Informatiebeveiligingsbeleid

UM

2020

Versie 3.0, november 2020

Colofon

Informatiebeveiligingsbeleid UM Versie 3.0 (2020)

Vervangt Informatiebeveiligingsbeleid UM versie 2.1

Auteur: Bart van den Heuvel, CISO, CIOffice

Vastgesteld door het CvB van de Universiteit Maastricht d.d.: 17 november 2020
Instemming door de Universiteitsraad d.d.: 22 september 2021
Instemming door het Lokaal Overleg op 30 juni 2021

Het informatiebeveiligingsbeleid van de Universiteit Maastricht is gebaseerd op het Model Informatiebeveiligingsbeleid van het Hoger Onderwijs, opgesteld door de SURF Community voor Informatiebeveiliging en Privacy (SCIPR), versie 3.0, maart 2020.

Inhoudsopgave

Samenvatting

Het succes van een organisatie als de UM 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 UM voorziet in adequate informatiebeveiliging en daarmee voldoet aan de relevante wet- en regelgeving.
Met het informatiebeveiligingsbeleid (IB-beleid) wil de UM 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. De 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 de UM 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 (CISO[1]), controles (UM-SOC[2] en de IT-auditor) en bijsturing: Plan, Do, Check, Act. Naast Security Oficers kunnen de Functionaris Gegevensbescherming, Internal Audit en de Quality & Risk Board hier bij adviseren, met name om tot een goede kosten/baten afweging te komen (risk appetite).

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] CISO: Corporate (Chief) Information Security Officer
[2] UM-SOC staat voor UM-"Security Operations Center", ondergebracht bij ICTS en inhoudelijk aangestuurd door de CISO

1. Inleiding

Het succes van de UM 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.

De digitale werkelijkheid is constant in beweging en dat brengt steeds nieuwe en andere risico's met zich mee voor de Informatieveiligheid[3]. 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 UM-diploma, behaalde cijfers of de legitimiteit van onderzoekconclusies ondermijnen.
Ook de privacy[4] van studenten, medewerkers en gasten en de reputatie van de UM kunnen worden geschaad. Informatiebeveiliging is daarom van cruciaal belang.
"Protect and Comply" is dan ook een van de drie pijlers in de in 2018 vastgestelde I-Strategie van de UM.

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 UM 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 UM. 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[5] (arbowetgeving), veiligheid in onderwijs en onderzoek, fysieke beveiliging en business-continuïteit. Soms overlappen ze elkaar gedeeltelijk.

2. Wet- en regelgeving

De UM 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 UM altijd kan verantwoorden waarom zij wel of niet voldoet. In bijlage D is een overzicht opgenomen van de relevante wet- en regelgeving

[3] Zie toelichting paragraaf 3.1 over verschillen in de definities 'informatieveiligheid' en 'informatiebeveiliging'
[4] Voor het specifieke Privacy beleid van de UM zie https://www.maastrichtuniversity.nl/privacy
[5] *Safety* wordt als verzamelterm gebruikt voor de verschillende aspecten van personele veiligheid: Arbo en milieu, sociale veiligheid, bedrijfshulpverlening e.d.

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.

Informatieveiligheid is binnen de UM een verantwoordelijkheid van iedereen. De eindverantwoordelijkheid voor informatieveiligheid ligt bij het College van Bestuur van de UM.

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 en de eventuele gevolgen hiervan verminderen.

Met het informatiebeveiligingsbeleid (IB-beleid) wil de UM 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 van de instelling.

De UM heeft de ambitie om 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 IB-beleid, en de opvolging daarvan, moet de UM in staat stellen om deze ambitie waar te maken en om 'in control' en compliant te zijn. Op basis daarvan kunnen de betrokken decanen en directeuren samen met het College van Bestuur (CvB) verantwoording afleggen aan de Raad van Toezicht (RvT). De uitvoering van het beleid is ook de basis is om te voldoen aan wettelijke voorschriften.

Randvoorwaarden

Om deze doelstellingen te kunnen bereiken zijn de volgende randvoorwaarden voor de UM 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[6] 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 informatiebeveiligingsmanagementsysteem (ISMS[7], zie bijlage A) van de UM. 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 UM. De UM streeft er wel naar om voor specifieke onderdelen van de informatievoorziening een formele certificering te behalen om daarmee de kwaliteit van die onderdelen aan te kunnen tonen[8].
- *Volwassenheid*
  IBHO omschrijft een norm voor de volwassenheid van de Informatiebeveiliging volgens het Capability Maturity Model (CMM)[9]. De UM streeft naar een volwassenheidsniveau volgens de SURF-richtlijnen.
- *Maatregelen*
  De UM 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. De specifieke maatregelen voor de UM zijn te vinden op https://www.maastrichtuniversity.nl/informatiebeveiliging.

3.3. Doelgroep

Het IB-beleid is bestemd voor iedereen die – intern of extern – te maken heeft met de bedrijfsprocessen van de UM. Het beleid richt zich in eerste instantie op het bestuur en hoger management (de proceseigenaren), de beveiligingsorganisatie en de 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 de UM wordt informatieveiligheid breed geïnterpreteerd. Het gaat over het omgaan met alle vormen van formeel vastgelegde informatie (dus niet alleen digitale informatie), die de instelling of haar relaties genereren en beheren, in eigen UM-systemen of in extern beheerde systemen (outsourcing). 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 UM kan aanspreken.

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

Onder apparaten en applicaties vallen:

[6] De actuele documenten zijn te vinden op https://www.surf.nl/informatiebeveiliging en https://www.surf.nl/surfaudit-inzicht-in-je-informatiebeveiliging-en-privacy. Voor leden van de SCIPR-community zijn ondersteunende wiki's beschikbaar: https://wiki.surfnet.nl/display/SCIPR/SCIPR+Home en https://wiki.surfnet.nl/display/SA/SURFaudit+Home
[7] ISMS: Information Security Management System.
[8] Denk bv. aan een ISO-27001 certificaat voor opslagvoorzieningen ten behoeve van Onderzoek.
[9] https://nl.wikipedia.org/wiki/Capability_Maturity_Model

- Alle fysiek op het netwerk aangesloten apparaten zoals servers, werkstations, laptops, gebouwbeheerssystemen en communicatiesystemen.
- Alle draadloos op het netwerk aangesloten mobiele apparaten, zoals notebooks, tablets, smartphones, smartwatches.
- IoT[10]-devices, zoals bewakingscamera's en sensoren.
- Alle op deze apparaten beschikbare (web/cloud)services en applicaties ('apps').

De UM faciliteert het gebruik van privéapparaten (BYOD[11]) voor studenten en gasten en in beperkte mate ook voor medewerkers. Het gebruik van BYOD op het UM-netwerk voor toegang tot applicaties of informatie van de instelling valt onder dit IB-beleid.

Het beleid is daarmee locatie- en apparatuur-onafhankelijk: het geldt ook als men op een andere locatie dan op het terrein van de UM (zoals thuis, in de trein of bij een andere onderwijsinstelling) of met niet door de UM beheerde apparatuur (zoals een thuis werkplek of BYOD) met informatie of informatievoorzieningen van de UM werkt.

4. Beleidsprincipes informatiebeveiliging

4.1. Inleiding

De UM is een instelling met een open karakter. Vanuit het onderwijs- en onderzoeksperspectief is de insteek "*Open waar mogelijk, gesloten waar nodig*". Dat past ook bij de FAIR[12] doelstellingen in het onderzoekdomein. Adequate beveiliging van informatie is steeds een randvoorwaarde en het openstellen van informatie moet een bewuste keuze zijn.

De UM 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 B.

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 tot zijn recht komt en de risico's voldoende worden afgedekt, volgens het uitgangspunt "Pas toe of leg uit"[13].

Om tot een goede afweging te komen of vervangende maatregelen inderdaad tot een acceptabel restrisico leiden, moeten ze aan het IB-beleid van de UM 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.

[10] Internet of Things
[11] Bring Your Own Device
[12] Findable – Accessible – Interoperable – Reusable (zie https://nl.wikipedia.org/wiki/FAIR-principes)
[13] "pas toe" gaat over de specifieke maatregelen, voor "leg uit" dienen de principes als referentie.

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 de UM. De beleidsprincipes vormen de basis voor de communicatie rondom het IB-beleid van de UM.

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

- Het ISMS (bijlage A).
- Richtlijnen voor projectmatig werken, werkinstructies en awareness-programma's.
- Classificatie (bijlage C) 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 de UM 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 de UM. 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	Denk aan het inrichten van een risicomanagementproces (classificatie), het vastleggen van verantwoordelijkheden, het borgen van risico's in contracten. Zie bijlage B 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. Goede communicatie wordt daarom actief bevorderd, op en tussen alle niveaus in de instelling.
Implicaties	Denk hierbij aan het vastleggen van afspraken in arbeidsvoorwaarden, omgangsvormen, gedragscodes en huisregels, etc. Zie bijlage B 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, bewustzijn en controles.
Implicaties	Denk hierbij aan het houden van awareness campagnes, het inrichten van een audit-proces. Zie bijlage B 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 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	Denk hierbij aan het vaststellen en toetsen van beveiligingseisen in projecten en het inregelen van autorisatieschema's. Zie bijlage B 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 met SSL-technologie. Zie Bijlage B voor een overzicht van alle implicaties.

Tabel 1: beleidsprincipes

5. Governance informatiebeveiligingsbeleid

5.1. Afstemming met samenhangende Risico's

Bij governance moet er aandacht zijn voor alle soorten risico's en hun onderlinge samenhang. Om die reden besteedt de UM op strategisch niveau veel aandacht aan afstemming van informatiebeveiliging, arboveiligheid, fysieke beveiliging, business-continuïteit en privacybescherming. Waar mogelijk en nodig vertaalt deze afstemming zich ook naar het tactische en operationele niveau.

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

5.2. Rollen en hun inpassing in IB-Governance

Deze paragraaf beschrijft hoe de IB-Governance is georganiseerd, wie waarvoor verantwoordelijk is en aan wie wordt gerapporteerd. In de diverse rollen is onderscheid gemaakt in richtinggevend (strategisch), sturend (tactisch) en uitvoerend (operationeel). De verantwoordelijkheden die bij de diverse rollen horen zijn opgenomen in de RASCI-tabel in bijlage E en zijn geborgd in de mandaatregeling van de UM.

De benaming van de specifieke rollen voor Informatiebeveiliging sluiten zoveel mogelijk aan bij het PvIB[14]:

	Informatieveiligheid (risicomanagement)	**Informatiebeveiliging** (ICT-beveiliging)
Strategisch/tactisch	CISO	CISM (ICT-beveiligingsmanager)
Tactisch/operationeel	(L)ISO	(L)ISM (ICT-beveiligingsspecialist)

Tabel 2: rolbenaming conform PvIB

CISO: Corporate (Chief) Information Security Officer
CISM: Corporate (Chief) Information Security Manager
Parallel aan de IB-rollen zijn er ook privacy rollen ingevuld: een (Centrale) Privacy Officer ((C)PO) vergelijkbaar met de CISO en Lokale Privacy Officers (LPO) bij de beheerseenheden. Lokaal zijn deze rollen doorgaans gecombineerd als rollen van de informatiemanager (IM) bij de beheerseenheden.

De IB-Governance bij de UM is ingericht volgens het zogenaamde Three Lines of Defence model[15] (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[16]. De decanen en 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. De informatiemanagers bij de beheerseenheden zijn in hun rol als LISO de contactpersoon binnen de beheerseenheid op het gebied van Informatiebeveiliging.

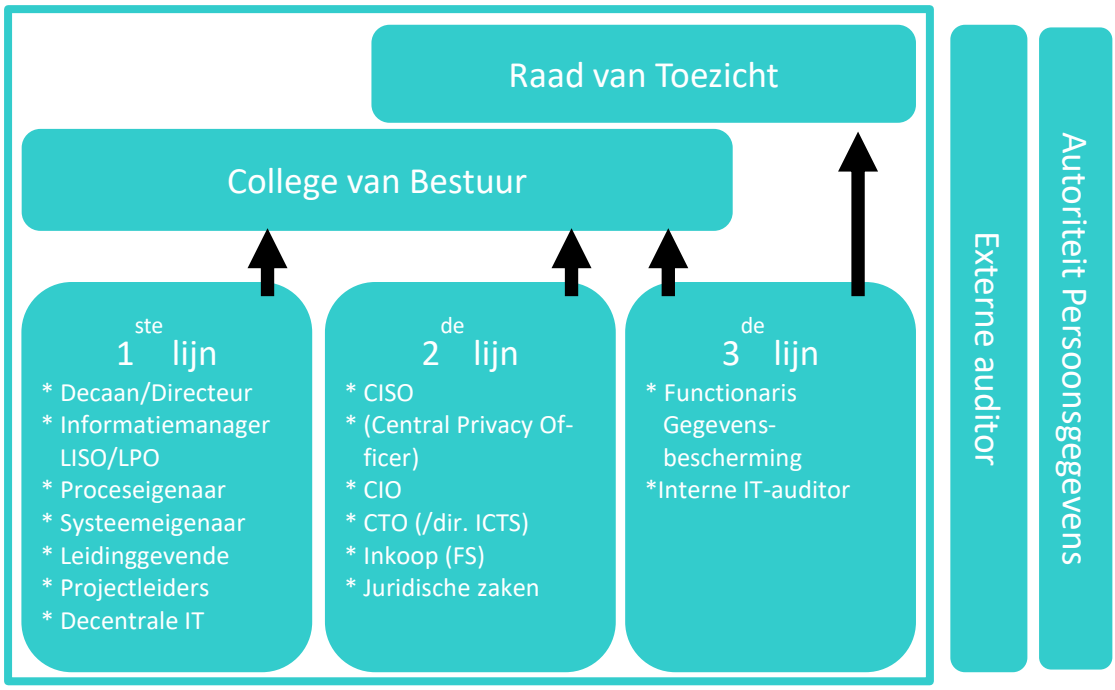
Daarnaast moet er een functie zijn die de eerste lijn ondersteunt, adviseert, coördineert en die bewaakt of het management zijn verantwoordelijkheden ook daadwerkelijk neemt. Dit is de tweede lijn. Ook bepaalde beleidsvoorbereidende taken, het organiseren van de PDCA-cyclus, van integrale risicoanalyses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

5.2.2 De derde lijn

[14] Beroepsprofielen Informatiebeveiliging: https://www.pvib.nl/kenniscentrum/documenten/beroepsprofielen-informatie-beveiliging-2-0
[15] https://www.icas.com/ca-today-news/internal-audit-three-lines-of-defence-model-explained
[16] Dit is daarmee in lijn met het integraal management model van de UM

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) en de interne IT-auditor behoren typisch tot de derde lijn. Beiden opereren volledig los van alle andere organisatieonderdelen en rapporteren niet alleen aan het CvB, maar ook aan de RvT.



Schema: Three Lines of Defence vertaald naar Onderwijs

In bijlage E worden de diverse rollen in de IB-Governance en het 3LoD model verder beschreven. De Raad van Toezicht, de externe auditor en de externe toezichthouders (Autoriteit Persoonsgegevens, maar ook Onderwijsinspectie) worden verder buiten beschouwing gelaten

5.2.3 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, resp. directeuren door gemandateerd en daarmee dieper binnen de organisatie belegd.

5.2.4 Taken, bevoegdheden, verantwoordelijkheden

De diverse taken, bevoegdheden en verantwoordelijkheden zijn onderverdeeld in Strategisch, Tactisch en Operationeel niveau. Deze drie niveaus kenmerken zich door hun overlegstructuur.

Strategisch niveau	Tactisch niveau	Operationeel niveau
De Corporate Information Security Officer (CISO) is een rol op strategisch (en tactisch) niveau. De CISO is verantwoordelijk voor het beleid en het ISMS-proces. De decentrale LISO's vertalen dat beleid naar hun afdelingen.	De rol van (Corporate) Information Security Manager of (C)ISM is tactisch (en operationeel). De (C)ISM is verantwoordelijk voor de vertaling van de strategie en het beleid naar tactische (en operationele) plannen. Dit doet	Het operationele niveau is verantwoordelijk voor de implementatie van de informatiebeveiligingsmaatregelen en de afhandeling van incidenten. Dat gebeurt in overleg met de functionele beheerders en relevante

Strategisch niveau	Tactisch niveau	Operationeel niveau
	hij samen met de CISO en in overleg met de LISO's (vanwege de uniformiteit), de systeem- en proceseigenaren en de (Centrale/Lokale) Privacy Officer.	IT-functionarissen en waar nodig met de tactische laag (de LISO's).

In de volgende tabel zijn de taken, bevoegdheden en verantwoordelijkheden per niveau samengevat, aangevuld met de onderliggende documenten[17].

Niveau	Wat?	Wie?	Overleg	Documenten
Richtinggevend (strategisch)	• Bepalen IB-strategie • Organisatie voor IB inrichten • IB planning en control vaststellen • Business continuity management • Communicatie naar management en organisatie	CvB (de portefeuillehouder Informatieveiligheid) op basis van advies CISO, CIO en CTO	CvB stelt vast, I-Board, Q&R-board[18] en CBB adviseren	• IB beleid • Privacybeleid • Gedrag- en Integriteitscode • ISMS • 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 • CISO • LISO (= Rol van Informatie Manager) • Centrale Privacy Officer	Informatie Managers Overleg (I4MU)	• Classificaties/Risicoanalyses en audits, inclusief DPIA's en SURFaudit • IB baselines (basismaatregelen en uitwerking conform CIS-20-raamwerk) • Jaarplan en –verslag • Cyber Crisis bijlage bij Crisisprotocol • Business continuity plan • Responsible Disclosure procedure
Uitvoerend (operationeel)	• Implementeren IB-maatregelen. • Registreren en evalueren incidenten, inclusief datalekken • Communicatie eindgebruikers • Uitvoeren audits en pentesten	• IT in samenwerking met proces- en systeemeigenaren • Functioneel beheer • (C)ISM • UM-SOC[19] • UM-CERT[20] • Lokale Privacy Officer	DO-ICT UM-SOC/UM-CERT overleg	• SLA's (security-paragraaf) • Incidentregistratie inclusief evaluatie • UM-CERT Operationeel Model • UM-SOC Operationeel model

Overleg

[17] Sommige documenten zijn ten tijde van het vaststellen van dit beleid nog niet geproduceerd of bestuurlijk vastgesteld. Omdat ze bv. afhankelijk zijn van de bestuurlijke vaststelling van dit beleid.
[18] Quality & Risk Board
[19] UM-SOC staat voor UM-"Security Operations Center", ondergebracht bij ICTS en inhoudelijk aangestuurd door CISO.
[20] UM-CERT staat voor UM-"Computer Emergency Response Team"

Om de samenhang in de organisatie van de informatiebeveiligingsfunctie goed tot uitdrukking te laten komen en de initiatieven en activiteiten op het gebied van informatiebeveiliging binnen de verschillende onderdelen op elkaar af te stemmen wordt bij de UM gestructureerd overleg gevoerd over het onderwerp informatiebeveiliging op diverse niveaus.

Strategisch	Tactisch	Operationeel
Op strategisch niveau wordt richtinggevend gesproken over governance, risk en compliance, alsmede over doelen, scope en ambitie op het gebied van informatiebeveiliging, in samenhang met privacy. Dit gebeurt in het bestuur, geadviseerd door I-Board, de Q&R-board en de CISO en afgestemd op de I-strategie en de risicobereidheid (risk appetite) van de UM.	Op tactisch niveau wordt de strategie vertaald naar plannen, maatregelen, te hanteren normen, evaluatiemethoden, e.d. Deze plannen en instrumenten zijn sturend voor de uitvoering. Dit tactisch overleg wordt gevoerd tussen de CISO, de LISO's, (C)PO's en (C)ISM's). Waar nodig in overleg met overige betrokken functionarissen zoals UM-SOC/UM-CERT coördinator en proces- of systeemeigenaren.	Op operationeel niveau worden de zaken besproken die de dagelijkse bedrijfsvoering aangaan in de zin van uitvoering en implementatie

Alle drie overlegtypes worden zoveel mogelijk ingepast in bestaande overlegvormen met hetzelfde karakter. Zo bespreekt men op strategisch niveau niet alleen informatiebeveiliging en privacy, maar ook andere risico's waarmee de UM te maken kan krijgen, zoals financieel, personeel en commercieel.
Dat betekent bij de UM dat informatiebeveiliging op de agenda staat van het CvB, CBB, I-Board en Q&R-board. Op tactisch niveau zal het ook gaan over keuze van IT-functionaliteit en-services op de agenda van het overleg met de informatiemanagers (I4MU), die ook aanspreekpunt zijn voor de decentrale privacy rol (LPO). Op operationeel niveau staat informatiebeveiliging op de agenda van overleggen tussen IT-ondersteuners (DO-ICT), functioneel beheerders en IT-beheerders, maar ook op overleggen met key-users en projectteams, en in SCRUM sessies (Agile-Sprints).

Documenten

Voor informatiebeveiliging wordt bij de UM 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 bijlage F is een uitgebreider overzicht opgenomen van de documenten die de UM voor informatiebeveiliging hanteert zoals genoemd in bovenstaande tabel.

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. Bij de UM werken we daarom voortdurend aan het 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 LISO's. Bewustwording is een onderdeel van het introductieprogramma voor nieuwe medewerkers en studenten.

5.4. Controle, oefenen, naleving en sancties

Bij de UM is de Interne IT-auditor samen met de CISO voor de planning van interne IT audits[21] op navolging van het IB-beleid. De CISO is daarnaast verantwoordelijk voor de controle op de uitvoering van de informatiebeveiligingsjaarplannen. De LISO's en (C)ISM's ondersteunen daarbij. De uitvoering van de audits is belegd bij UM-SOC en de Interne IT-auditor.

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-/UM-CERT-firedrills[22].

De informatiesystemen (of-processen) van de UM worden intern ge-audit. 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. De externe controle wordt in een cyclus van vier jaar uitgevoerd door een onafhankelijke partij. Dit is qua planning gekoppeld met het accountantsonderzoek[23] en dit wordt zoveel mogelijk gecombineerd met de normale planning & control-cyclus.

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.

De UM neemt deel aan de SURFaudit selfassessment cyclus en de bijbehorende tweejaarlijkse benchmark. Minimaal eens per 4 jaar wordt een SURF Peer review aangevraagd.

De bevindingen van de interne en externe controles en mogelijke externe eisen met betrekking tot beveiliging, zijn input voor de nieuwe jaarplannen van de UM. 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 Gegevensbescherming' (FG) verantwoordelijk.

Als uit de controles blijkt dat de naleving ernstig tekortschiet, dan kan de UM de betrokken verantwoordelijke medewerkers of studenten een sanctie opleggen. De sanctie wordt opgelegd binnen de kaders van de CAO-NU en arbeidsovereenkomsten, de Acceptable Use Policy (AUP) en eventuele andere bestuurlijk vastgestelde integriteits- en gedragscodes 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 resp. directeur).

5.5. Financiering

[21] In overleg net de Functionaris gegevensbescherming bij voorkeur te combineren met Privacy-audits.
[22] Als voorbeeld gelden de (N)OZON oefening die jaarlijks door SURF worden gecoördineerd.
[23] (beperkt zich tot z.g. general-IT-controls die in relatie staan met de verantwoording van de jaarrekening)

Financiële middelen voor informatiebeveiliging worden structureel opgenomen in de diverse (project)begrotingen. De financiering van informatiebeveiliging wordt bij de UM centraal en decentraal geregeld.

Centraal

Algemene zaken, zoals het opstellen van een informatiebeveiligingsplan voor de instelling of een externe audit, worden uit de algemene middelen betaald. Instelling brede bewustwordingscampagnes en trainingen worden ook uit deze middelen betaald.

Decentraal

De beveiliging van informatiesystemen en processen, inclusief de kosten daarvan, zijn integraal onderdeel van verantwoord beheer van het betreffende informatiesysteem of proces. Beveiligingskosten van werkplekken maken integraal onderdeel uit van de werkplekkosten. Voorlichting en training voor specifieke toepassingen of doelgroepen worden uit decentrale middelen betaald.

6. Melding en afhandeling van incidenten.

Een incident is een gebeurtenis of een dreiging 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.

Incidenten kan men bij de UM melden bij het UM-CERT meldpunt: Servicedesk-ICTS@maastrichtuniversity.nl (+31 43 3885555). De UM heeft de contactgegevens van dit meldpunt duidelijk gecommuniceerd naar haar medewerkers, studenten en derden.

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

Incidenten of dreigingen van incidenten kunnen ook naar voren komen tijdens regulier of incidentele controles/audits of door signaleringen vanuit het 24/7 beschikbare monitor systeem van UM-SOC.

De incidenten worden afgehandeld volgens het door de UM vastgestelde Incident managementproces, waar de afhandeling van datalekken een onderdeel van is. Het UM-SOC- resp. het UM-CERT Operational Model[24] beschrijft het proces als het gaat over ernstige incidenten en incidenten buiten reguliere bedrijfstijden. Onderdeel van dat proces is het mandaat van UM-SOC resp. UM-CERT om IT-voorzieningen, waarvoor een te hoog risico wordt geconstateerd, per direct af te (laten) sluiten.

Er is een door het College van Bestuur vastgesteld beleid voor Responsible Disclosure[25]. Daarmee geeft de UM mogelijke melders van kwetsbaarheden in de informatiesystemen een garantie dat de UM, onder voorwaarden, geen juridische stappen tegen hen onderneemt.

[24] Voor UM-SOC nog vast te stellen en voor UM-CERT zie https://www.maastrichtuniversity.nl/nl/over-de-um/service-centra/ict-servicecentrum/um-cert

[25] Tzt referentie toevoegen: Dit beleid moet nog formeel worden vastgesteld. Het beleid zal worden opgesteld conform de richtlijnen van het Openbaar Ministerie/NCSC"

7. Vaststelling & Wijziging

Het College van Bestuur stelt, met instemming van de medezeggenschap, het IB-beleid vast dat de Corporate Information Security Officer (CISO) voorstelt. Het IB-beleid volgt de kaders van het instellingsbeleid zoals de (I-)strategie. Het wordt 1x per 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, versie 3.0, is vastgesteld door het bestuur van de UM op 17 november 2020 en kan worden aangehaald als “Informatiebeveiligingsbeleid UM 2020”.

Bijlage A - De inrichting van een ISMS

Informatiebeveiliging is een continu proces. Kort gezegd: eerst moet worden vastgesteld wat nodig is, waarna maatregelen worden getroffen. Deze maatregelen worden vastgelegd in een jaarplan. De maatregelen kunnen veranderen (omdat bedreigingen en risico's veranderen, maar ook wet- en regelgeving is aan verandering onderhevig). Controle kan dan aanleiding geven tot bijsturing van de maatregelen. Daarnaast kan ook het totaalpakket van eisen, maatregelen en controle aan een herijking toe zijn en zal dus periodiek geëvalueerd moeten worden. Het gehele proces van informatiebeveiliging volgt dus een Plan-Do-Check-Act (PDCA)-cyclus (zie afbeelding). De complete set van maatregelen, processen en procedures wordt vastgelegd in een Information Security Management System (ISMS) en biedt daarmee ondersteuning in het doorlopen van de PDCA-cyclus. Door herhaling van de PDCA-cyclus werkt de UM doorlopend aan het verbeteren van het ISMS en is daardoor meer 'in control'. De jaarlijkse planningen zijn te vinden zijn in de planning van de CISO, en meer in detail in de IT-jaarplannen van de beheerseenheden.

Standaarden

De UM onderhoudt een ISMS op basis van de internationale ISO27001 standaard en gebruikt het CIS-20[26] framework als ondersteunend hulpmiddel om invulling te geven aan het ISMS

Uitwerking

Na het vaststellen van de context van de organisatie (IB-beleid i.r.t. de externe en interne omgeving) en van de behoeften en verwachtingen van belanghebbende partijen en een scope-bepaling, wordt het ISMS opgesteld op basis van een PDCA-cyclus met de volgende fasen:

Plan In de planfase worden de volgende zaken gedefinieerd: • Context en scope • risico's en kansen • bedrijfsmiddelen (assets) • middelen en competenties • bewustzijn en communicatie • gedocumenteerde informatie	**Do** Bij de uitvoering van het ISMS gaat het om: • de operationele planvorming en beheersing • risicobeoordeling(en) • risicobehandeling
Check De checkfase omvat de evaluatie van de werking van het ISMS: • bewaking, meting, analyse en evaluatie • interne audit • management review	**Act** Op basis van de uitkomsten van de checkfase worden verbeteringen doorgevoerd

[26] https://www.cisecurity.org/controls/cis-controls-list/

BIJLAGE B - 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 UM. 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 (bijlage C). • De UM stelt een Classificatie Richtlijn[27] (zie ook bijlage C) vast. • Een gegevensbeschermingseffectbeoordeling (DPIA – Data Protection Impact Assessment) in het kader van de AVG maakt waar nodig onderdeel uit van de risicoanalyse. • Er 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 UM, uiteindelijk te bepalen door het bestuur. • 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, afhankelijk van het benodigde mandaat) 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 afgezet worden tegen gebruiksgemak. • 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 UM blijft verantwoordelijk voor adequate bescherming van informatie bij gebruik van externe diensten voor informatieverwerking.

[27] https://www.maastrichtuniversity.nl/informatiebeveiliging

	• 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 de UM is een zogenaamde Acceptabel Use Policy (AUP) beschikbaar die is gepubliceerd via de website van de UM. 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 Jaargesprekken en 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 UM-CERT • 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.

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 (ISMS, bijlage A) 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 de UM rond toegang en gebruik van IT-middelen. • Periodiek (minimaal jaarlijks) worden accounts met hoge privileges gevalideerd. • De UM organiseert regelmatig cybersecurity-awareness activiteiten voor de diverse doelgroepen: studenten, medewerkers, leidinggevenden en partners van de UM. • 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 UM 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. • 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 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 C – Risico bereidheid en Classificatie

Bij de UM zijn alle gegevens, processen, informatiesystemen en applicaties waarop dit informatiebeveiligingsbeleid van toepassing is, geclassificeerd. Deze classificatie is afhankelijk van de te verwerken gegevens en wordt bepaald op basis van de risicobereidheid (risk appetite) van de UM aan de hand van risicoanalyses en schade categorieën. Het classificatieproces is vastgelegd in een door het CvB vastgestelde Classificatierichtlijn[28].
Het niveau van de beveiligingsmaatregelen is afhankelijk van een vastgestelde risicoklasse.
Deze bijlage geeft een overzicht van de vastgestelde risicobereidheid, de gehanteerde schade categorieën en het vastgestelde classificatieproces.

Risico bereidheid

Met een risicoanalyse kan de mogelijke schade worden geëvalueerd die een dreiging kan toebrengen aan specifieke informatie (bijv. misbruik door oneigenlijke toegang, ongeautoriseerde toegang) en wat de kans is dat die schade optreedt.
Niet alle risico' s hoeven gemitigeerd te worden. De UM is bereid om sommige risico' s te accepteren. De risicobereidheid in onderstaande tabel kan gezien worden als een risicoanalyse op basis van algemene waarden in plaats van concrete risico's.
De risicobereidheid van de UM is in onderstaand schema weergegeven.

Tabel 1: Risicobereidheid

Risico		**Schade (Impact)**			
		Verwaarloosbaar	Enig	Ernstig	Ontwrichtend
Kans	Minimaal	Acceptabel	Acceptabel	Acceptabel	Acceptabel
	Klein	Acceptabel	Acceptabel	Acceptabel	Niet acceptabel
	Reëel	Acceptabel	Acceptabel	Niet acceptabel	Niet acceptabel
	Hoog	Acceptabel	Niet acceptabel	Niet acceptabel	Niet acceptabel

Schade categorieën

Schade kan onderverdeeld worden in verschillende categorieën. De hieronder voorgestelde schade categorieën geven een indicatie van het belang van de informatie. Gekoppeld aan de risicobereidheid worden maatregelen geselecteerd die de kans op inbreuken op de beveiliging terugdringen tot een voor de organisatie acceptabel niveau.
De schade categorieën bij de UM zijn als volgt bepaald:

[28] Zie Https://www.maastrichtuniversity.nl/informatiebeveiliging.

Tabel 2: Indicatie schade categorieën

	INDICATIE SCHADE CATEGORIEËN			
IMPACT	Imago	onderwijs	Onderzoek	financieel
VERWAAR-LOOSBAAR	Een klein aantal negatieve berichten in lokale media (inclusief sociale media)	Hooguit verstoring van een beperkt aantal activiteiten op een instituut of vakgroep.	Geen of korte onderbrekingen in lopend onderzoek, voornamelijk reeds publieke of niet-gevoelige data	Directe schade ligt tussen 0 en €10.000
ENIG	Negatieve berichtgeving in de media gedurende een paar dagen (inclusief sociale media)	Verstoring van een deel van het onderwijs (zoals een deel van instituut of vakgroep)	Niet openbare onderzoeksgegevens, langdurige onderbreking of invalidatie van onderzoek	Directe schade tussen €10.000 en €50.000
ERNSTIG	Aanhoudende negatieve berichtgeving in de lokale media (inclusief sociale media). Details maatschappelijk gevoelige werkzaamheden (zoals dierproeven).	Langdurige verstoring van een groot deel van het onderwijs op een of meer instituten.	Publicatiebeperkingen, reputatieschade aan onderzoeker of instelling, patenten of contractuele afspraken	Directe schade tussen €50.000 en €10.000.000
ONTWRICHTEND	Aanhoudende negatieve berichtgeving in de landelijke/internationale media (inclusief sociale media).	Merendeel van het onderwijs wordt langdurig onmogelijk op een of meer instituten	Verregaande contractuele verplichtingen, uitsluiting toekomstige subsidies of levensbedreigend onderzoek	Directe schade is groter dan €10.000.000

Classificatie aan de hand van 3 kwaliteitsaspecten en 3 risico klassen

De eigenaar van informatie bepaalt de schade categorie op basis van de maximale schade/waarde van de data. De waarde van een aantal datatypen is al vastgesteld voor de hele organisatie (tabel 2).

De eigenaar houdt bij het bepalen rekening met **drie kwaliteitsaspecten (B,I,V)**:

B = Beschikbaarheid	Is de informatie/functie aanwezig/bruikbaar/leesbaar op alle noodzakelijke momenten en met de juiste performance.
I = Integriteit	Is de informatie/functie betrouwbaar/compleet/onaangetast?
V = Vertrouwelijkheid	Hebben alleen rechthebbenden toegang tot de informatie/functie?

Daarnaast zijn bij het bepalen van maatregelen de volgende 2 aspecten van belang:

Controleerbaarheid
Hierbij gaat het om de controleerbaarheid[29] van de maatregelen die genomen zijn om deze kwaliteitsaspecten te borgen.

[29] Controleerbaarheid: de mate waarin het mogelijk is om achteraf parameters die van belang zijn voor beschikbaarheid, integriteit of vertrouwelijkheid te verifiëren. Zulke parameters zijn bijvoorbeeld *downtime*, toegang en transacties.

Privacybescherming
De aspecten Integriteit en Vertrouwelijkheid zijn ook van belang om de Privacy rechten van Betrokkenen te kunnen waarborgen bij de verwerking van persoonsgegevens. De hieruit voortvloeiende risico's worden bepaald in een zogenaamde Gegevensbeschermingseffectbeoordeling (GBEB, ook wel DPIA[30] genoemd) in het kader van de AVG.

Voor de feitelijke classificatie wordt per kwaliteitsaspect gekozen voor een indeling in 3 risico klassen: Laag, Midden en Hoog. De indeling in 3 klassen maakt het eenvoudig om per kwaliteitsaspect een indeling in een klasse te maken en daar dan voor de hele instelling generieke maatregelen aan te koppelen.

De onderstaande tabel geeft een handvat voor het inschatten de risicoklasse aan de hand van een generieke impactindicatie per kwaliteitsaspect. Het uitgangspunt is dan dat de schade kán optreden.

Tabel 3: Indeling van de impact in risico klasse.

KLASSE	BESCHIKBAARHEID	INTEGRITEIT	VERTROUWELIJKHEID
LAAG	algeheel verlies of niet beschikbaar zijn van deze informatie gedurende langer dan 1 week brengt geen merkbare (meetbare) schade toe aan de belangen van de instelling, haar medewerkers of haar studenten of klanten	het bedrijfsproces staat enkele integriteitsfouten toe.	informatie die toegankelijk mag of moet zijn voor alle of grote groepen medewerkers of studenten. Vertrouwelijkheid is gering. Daar waar informatie openbaar is, is inzage geen issue, beheer (ten behoeve van de integriteit) wel.
MIDDEN	algeheel verlies of niet beschikbaar zijn van deze informatie gedurende langer dan 48 uur brengt merkbare schade toe aan de belangen van de instelling, haar medewerkers of haar studenten of klanten	het bedrijfsproces staat zeer weinig integriteitsfouten toe. Bescherming van integriteit is absoluut noodzakelijk.	informatie die alleen toegankelijk mag zijn voor een beperkte groep gebruikers. De informatie is vertrouwelijk.
HOOG	algeheel verlies of niet beschikbaar zijn van deze informatie gedurende langer dan 4 uur brengt merkbare schade toe aan de belangen van de instelling, haar medewerkers of haar studenten of klanten	het bedrijfsproces staat geen integriteitsfouten toe	dit betreft zeer vertrouwelijke informatie, alleen bedoeld voor specifiek benoemde personen, waarbij onbedoeld bekend worden buiten deze groep grote schade kan toe brengen.

Ten aanzien van alle aspecten BIV kunnen in bijzondere gevallen, bijvoorbeeld als gevolg van externe eisen, zwaardere klassen worden vastgesteld door het bestuur. De CISO zorgt ervoor dat zulke bijzondere klassen als uitzondering worden aangemerkt en behandeld.

Hiermee wordt de risico-classificatie vastgesteld. Het feitelijke risico wordt bepaald door de impact te vermenigvuldigen met káns dat de schade optreedt. Door afdoende mitigerende maatregelen te nemen, kunnen kans en impact gereduceerd worden, en daarmee het risico gemitigeerd.
De uitkomst van de classificatie is dus bepalend voor de maatregelen die genomen moeten worden om de informatie adequaat te beveiligen.
De UM heeft een informatiebeveiliging baseline[31] vastgesteld als minimale set maatregelen. Aan de hand van de classificatie worden aanvullende maatregelen voorgeschreven conform de centraal vastgestelde maatregelentabel[32].

[30] Data Protection Impact Assessment
[31] Alle "Laag" maatregelen in de UM-Maatregelendatabase
[32] De "Midden" en "Hoog" maatregelen in de UM-Maatregelendatabase

Bijlage D – Wet- en regelgeving

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

1. Wet op het Hoger onderwijs en Wetenschappelijk onderzoek (WHW)
   De UM heeft een kwaliteitszorgsysteem conform de InstellingsToets 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 UM heeft een separaat gegevensbeschermingsbeleid vastgesteld waarin naleving van de AVG wordt geborgd. Naleving van het informatiebeveiligingsbeleid inclusief de daarin vermelde technische en organisatorische maatregelen zorgen samen met de procedures en maatregelen uit het privacy beleid tot voldoen aan de AVG.

3. Wettelijke Bewaartermijnen/Archiefwet
   De UM 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. De UM hanteert daarbij het Basisselectiedocument[33] van de sector universiteiten. Dit selectiedocument gaat over alle informatie zoals die bijvoorbeeld is vastgelegd in (gedigitaliseerde) documenten, informatiesystemen, websites en e-mail. Dit is onderdeel van de jaarlijkse externe accountantsrapportages.

4. Auteurswet
   De UM respecteert auteursrechten en handelt daarnaar.

5. Telecommunicatiewet / Wet Netneutraliteit
   Omdat de doelgroep van de UM voldoende afgebakend is worden de netwerkvoorzieningen van de UM niet aangemerkt als een openbaar netwerk in de zin van de Telecommunicatiewet. Uitzondering hierop zijn enkele voorzieningen ten behoeve van studentenhuisvesting. Hiervoor zijn procedures conform de Wet Netneutraliteit ingericht.

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 de UM een adequaat basisniveau van beveiliging heeft tegen deze dreigingen. Indien er aanvallen op de UM plaatsvinden die de beveiliging significant doorbreken en die vallen onder de Wet Computercriminaliteit, zal het bestuur van de UM aangifte doen.

7. Overige codes en landelijke afspraken
   Het informatiebeveiligingsbeleid bij de UM is gebaseerd op het SURF Normenkader en de instelling is

[33] https://www.nationaalarchief.nl/archiveren/kennisbank/selectielijst-universiteiten-en-universitair-medische-centra-2020

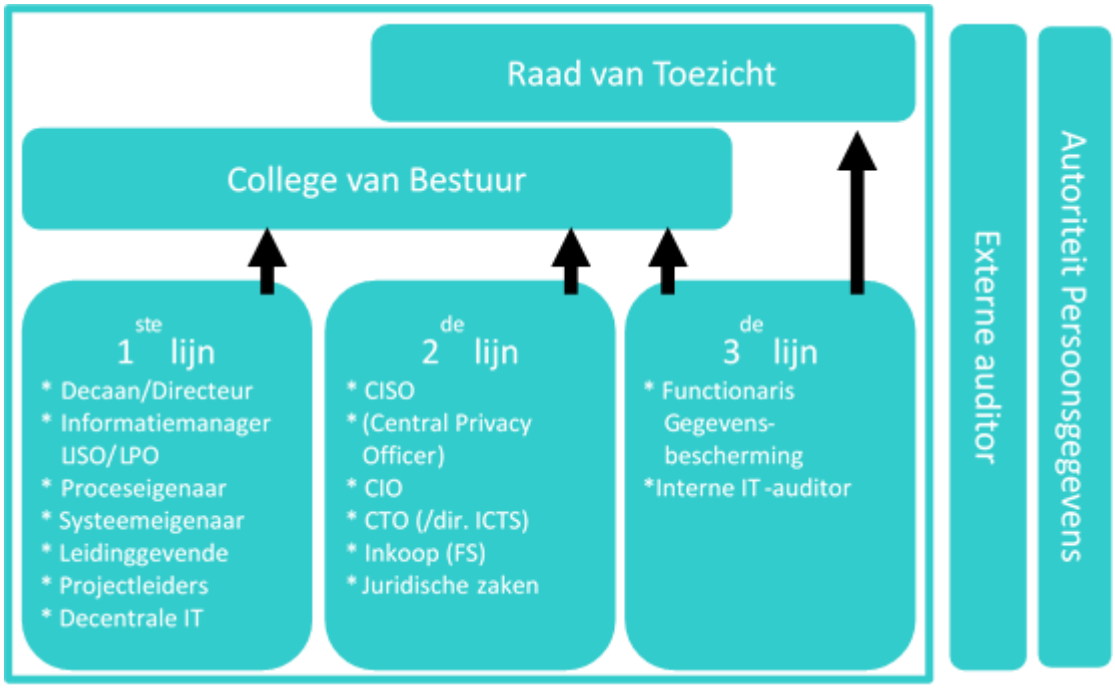
deelnemer in de VSNU[34]. De UM is in dit kader gehouden aan de volgende codes en landelijke afspraken:

- Code goed bestuur universiteiten.
- Nederlandse gedragscode wetenschappelijke integriteit.
- Juridisch Normenkader Hoger Onderwijs.
- Basisselectie document WO
- FAIR-principes

[34] Vereniging Samenwerkende Nederlandse Universiteiten

Bijlage E – Rollen in de IB-Governance

In deze bijlage worden de diverse rollen in het 3LoD model verder “top down” beschreven en hun onderlinge samenhang is samengevat in een tabel. De Raad van Toezicht, Externe Audit en Autoriteit Persoonsgegevens worden buiten beschouwing gelaten.



Schema: Three Lines of Defence, vertaald naar Onderwijs

College van Bestuur

Het bestuur is verantwoordelijk voor de informatiebeveiliging binnen de UM en stelt het beleid en het risicomanagementproces (o.a. de classificatie richtlijn) 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 één van haar leden aan als portefeuillehouder informatieveiligheid.

De inhoudelijke verantwoordelijkheid voor zover het de digitale informatiebeveiliging betreft is door de portefeuillehouder belegd bij de CISO. Deze heeft de opdracht om op de digitale informatiebeveiliging van de gehele instelling toe te zien. De niet-digitale informatiebeveiliging wordt belegd bij de betreffende proceseigenaren.
Omdat de uitvoerende verantwoordelijkheid voor de totale digitalisering van de UM, en daarmee ook voor de kwaliteit van Security (en Privacy), belegd is bij de CIO, is de CIO hiërarchisch leidinggevende van de CISO en operationeel gemandateerd door het CvB.

Functionaris Gegevensbescherming (FG of Data Protection Officer)

De FG houdt binnen de UM toezicht op de toepassing en naleving van de AVG, zoals beschreven in het privacybeleid van de UM[35]. De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie in de instelling.

Interne IT-auditor

De interne IT-auditor is onderdeel van de interne audit-organisatie en controleert jaarlijks het goed en betrouwbaar functioneren van de interne IT-organisatie. Dit omvat o.a. de structuur en verantwoordelijkheden van de IT-organisatie, de hardware, de software, het interne- en (indien aanwezig) externe netwerk,

[35] Voor het specifieke Privacy beleid van de UM zie https://www.maastrichtuniversity.nl/privacy

veiligheids- en calamiteitensystemen. De interne IT-auditor rapporteert aan de opdrachtgever, doorgaans is dit de portefeuillehouder in het bestuur, aan de Raad van toezicht en aan de belangrijkste stakeholders CIO/CTO/CISO/FG.

Corporate Information Security Officer (CISO)

De CISO is een rol op strategisch (en tactisch) niveau. Hij adviseert en rapporteert direct aan het bestuur. De CISO formuleert het beveiligingsbeleid, helpt bij een juiste vertaling daarvan naar instellingsonderdelen, ziet toe op de (uniforme) naleving ervan en rapporteert over lacunes, inconsistenties en onvolkomenheden. De CISO kan zowel gevraagd als ongevraagd advies geven. De CISO heeft de CIO als hiërarchisch leidinggevende.
De rol van CISO is belegd bij één persoon, maar er kunnen (de)centraal meer (Local) Information Security Officers zijn ofwel (L)ISO's.
De CISO heeft verschillende bevoegdheden. Zo kan hij onderzoek doen, onderzoek laten uitvoeren (audits), informatie opvragen en deze in principe ook krijgen. In het geval de privacy in het geding is (en in alle bijzondere gevallen) beslist het bestuur. Binnen de UM vervult de CISO ook de rol van Business Continuity Manager (BCM). Dit is ook een strategisch/tactische rol die tot doel heeft de business continuïteit te bewaken.

LISO (rol van de Informatiemanager)

Binnen alle beheerseenheden van de UM is een Local Information Security Officer rol (LISO) expliciet belegd bij de Informatiemanager. De LISO adviseert en rapporteert hiërarchisch aan de directeur van de beheerseenheid. De LISO wordt geconsulteerd bij de invulling van de tactisch/operationele maatregelen die naar aanleiding van het IB-beleid worden vastgesteld en is verantwoordelijk voor de vertaling, de planning en de invulling van de maatregelen in de eigen beheerseenheid[36], evenals de controle op en rapportage over de maatregelen. De LISO is tevens eerste aanspreekpunt voor UM-CERT en UM-SOC bij Security-incidenten.

(Corporate) Information Security Manager ((C)ISM)

De CISM vervult een rol bij de vertaling van de strategie naar tactische (en operationele) technische plannen en maatregelen. Dit doet hij samen met de CISO, de LISO's en met de systeem- en proceseigenaren. Tevens adviseert de CISM over specifieke informatiebeveiligingsmaatregelen bv. in projecten, bij acquisities van software of hardware, etc.
Bij De UM vervult het UM-SOC de rol van CISM. Het UM-SOC heeft de CTO als hiërarchisch leidinggevende.
Naast de CISM zijn er binnen de beheerseenheden, naast de LISO's, meerdere IT-ondersteuners die de UM-breed vastgestelde maatregelen en operationele plannen doorvertalen naar de eigen organisatie[37].

(Corporate en Local) Privacy Officer

De Privacy Officer houdt zich binnen de UM centraal of binnen de beheerseenheden bezig met de toepassing en naleving van de AVG. Binnen alle beheerseenheden van de UM is een Local Privacy Officer rol (LPO) expliciet belegd. De LPO is het eerste aanspreekpunt van de FG en het centrale UM-Privacy Team bij privacy aangelegenheden, zoals datalekken. Meestal wordt deze rol gecombineerd met de LISO rol bij de Informatiemanager. Er is altijd sprake van samenwerking van de LPO met de CISM en (C/L)ISO, bijvoorbeeld bij het analyseren van (mogelijke) datalekken. Andere voorbeelden hiervan zijn bij het beoordelen van risico's en maatregelen in het geval van een Gegevensbeschermingseffectbeoordeling (DPIA) of bij het afsluiten van verwerkersovereenkomsten in het kader van de AVG.

Proceseigenaar

Een proceseigenaar is verantwoordelijk voor een van de primaire of ondersteunende processen, al dan

[36] Vaak wordt daarom de LISO-rol gecombineerd met de dagelijkse leiding over de lokale IT-ondersteuning in de beheerseenheden.
[37] Doorgaans onder aansturing van de LISO

niet gebruikmakend van meerdere systemen.
Vaak is de proceseigenaar van een primair proces (bv HR- of Studenten-administratie) ook formeel intern verantwoordelijk voor de gegevens die in dat proces en de daarvan afgeleide processen worden verwerkt (informatie- of broneigenaar).

Systeemeigenaar, applicatie-eigenaar

Een systeemeigenaar is iemand die verantwoordelijk is voor een belangrijk systeem, platform of applicatie, waarmee een of meerdere processen worden ondersteund.

Leidinggevende (inclusief onderwijsverantwoordelijken)

Naleving van het IB-beleid 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.

UM-CERT coördinator

Een specifieke rol op het gebied van informatiebeveiliging is de UM-CERT[38]-coördinator.
Deze wordt bij de UM in die rol benoemd door het bestuur. Hij is verantwoordelijk voor information security incident management binnen de instelling, en is in dat kader, binnen het operationele model van UM-CERT, ook bevoegd het tijdelijk isoleren van computersystemen of netwerksegmenten te gelasten. De UM-CERT coördinator werkt voor het uitvoeren van deze taken samen met andere, formeel benoemde, UM-CERT-leden conform het door het bestuur vastgestelde UM-CERT operationeel model

RASCI tabel

R = responsible = responsible for implementation = Verantwoordelijk voor implementatie
A = accountable = ultimately responsible = Eindverantwoordelijk (gemandateerd)
S = Supportive = Supports during process = Ondersteunend bij het proces
C = Consulted = consulted during process = Wordt om adviesgevraagd tijdens proces
I = Informed = informed of results = wordt geïnformeerd

NB1: Het CvB is eindverantwoordelijk, maar veelal is de CIO gemandateerd.
NB2: In de BE's is Decaan/Directeur eindverantwoordelijk, maar veelal proces- of systeem/applicatie-eigenaar/beheerder gemandateerd

	CvB/CIO	CISO	LISO	CISM / UM-SOC	ISM / IT-medewerker	UM-CERT	Proces eigenaar	Systeem / applicatie eigenaar	Leidinggevende	Interne IT Auditor
IB-beleid	A	R	C	C	I	I	I	I	I	C
Risico management	A	R	C	C			C	C	I	C
Classificatie		C	R				A	A	I	
Maatregelen		C	A	S	R		A	A	I	
Audit (agenda, uitvoer)	A	R	S	R			S	S	I	R

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

	CvB/CIO	CISO	LISO	CISM / UM-SOC	ISM / IT-medewerker	UM-CERT	Proces eigenaar	Systeem / applicatie eigenaar	Leidinggevende	Interne IT Auditor
Incident Handling UM[39]	**I**	**A**	**S**	**R**	**S**	**R**	**I**	**I**	**I**	
Incident Handling BE[40]	**I**	**C**	**R**	**S**	**S**	**S**	**I**	**I**	**A**	

[39] Zolang geen CMT en daarnaast is kan een S,C of I rol nodig zijn bij Legal en M & C

[40] Zolang geen CMT en daarnaast is kan een S,C of I rol nodig zijn bij Legal en M & C

Bijlage F – Documenten informatiebeveiliging

Voor informatiebeveiliging wordt bij de UM 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 UM de volgende documenten:

1. *Het IB-beleid*
   Het IB-beleid ligt ten grondslag aan de aanpak van (digitale) informatiebeveiliging binnen de UM. Het beleid wordt opgesteld door de CISO en vastgesteld door het bestuur.

2. *Beschrijving van het Information Security Management System (proces en vastlegging)*

3. *Classificatie Richtlijn, DPIA, regelingen (bv. basishygiëne) en werkinstructies*

4. *Maatregelen database*
   De maatregelendatabase beschrijft de maatregelen die minimaal nodig zijn om het voor de UM vastgestelde minimale niveau van informatiebeveiliging te kunnen waarborgen, gekoppeld aan de classificatierichtlijn. Dit vloeit voort uit het beleid of uit aanvullende besluiten die door het bestuur genomen zijn. Deze maatregelen moeten overal in de instelling worden genomen. De maatregelen worden opgesteld door de CISO en vastgesteld in het Informatie Managers overleg (I4MU). Wanneer er processen of systemen zijn die naar aanleiding van de classificatie of een andere risicoanalyse (bijvoorbeeld een DPIA) hogere beveiligingseisen nodig hebben, dan worden er aanvullende maatregelen genomen.

5. *Jaarplan/verslag*
   De CISO levert, in lijn met de PDCA-cyclus, jaarlijks een verslag over het afgelopen jaar en een jaarplan voor het volgende jaar op aan het bestuur. 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. Het jaarplan wordt in ieder geval afgestemd met het Privacy jaarplan wat door de FG wordt opgesteld.
   De verslagen worden geconsolideerd in de bestuurlijke Planning & Control-cyclus. 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

6. *Policies*
   Gedragscodes en richtlijnen op het gebied van informatiebeveiliging voor medewerkers, studenten en derden (al dan niet voor specifieke doelgroepen), zoals:
   - Privacy Beleid;
   - Acceptable Use Policy, voor het veilig gebruik van IT-voorzieningen, e-mail en internetgebruik door medewerkers, studenten en derden;
   - Integriteits-/gedragscode voor ICT-functionarissen;
   - RFC-2350 voor UM-CERT (zie hoofdstuk 6. Melding en afhandeling van incidenten (UM-CERT);
   - UM-CERT Operationeel model;
   - UM-SOC Operationeel model;
   - Richtlijn responsible disclosure;
   - Diverse richtlijnen die voortkomen uit het CIS-20 Framework;
   - Richtlijn Authenticatie (inclusief wachtwoordbeleid);

- Richtlijn Autorisatie;
- Toepassing van cryptografische hulpmiddelen.

Daarnaast is informatiebeveiliging een vast onderdeel van de volgende documenten:

7. *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[41] die een informatiebeveiliging bijlage bevat.

8. *Business Continuity Plan*
   Het Business Continuity Plan wordt opgesteld op initiatief van de Business Continuity Manager en in samenwerking met het bestuur, de CISO, de proceseigenaren, CIO, CTO, Directeur Facility Services.

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