, wordt het incident ook met het bestuur besproken. Als er verontrustende trends worden geconstateerd, dan speelt Windesheim hierop in door het nemen van extra maatregelen of het creëren van bewustwording binnen de organisatie.