Informatiebeveiligingsbeleid

UM

2013

Colofon

Informatiebeveiligingsbeleid UM Versie 2.1 (2013)

Vervangt Informatiebeveiligingsbeleid UM versie 1.0 (2003)

Auteur: Bart van den Heuvel, CISO, ICTS

Vastgesteld door het CvB van de Universiteit Maastricht d.d.: 17 juni 2013
Instemming door de Universiteitsraad d.d.: 25 september 2013

Versie 2.1: tekstueel aangepast in lijn met de Engelstalige versie

Het informatiebeveiligingsbeleid van de UM is gebaseerd op het Model Informatiebeveiligingsbeleid van het Hoger Onderwijs, een gezamenlijk product van het SURF CIO-beraad en SURFibo.

Inhoudsopgave

1 Inleiding

Onder informatiebeveiliging wordt verstaan het treffen en onderhouden van een samenhangend pakket aan maatregelen om de kwaliteitsaspecten beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening te garanderen.

De kwaliteitsaspecten:
- Beschikbaarheid: de mate waarin gegevens of functionaliteit op de juiste momenten beschikbaar zijn voor gebruikers;
- Integriteit: de mate waarin gegevens of functionaliteit juist zijn;
- Vertrouwelijkheid: de mate waarin de toegang tot gegevens of functionaliteit beperkt is tot degenen die daartoe bevoegd zijn.[1]

Hierbij gaat het ook om de controleerbaarheid van de maatregelen die genomen zijn om deze kwaliteitsaspecten te borgen.

Informatiebeveiliging is een beleidsverantwoordelijkheid van het bestuur van de UM. In het onderzoek en onderwijsveld is sprake van toenemende afhankelijkheid van informatie en computersystemen, waardoor nieuwe kwetsbaarheden en risico's kunnen optreden. Het is daarom van belang hiertegen adequate maatregelen te nemen. Immers, onvoldoende informatiebeveiliging kan leiden tot onacceptabele risico's bij de uitvoering van onderwijs en onderzoek en bij de bedrijfsvoering van de instelling. Incidenten en inbreuken in deze processen kunnen leiden tot financiële schades en imagoverlies.

De UM heeft de ambitie om met het onderhavige beleidsdocument informatiebeveiliging structureel naar een hoger niveau te brengen en daar te houden door de aspecten Governance, wet- en regelgeving, de organisatie van de informatiebeveiligingsfunctie en het informatiebeveiligingsbeleid - ook in hun onderlinge relatie - duidelijk te beschrijven en vast te stellen.

1.1 Reikwijdte van het beleid

In de reikwijdte van het beleid wordt beschreven wat de afbakening is van het toepassingsgebied ervan.

Bij de UM wordt informatiebeveiliging breed geïnterpreteerd. We realiseren ons dat er een belangrijke relatie en een gedeeltelijke overlap ligt met aanpalende beleidsterreinen, zoals safety (ARBO- en milieuwetgeving), security (fysieke beveiliging) en business continuity. Op strategisch niveau wordt aandacht geschonken aan deze raakvlakken en wordt zowel planmatig als inhoudelijk afstemming gezocht (zie ook hoofdstuk 4).

Het informatiebeveiligingsbeleid binnen de UM heeft betrekking op alle medewerkers, studenten, gasten, bezoekers en externe relaties (inhuur / outsourcing), alsmede op alle organisatieonderdelen. Tevens vallen onder het informatiebeveiligingsbeleid alle apparaten van waaraf geautoriseerde toegang tot het instellingsnetwerk en overige instellings ICT faciliteiten verkregen kan worden.

Bij het informatiebeveiligingsbeleid ligt de nadruk op die toepassingen en informatie die vallen onder de verantwoordelijkheid van de UM. Dit heeft zowel betrekking op gecontroleerde informatie, die door de instelling zelf is gegenereerd en wordt beheerd, als ook op niet-gecontroleerde informatie, bijv. uitspraken in discussies, op persoonlijke websites of social media, waarop de instelling kan worden aangesproken.

[1] Overbeek, Roos Lindgreen, Spruit: Informatiebeveiliging onder controle, ISBN 90-430-0289-5

1.2 Doelstelling informatiebeveiligingsbeleid

Het informatiebeveiligingsbeleid bij de UM heeft als doel het waarborgen van de continuïteit van de bedrijfsvoering en het minimaliseren van de schade door het voorkomen van beveiligingsincidenten en het minimaliseren van eventuele gevolgen.

Het doel van het informatiebeveiligingsbeleid voor de UM is concreet het volgende:

- Kader: het beleid biedt een kader om (toekomstige) maatregelen in de informatiebeveiliging te toetsen aan een vastgestelde norm of best practice; en om de taken, bevoegdheden en verantwoordelijkheden in de organisatie te beleggen;
- Normen: de basis voor de inrichting van het security management is ISO 27001.[2] Maatregelen worden op basis van best practices in het hoger onderwijs en o.b.v. ISO 27002 genomen;[3]
- Expliciet: uitgangspunten en organisatie van informatiebeveiligingsfuncties zijn vastgelegd en worden gedragen door het College van Bestuur, en afgeleid daarvan, door de hele organisatie;
- Daadkrachtig: duidelijke keuzes in maatregelen, actieve controle op beleidsmaatregelen en de uitvoering daarvan;
- Compliance: het beleid biedt de basis om te voldoen aan wettelijke voorschriften.

Door het goed structureren van het informatiebeveiligingsbeleid bij de UM wordt aantoonbaar dat dit beleid bijdraagt aan de realisering van de overall doelstellingen die de UM voor zichzelf heeft geformuleerd (‘alignment’). Die doelstellingen zijn het bieden van een kwalitatief hoogwaardige onderwijs- en onderzoekomgeving, die bijdraagt aan de verbetering van de kwaliteit van de samenleving als geheel. Deze omgeving behoort veilig te zijn en te voldoen aan relevante wet- en regelgeving.

[2] NEN-ISO/IEC 27001: Eisen aan Managementsystemen voor informatiebeveiliging
[3] NEN-ISO/IEC 27002: Code voor Informatiebeveiliging

2 Beleidsprincipes informatiebeveiliging

2.1 Beleidsuitgangspunten en principes

Security management wordt als proces ingericht (ISMS: Information Security Management System). Dat houdt in dat de jaarlijkse planning en controlecyclus, gebaseerd is op ISO 27001 (Plan, Do, Check, Act). Hierin worden jaarplannen opgesteld en uitgevoerd. De resultaten ervan worden geëvalueerd en vertaald naar nieuwe jaarplannen.

De beleidsuitgangspunten bij de UM zijn:

- Onze filosofie is dat we een open instelling zijn, waar veel mogelijk is. Dit open karakter kenmerkt vooral het onderzoek. De benadering van ICT en beveiliging is minder open. Er wordt van medewerkers en studenten verwacht dat ze zich qua techniek en ook qua houding 'fatsoenlijk' gedragen (eigen verantwoordelijkheid). Niet acceptabel is dat door al dan niet opzettelijk gedrag onveilige situaties ontstaan die leiden tot schade en/of imagoverlies. Het is om deze reden dat er gedragscodes zijn geformuleerd en geïmplementeerd.
- De beveiliging dient te voldoen aan de relevante wet- en regelgeving, in het bijzonder aan de Wet Bescherming Persoonsgegevens (2001).
- De beveiliging dient de volgende aspecten te waarborgen:
    - beschikbaarheid;
    - integriteit;
    - vertrouwelijkheid.

De UM hanteert de volgende beleidsprincipes:

- Informatiebeveiliging is een procesverantwoordelijkheid: dat betekent dat de procesmanagers (c.q. systeemeigenaren) de primaire verantwoordelijk dragen voor een goede informatiebeveiliging van de informatie waarvoor zij verantwoordelijk zijn (bronprocessen/systemen zoals SAP-HR HCM en SAP-SLM en afgeleide processen/systemen zoals UMcard en ELEUM). Dit omvat ook de keuze van maatregelen en de uitvoering en handhaving ervan
- Informatiebeveiliging is een lijnverantwoordelijkheid: dat betekent dat de lijnmanagers (directeuren/afdelingshoofden) de primaire verantwoordelijk dragen voor een goede informatiebeveiliging op hun /beheerseenheid/afdeling. Dit omvat ook de keuze van maatregelen en de uitvoering en handhaving ervan.
- Informatiebeveiliging is ieders verantwoordelijkheid. Verwachtingen t.a.v. individuen: communiceer met medewerkers, studenten, docenten en derden dat er van hen verwacht wordt dat ze actief bijdragen aan de veiligheid van geautomatiseerde systemen en de daarin opgeslagen informatie. Dat gebeurt in de aanstellingsbrief, tijdens functioneringsgesprekken, met een instellingsbrede gedragscode, met periodieke bewustwordingscampagnes, et cetera. Het opleggen van sancties na overtredingen maakt het geheel geloofwaardig.
- Informatiebeveiliging is een continu proces. Regelmatige herijking van beleid en audits: technologische en organisatorische ontwikkelingen binnen en buiten de instelling maken het noodzakelijk om periodiek te bezien of men nog wel op de juiste wijze bezig is de beveiliging te waarborgen. De audits maken het mogelijk het beleid en de genomen maatregelen te controleren op efficiency (controleerbaarheid).
  Wat betreft audits streeft de UM zowel wat betreft frequentie als wat betreft na te streven volwassenheidsniveau naar aansluiting bij ontwikkelingen in het Hoger Onderwijs, met name de kaderstelling in SURFaudit[4].
  Wat betreft de bijstelling van het beleid wordt verwezen naar de PDCA-cyclus in het ISMS-proces.
- Eigendom van informatie: de instelling is als rechtspersoon eigenaar van de informatie die onder haar verantwoordelijkheid wordt geproduceerd, tenzij dit voor bijvoorbeeld onderzoek anders is overeengekomen. Daarnaast beheert de instelling informatie, waarvan het eigendom

[4] SURFaudit gaat uit (2012) van minimaal een 2 jaarlijkse selfassessment en eens per 4 jaar een externe audit. Er is een volwassenheidsmodel vastgesteld conform het CMM model (0-5) waarbij een minimumniveau van 3 wordt nagestreefd.

(auteursrecht) toebehoort aan derden. Medewerkers en studenten dienen goed geïnformeerd te zijn over de regelgeving voor het (her)gebruik van deze informatie.
- Waardering van informatie: iedereen behoort de waarde van informatie te kennen en daarnaar te handelen. Deze waarde wordt bepaald door de schade als gevolg van verlies van beschikbaarheid, integriteit en vertrouwelijkheid. Classificatie kan hierbij behulpzaam zijn; zie volgende paragraaf.
- Bij projecten, zoals infrastructurele wijzigingen of de aanschaf van nieuwe systemen, wordt vanaf de start rekening gehouden met informatiebeveiliging.

2.2 Classificatie

Bij de UM dienen alle gegevens waarop dit informatiebeveiligingsbeleid van toepassing is, te worden geclassificeerd. Het niveau van de beveiligingsmaatregelen is afhankelijk van de klasse.

De classificatie van informatie is afhankelijk van de gegevens in het informatiesysteem en wordt bepaald op basis van risico analyses.
Voor dit doel heeft de UM een classificatierichtlijn vastgesteld[5], als hulpmiddel ten behoeve van een verplichte minimale (generieke) risico analyse.
Daarbij zijn de volgende aspecten van belang:
a. Beschikbaarheid
b. Integriteit
c. Vertrouwelijkheid
De UM heeft voor deze aspecten een indeling gemaakt in Standaard, Gevoelig of Kritiek

Ten aanzien van de beschikbaarheidseisen worden de volgende klassen onderscheiden:
- Standaard (Niet vitaal): 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 klanten;
- Gevoelig (Vitaal): 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 klanten;
- Kritiek (Zeer vitaal): 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 klanten.

Daarnaast kunnen een aantal algemene kenmerken, zoals mogelijke kritieke onderbrekingsmomenten aanleiding zijn om informatie(systemen) of processen in te delen in een hogere klasse.

Voor vertrouwelijkheid en integriteit worden de volgende indeling gevolgd.

Klasse	Basisprincipes
Standaard (Openbaar)	• Alle medewerkers en studenten (c.q. iedereen) mogen de gegevens inzien, bijvoorbeeld het UM intranet of de algemene website van de instelling • Een geselecteerde groep mag deze gegevens wijzigen
Gevoelig (Intern vertrouwelijk)	• Inzage is voorbehouden aan Privépersonen of iedereen binnen de instelling (medewerker, student of onderzoeker) die een bepaalde rol heeft c.q. tot een bepaalde besloten groep behoort; toegang kan zowel binnen als buiten de instelling (remote) worden verleend. Bijvoorbeeld selfservice, lesroosters, afdelingsintranetten, onderzoek databases etc. • Een geselecteerde groep mag deze gegevens wijzigen
Kritiek (Strikt Vertrouwelijk)	• Er is expliciet aangegeven wie welke rechten heeft t.a.v. de raadpleging en de verwerking van deze gegevens en vanuit welke werkstations de gegevens benaderbaar zijn. Bijvoorbeeld studieresultaten, onderzoek databases met (bijzondere) persoonsgegevens, etc.

[5] 2007: "Classificatie Richtlijn UM"

Daarnaast kunnen een aantal algemene kenmerken, zoals mogelijke contractafspraken of fraudegevoeligheid aanleiding zijn om informatie(systemen) of processen in te delen in een hogere klasse.

Welk beveiligingsniveau geschikt is voor bepaalde informatie of een bepaald informatiesysteem hangt af van de classificatie van de informatie die het systeem verwerkt. De classificatie dient door of namens de eigenaar van de (het) betreffende informatie(systeem) te worden bepaald. Onderstaande tabel geeft weer welk beveiligingsniveau bij welke klasse van informatie behoort:

Beschikbaarheid	
Standaard	Basisbescherming
Gevoelig	Basisbescherming +
Kritiek	Basisbescherming ++
Vertrouwelijkheid	
Standaard	Basisbescherming
Gevoelig	Basisbescherming +
Kritiek	Basisbescherming ++
Integriteit	
Standaard	Basisbescherming
Gevoelig	Basisbescherming +
Kritiek	Basisbescherming ++

Daar waar de basisbescherming niet voldoende is moeten voor elk informatiesysteem individueel afgestemde extra maatregelen worden genomen. Met basisbescherming + wordt dus een hoger beveiligingsniveau bedoeld dan bij basisbescherming. Basisbescherming ++ is het hoogste beschermingsniveau bij de UM. De UM heeft een Maatregelendatabase vastgesteld[6] waarin een aantal standaard maatregelen zijn vastgelegd (de baseline) en een set aanvullende maatregelen voor Gevoelige en Kritieke informatie(systemen).

[6] 2007: MIB-UM.

3 Wet- en regelgeving

3.1 Wettelijke voorschriften

Bij de UM wordt op de volgende wijze omgegaan met relevante wet- en regelgeving.

3.1.1 Wet op het Hoger onderwijs en Wetenschappelijk onderzoek

De UM heeft haar processen rondom onderwijs en onderzoek zodanig ingericht dat (onder meer) het zorgvuldig omgaan met gegevens in de studenten administratie en met de studieresultaten is gewaarborgd teneinde compliant te zijn aan de wet WHW. Daarnaast worden integriteitscodes voor wetenschappelijk onderzoek en voor ICT-medewerkers toegepast en nageleefd.

3.1.2 Wet Bescherming Persoonsgegevens

De UM heeft de wettelijke vereisten (juistheid en nauwkeurigheid van gegevens en passende technische en organisatorische maatregelen tegen verlies en onrechtmatige verwerking) geïmplementeerd via het informatiebeveiligingsbeleid. In de uitvoering van de beveiligingsmaatregelen werkt de UM conform de CBP Richtsnoer “Beveiliging van Persoonsgegevens” (feb 2013). Naleving van de beveiligingsmaatregelen leidt tot voldoen aan de wet bescherming persoonsgegevens.

3.1.3 Archiefwet

De UM houdt zich aan de voorschriften uit de Archiefwet en het Archiefbesluit over de wijze waarop omgegaan moet worden met informatie vastgelegd in (gedigitaliseerde) documenten, informatiesystemen, websites, e.d. Dit is onderdeel van de jaarlijkse externe accountantsrapportages.

3.1.4 Auteurswet

De UM verspreidt geen originele werken zonder dat daarvoor toestemming is verkregen van de eigenaar van de auteursrechten. Dit impliceert ook dat de UM het gebruik van software zonder het bezitten van de juiste licenties tegen gaat.

3.1.5 Telecommunicatiewet en netneutraliteit

Het netwerk van de UM is niet openbaar en daarmee zijn de Telecommunicatiewet en specifiek de bepalingen m.b.t. netneutraliteit niet van toepassing. De UM biedt internet-toegang ten behoeve van haar medewerkers en studenten alleen aan ter ondersteuning van hun werkzaamheden of studie. Voor zover de UM via haar netwerk internettoegang aanbiedt aan studenten in hun privé woonruimte zal ze daarvoor netneutraliteit toepassen. Internettoegang aan andere rechtspersonen binnen de UM-panden wordt aangeboden via separate openbare aanbieders, waarbij de Telecommunicatiewet van toepassing is.

De maatregelen die de UM genomen heeft om aan de privacywetgeving te voldoen zijn tevens toereikend om de bescherming van de persoonlijke levenssfeer van gebruikers bij het gebruik van UM’s internettoegang te waarborgen.

3.1.6 Wet Computercriminaliteit

De Wet Computercriminaliteit richt zich op de strafrechtelijke probleemgebieden in relatie tot het computergebruik. De wet schrijft voor dat “enige beveiliging” vereist is alvorens er sprake kan zijn

van het eventueel strafrechtelijk vervolgen van delicten jegens de onderwijsinstelling en het eventueel vrijwaren van bestuurders van de instelling.

Naleving van dit informatiebeveiligingsbeleid en implementatie van de basis maatregelen bij de UM moet leiden tot een niveau van beveiliging dat als voldoende mag worden gezien in het kader van de Wet Computercriminaliteit.

3.2 Overige richtlijnen en landelijke afspraken

Zoals eerder gesteld is het informatiebeveiligingsbeleid bij de UM gebaseerd op ISO 27001.

De UM voldoet aan de volgende richtlijnen en landelijke afspraken:

- Integriteitscodes voor wetenschappelijk onderzoek
- Studielink afspraken
- Aansluitvoorwaarden SURFnet/SURFconext.

Daarnaast is zoveel mogelijk voldaan aan gemeenschappelijke landelijke afspraken in de branche.

4 Governance informatiebeveiligingsbeleid

Het goed, efficiënt en verantwoord leiden van een organisatie wordt vaak aangeduid met de term governance. Het omvat vooral ook de relatie met de belangrijkste belanghebbenden van de instelling, zoals de eigenaren, werknemers, studenten, andere afnemers en de samenleving als geheel. Een goed corporate governance-beleid draagt zorg voor de rechten van alle belanghebbenden.

4.1 Afstemming met aanpalende beleidsterreinen

Onderdeel van governance is dat aan alle soorten risico's en hun onderlinge verwevenheid passende aandacht geschonken wordt. Het is om die reden dat bij de UM op strategisch niveau zowel aandacht geschonken wordt aan informatiebeveiliging, als aan fysieke beveiliging, ARBO-veiligheid en bedrijfscontinuïteit. Immers, samenwerking tussen deze disciplines is een noodzakelijke voorwaarde voor governance. Dit is vormgegeven door de (budgettaire) planningscyclus en de rapportagecyclus voor deze aspecten parallel te laten verlopen. Dat biedt handvatten om onderlinge interferentie op te merken en te behandelen. Waar wenselijk en mogelijk wordt deze afstemming ook vertaald naar het tactische en operationele niveau, maar alleen daar waar het toegevoegde waarde biedt.

In dit hoofdstuk wordt verder uitsluitend ingegaan op IT-governance en de positionering van informatiebeveiliging daarin.

4.2 Inpassing in de instellings IT-governance

In deze paragraaf wordt beschreven hoe IT-governance in de UM is georganiseerd en wie waarvoor verantwoordelijk is. Van belang daarbij is om onderscheid te maken naar richtinggevend of strategisch, sturend of tactisch en uitvoerend niveau. Wat betreft de benaming van rollen wordt zoveel mogelijk aangesloten bij het PvIB.[7]

De *Corporate Information Security Officer (CISO)* is een rol op strategisch (en tactisch) niveau. Hij adviseert samen met de directeur ICT en de CIO aan het Coördinerend Beraad bedrijfsvoering (CBB) en waar nodig het College van Bestuur. De CISO bewaakt de uniformiteit binnen de instelling en is verantwoordelijk voor het ISMS-proces.

De rol van *Information Security Manager* is vormgegeven op het stafniveau van elke faculteit of dienst en is belegd bij de Informatie Manager. Deze vervult een rol bij de vertaling van de strategie naar tactische (en operationele) plannen. Dit doen ze samen met de Corporate Information Security Officer (vanwege de uniformiteit), met de ICT-vertegenwoordiger van de beheerseenheid (DO-ICT-lid; tactisch/operationeel) en met de procesverantwoordelijken en eigenaren van de technische platforms.

Op operationeel niveau wordt overlegd met de functioneel beheerders en lokale IT-functionarissen (via DO-ICT leden). Er wordt aandacht geschonken aan de implementatie van de informatiebeveiligingsmaatregelen. Wat betreft (emergency) computer incidenten wordt afhandeling geïnitieerd of gecoördineerd door UM-CERT[8]

[7] Functies in de informatiebeveiliging. Platform voor Informatiebeveiliging(PvIB), 2006
[8] UM's Computer Emergency Response Team: http://www.maastrichtuniversity.nl/um-cert

Schematisch weergegeven:

Niveau	Wat?	Wie?	Overleg	Documenten
Richtinggevend	- Bepalen IB-strategie - Organisatie t.b.v. IB inrichten - IB-planning en control vaststellen - Business continuity management	CvB/CBB, i.c. Portefeuillehouder IB, o.b.v. advies CISO en directeur IT / CIO	- CvB/CBB stelt vast - Strategisch IB/ICT-overleg (UMIO) adviseert - Instemming U-raad indien van toepassing	- IB-beleidsplan - Gedrag en Integriteitscodes - Classificatie richtlijn/basisprincipes - Business continuity Plan
Sturend	Planning & Control IB: - voorbereiden normen en wijze van toetsen - evalueren beleid en maatregelen - begeleiding interne assessments en externe audits	- Systeem eigenaar - CISO - Information Security Manager	- Tactisch IB/ICT-overleg (in UMIO)	- IB-baseline (basis maatregelen) - Classificaties/ Risicoanalyses en audits - Jaarplan en verslag
Uitvoerend	- implementeren IB-maatregelen - registreren en evalueren incidenten - communicatie eindgebruikers	- Information Security Manager - Functioneel beheerder - ICTS operations (Servicedesk)	- Operationeel IB-overleg (in DO-ICT c.q. in beheerseenheid) - UM-CERT	- SLA's (security paragraaf) - Incidentregistratie incl. evaluatie - Operationeel Framework UM-CERT

De financiering van informatiebeveiliging wordt bij de UM als volgt geregeld.
Algemene zaken, zoals het opstellen van een informatiebeveiligingsplan voor de gehele instelling of een externe audit, worden uit het centrale ICT-budget betaald. De beveiliging van informatiesystemen komt ten laste van het informatiesysteem zelf. Beveiligingskosten van werkplekken maken integraal onderdeel uit van de werkplekkosten.
Ook UM-CERT wordt gefinancierd uit de lopende ICT budgetten (voornamelijk ICTS-Operations) omdat de feitelijke taken al tot het pakket van deze UM-CERT-leden horen. UM-CERT heeft enkel aanvullende mandaten, inclusief een mandaat voor een nood-budget voor ondersteuning bij ernstige (UM brede) incidenten.

Voor awareness en training geldt dat er instellingsbrede bewustwordingscampagnes kunnen zijn (centraal gefinancierd) en er kan sprake zijn van lokale voorlichting en training voor specifieke toepassingen of doelgroepen (decentraal gefinancierd).

4.3 Documenten informatiebeveiliging

Voor informatiebeveiliging wordt bij de UM dezelfde managementcyclus gevolgd, die ook voor andere onderwerpen geldt: beleid, analyse, plan implementatie, uitvoering, controles en evaluatie.

In het kader van informatiebeveiliging kent de UM de volgende documenten:

1. Het informatiebeveiligingsbeleid
   Het informatiebeveiligingsbeleid (dit document) ligt ten grondslag aan de aanpak van informatiebeveiliging binnen de instelling. In het informatiebeveiligingsbeleid worden de randvoorwaarden en uitgangspunten vastgelegd en de wijze waarop het beleid wordt vertaald in concrete maatregelen. Om er voor te zorgen dat het beleid gedragen wordt binnen de

organisatie en de organisatie er naar handelt wordt het uitgedragen door (of namens) het College van Bestuur. Het informatiebeveiligingsbeleid, wordt opgesteld door de Corporate Information Security Officer en vastgesteld door het College van Bestuur.

2. Classificatierichtlijn en maatregelendatabase (basis en aanvullend niveau maatregelen)
   De classificatierichtlijn stelt de criteria vast om te komen tot een indeling in klassen van maatregelen (Standaard, Gevoelig of Kritiek) met betrekking tot de aspecten beschikbaarheid, Integriteit en vertrouwelijkheid (BIV). Bovendien worden in de classificatierichtlijn een aantal basis beveiligingsprincipes vastgelegd.
   De maatregelendatabase beschrijft in meer detail de principes die geïmplementeerd moeten worden om instelling breed een minimaal niveau van informatiebeveiliging te kunnen waarborgen (baseline) en de aanvullende maatregelen voor als Gevoelig of Kritiek geclassificeerde gegevens of systemen.
   De feitelijke maatregelen vloeien voort uit het beleid of uit besluiten die door het tactisch overleg genomen zijn. De basis maatregelen dienen dus overal in de instelling genomen te worden. De baseline wordt gemaakt door de Security Managers en goedgekeurd door het College van Bestuur. Wanneer er systemen zijn die naar aanleiding van de classificatie of een aanvullende risicoanalyse hogere beveiligingseisen nodig hebben, dan worden de bijbehorende maatregelen bovenop de minimale maatregelen genomen.

3. Jaarplan/verslag
   Elk jaar levert de Corporate Information Security Officer (CISO) een jaarverslag en een jaarplan voor het volgende jaar op ten behoeve van Directeur ICT, CIO en Portefeuillehouder Bedrijfsvoering CvB. Als basis wordt daarbij gebruik gemaakt van vergelijkbare jaarverslagen en jaarplannen van de Information Security Managers. Een jaarplan is mede gebaseerd op de resultaten van de periodieke controles/audits. Er wordt o.a. ingegaan op specifieke incidenten, resultaten van risicoanalyses (incl. genomen maatregelen) en andere initiatieven die het afgelopen jaar hebben plaatsgevonden. Dergelijke verslagen kunnen geconsolideerd worden in de bestuurlijke Planning & Control-cyclus. Waar nodig wordt apart aandacht besteed aan decentrale systemen.

4. Business Continuity Plan
   Business Continuity Management (BCM) is de benaming van het proces dat potentiële bedreigingen voor een organisatie identificeert en bepaalt wat de impact op de “operatie” van de organisatie is als deze bedreigingen daadwerkelijk manifest worden. Het product van BCM bestaat uit een samenhangend stelsel van maatregelen, die zowel preventief, detectief, repressief als correctief werkzaam zijn.

   Het Business Continuity Plan wordt gecoördineerd door de Business Continuity Manager (c.q. de CISO) en wordt mede ingevuld vanuit de proces- en systeemeigenaren. De vaststelling van het plan vindt plaats door het CBB op advies van de directeur ICT, de CIO, de directeur Facilitaire Zaken en de directeur Financiën.

5. Diensten niveau overeenkomsten (SLA’s)
   Een ‘service level agreement’ is een overeenkomst tussen een leverancier en een afnemer met afspraken en randvoorwaarden over geleverde diensten. Dit kan zowel intern als extern zijn. Bijvoorbeeld de ICT-afdeling sluit met externe leveranciers een SLA af t.b.v. de ondersteuning van concernsystemen en met de interne UM klanten sluit de ICT-afdeling SLA’s af mbt te leveren diensten als de Servicedesk, E-mailvoorzieningen etc. In deze contracten zit standaard een informatiebeveiligingsparagraaf, waarin de verantwoordelijkheden van de leverancier zijn opgenomen.

6. Inhuur- en uitbestedingscontracten
   Bij de inhuur van diensten en personeel van derde partijen zal ook aandacht aan informatiebeveiliging besteed moeten worden, bijvoorbeeld door te stellen dat het instellingsbeleid ook van toepassing is voor hen. Hetzelfde is van belang bij uitbestedingen.

Meestal zijn ook de UM Algemene ICT-inkoopvoorwaarden van toepassing.

7. Gedrag en integriteitscodes
   Gedragscodes en richtlijnen voor medewerkers, studenten en derden, al dan niet voor specifieke doelgroepen, op het gebied van informatiebeveiliging, vastgesteld door het CvB met instemming resp. advies van de medezeggenschapsorganen:
   - Acceptable Use Policies AUP's, voor het veilig gebruik van ICT-voorzieningen
   - integriteits- en gedragscode voor ICT-functionarissen;

8. Policies
   Aanvullende richtlijnen op operationeel niveau, zoals:
   - wachtwoordpolicy;
   - basiseisen werkstations (inclusief BYOD-richtlijnen)
   - policies voor inrichting en beheer van servers en netwerkcomponenten
   - toepassing van cryptografische hulpmiddelen;
   - specifieke gebruiks- en beheersvoorwaarden;
   - Sanctie policy, bv. voor het afsluiten van servers en werkstations bij incidenten;
   - gedragscode voor veilig e-mail- en internetgebruik.

4.4 Controle, naleving en sancties

Bij de UM zijn de Corporate Information Security Officer in samenwerking met de interne auditor leidend bij de controle op de uitvoering van de informatiebeveiligingsjaarplannen.

De externe controle wordt uitgevoerd door onafhankelijke accountants. Dit is gekoppeld aan het jaarlijkse accountantsonderzoek en wordt zoveel mogelijk gecoördineerd met de normale Planning & Control cyclus. Verder worden ook branche specifieke audits uitgevoerd, zoals de SURFaudit.

De bevindingen van de interne en externe audits zijn input voor de nieuwe jaarplannen van de UM.

De naleving bestaat uit algemeen toezicht op de dagelijkse praktijk van het security management proces. Van belang hierbij is dat lijnmanagers hun verantwoordelijkheid nemen en hun medewerkers aanspreken in geval van tekortkomingen. Voor de bevordering van de naleving van de Wet Bescherming Persoonsgegevens vervult de functionaris gegevensbescherming[9] een belangrijke rol.

Mocht de naleving ernstig tekort schieten, dan kan de UM de betrokken verantwoordelijke medewerkers een sanctie op te leggen, binnen de kaders van de CAO en de wettelijke mogelijkheden. Aan studenten kunnen sancties opgelegd worden in lijn met de wet Hoger en Wetenschappelijk onderwijs.

4.5 Bewustwording en training

Beleid en maatregelen zijn niet voldoende om risico's op het terrein van informatiebeveiliging uit te sluiten. In de praktijk blijkt de mens meestal de belangrijkste speler. Daarom wordt bij de UM het bewustzijn voortdurend aangescherpt, zodat kennis van risico's wordt verhoogd en het (veilig en verantwoord) gedrag wordt aangemoedigd. Onderdeel van het beleid zijn de regelmatig terugkerende bewustwordingscampagnes voor medewerkers, studenten en gasten. Zulke campagnes kunnen aansluiten bij landelijke campagnes in het hoger onderwijs, zo mogelijk in afstemming met beveiligingscampagnes voor ARBO, milieu en fysiek. Verhoging van het beveiligingsbewustzijn is zowel een verantwoordelijkheid van de (decentrale) Information Security Managers als de Corporate Information Security Officer; uiteindelijk is ook hiervoor het College van

[9] Met ingang van 2014 is de instelling verplicht deze rol formeel te beleggen

Bestuur eindverantwoordelijk.
Er worden methodes geïmplementeerd om bewustwording te verankeren in het loopbaantraject, bv. door de evaluatie van gedrags- en integriteitscodes als vast agendapunt op te nemen op de agenda van jaargesprekken.

4.6 Organisatie van de informatiebeveiligingsfunctie

Om informatiebeveiliging gestructureerd en gecoördineerd op te pakken wordt bij de UM een aantal rollen onderkend die aan functionarissen in de bestaande organisatie zijn toegewezen.

4.6.1 College van Bestuur

Het College van Bestuur is eindverantwoordelijk voor de informatiebeveiliging binnen de UM en stelt het beleid, gedragscodes en de classificatierichtlijn met de basisprincipes op het gebied van informatiebeveiliging vast. De inhoudelijke verantwoordelijkheid voor informatiebeveiliging aan de Corporate Information Security Officer. Deze heeft de opdracht om voor de informatiebeveiliging voor de gehele instelling zorg te dragen.

4.6.2 Portefeuillehouder informatiebeveiliging

De portefeuillehouder informatiebeveiliging is het Collegelid dat informatiebeveiliging in portefeuille heeft. Hij is eindverantwoordelijk voor informatiebeveiliging binnen de UM.

4.6.3 Corporate Information Security Officer

De Corporate Information Security Officer is een rol op strategisch (en tactisch) niveau. Hij adviseert samen met de directeur ICT en CIO (Informatiemanagement) aan het Coördinerend beraad Bedrijfsvoering (CBB) en waar nodig het College van Bestuur. De Corporate Information Security Officer bewaakt de uniformiteit binnen de instelling en het ISMS-proces.

4.6.4 Information Security Manager

De rol van Information Security Manager is vormgegeven op het stafniveau van elke beheerseenheid. Bij de UM wordt deze rol ingevuld door de Informatie Manager. Deze vervult een rol bij de vertaling van de strategie naar tactische (en operationele) plannen. Dit doen ze samen met de Corporate Information Security Officer (vanwege de uniformiteit) en met de eigenaren van de processen en de ICT-voorzieningen.

4.6.5 Proces eigenaar

Een proces eigenaar is iemand die verantwoordelijk is voor een van de primaire of ondersteunende processen, zoals inkoop, HRM en onderwijs.

4.6.6 Eigenaar van een ICT-voorziening

De eigenaar van een ICT-voorziening is er verantwoordelijk voor dat een applicatie een goede ondersteuning biedt aan een specifiek proces. Dit betekent dat de eigenaar er voor zorgt dat zowel nu als in de toekomst de applicatie blijft beantwoorden aan de eisen en wensen van de gebruikers en aan wet- en regelgeving. Uiteraard moet de applicatie voldoen aan het informatiebeveiliging beleid en tenminste aan de basis maatregelen.

4.6.7 Informatiearchitect

De informatiearchitect adviseert over specifieke informatiebeveiligingsmaatregelen in processen en systemen en bewaakt de consistentie van de maatregelen.

4.6.8 Leidinggevende

Naleving van het informatiebeveiligingsbeleid is onderdeel van de integrale bedrijfsvoering. Iedere leidinggevende heeft de taak om:

- er voor te zorgen dat zijn medewerkers op de hoogte zijn van het beveiligingsbeleid;
- toe te zien op de naleving van het beveiligingsbeleid door zijn medewerkers;
- periodiek het onderwerp informatiebeveiliging onder de aandacht te brengen in werkoverleggen;
- als aanspreekpunt beschikbaar te zijn voor alle personeel gerelateerde informatiebeveiligingszaken.

De leidinggevende kan hierin ondersteund worden door de Information Security Manager of Corporate Information Security Officer.

4.6.9 Functionaris Gegevensbescherming

De functionaris voor de gegevensbescherming (FG) houdt binnen de UM toezicht op de toepassing en naleving van de Wet bescherming persoonsgegevens. De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie in de organisatie.

4.6.10 CERT-coördinator

De CERT-coördinator bij de UM wordt benoemd door de directeur ICTS op instellingsniveau en opereert in diens opdracht. De CERT-coördinator is voorzitter van het UM-CERT team. Het team heeft aanvullende mandaten, rechtstreeks onder de portefeuillehouder van het CvB, met bevoegdheden om het beperken van functionaliteit van computersystemen, netwerksegmenten of gebruikers(groepen) uit te voeren of te gelasten.

4.7 Overleg

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 vele niveaus.

Op strategisch niveau wordt richtinggevend gesproken over governance en compliance, alsmede over doelen, scope en ambitie op het gebied van informatiebeveiliging. Dit gebeurt in het overleg tussen Directeur ICTS/CIO en portefeuillehouder CvB en in het CBB. Het door de CIO gecoördineerde Informatie Managers Overleg heeft een adviserende rol m.b.t. het strategisch niveau.

Op tactisch niveau wordt de strategie vertaald naar plannen, te hanteren normen, evaluatiemethoden, e.d. Deze plannen en instrumenten zijn sturend voor de uitvoering. Dit tactisch overleg is per faculteit of dienst georganiseerd door de directeur/Informatie Manager. Overkoepelend tactisch advies wordt gegeven vanuit de ICT-vertegenwoordigers van de Beheerseenheden in het DO-ICT overleg.

Op operationeel niveau worden de zaken besproken die de dagelijkse bedrijfsvoering (uitvoering) aangaan. Overkoepelende onderwerpen m.b.t. informatiebeveiliging worden besproken in het door ICTS gecoördineerde overleg met ICT-vertegenwoordigers van de Beheerseenheden (DO-ICT). Ook het gebruikersoverleg wat georganiseerd wordt door alle Proces(/systeem)eigenaren is binnen de UM een gestructureerd overleg waar operationele zaken

aan de orde kunnen worden gesteld. Verder wordt operationeel overleg decentraal georganiseerd, indien nodig in elk organisatieonderdeel.

Voor alle drie de typen overleg geldt dat het zoveel mogelijk ingepast moet worden in bestaande overlegvormen met hetzelfde karakter. Zo zal op strategisch niveau niet alleen over informatiebeveiliging gesproken worden, maar ook over andere risico's waarmee de instelling te maken kan krijgen, zoals financieel, personeel en commercieel.

5 Melding en afhandeling van incidenten

Incidentbeheer en –registratie hebben betrekking op de wijze waarop geconstateerde dan wel vermoede inbreuken op de informatiebeveiliging door de medewerkers, studenten en onderzoekers gemeld worden en de wijze waarop deze worden afgehandeld.

Het is van belang om te leren van incidenten. Incidentregistratie en periodieke rapportage over opgetreden incidenten horen thuis in een volwassen informatiebeveiligingsomgeving. Bij de UM functioneert Servicedesk-ICTS als centraal meldpunt en deze functie is algemeen bekend gemaakt.

Elke eenheid is zelf verantwoordelijk voor het signaleren en melden van incidenten en inbreuken op informatiebeveiliging. De lijnmanager, de lokale IT-ondersteuner (LO) of de eindgebruiker dienen de incidenten en inbreuken direct te melden aan het centrale meldpunt: Servicedesk-ICTS.

Servicedesk-ICTS maakt een eerste inschatting van alle binnenkomende incidenten en overige aanvragen. Indien het een beveiligingsincident betreft wordt het incident toebedeeld aan de Security-groep met in eerste aanleg de classificatie High. Binnen de security-groep wordt binnen maximaal 4 uur een verdere analyse plaats en wordt ofwel verdere actie ondernomen (best effort) ofwel er vindt een her-classificatie naar een lager niveau plaats.
De incidenten worden afgehandeld en dienen als input voor de incidentrapportages, waarover zo nodig in het operationeel overleg wordt gesproken. Op kwartaalbasis vindt een geaggregeerde rapportage plaats die op tactisch en strategisch niveau besproken wordt. Bij constatering van bepaalde trends kan hierop meteen worden ingespeeld, bijvoorbeeld door het nemen van extra maatregelen of een bewustwordingscampagne.

5.1 Computer Emergency Response Team (CERT)

Het doel van de CERT bij de UM is instellingsbrede zorg voor afhandeling van ernstige informatiebeveiligingsincidenten en voorstellen tot preventie. De CERT houdt zich ook bezig met beveiligingsincidenten buiten de UM als daar eigen medewerkers of studenten in enige rol bij betrokken zijn. In zulke gevallen wordt in principe gebruik gemaakt van de diensten van SURFcert, die wereldwijd in verbinding staat met andere CERTs.

De leden van de CERT zijn benoemd door de directeur ICTS en opereren in diens opdracht.
Het team heeft aanvullende mandaten, rechtstreeks onder de portefeuillehouder van het CvB.
De CERT is gerechtigd om het beperken van functionaliteit van computersystemen, netwerksegmenten of gebruikers(groepen) te gelasten.

De CERT van de UM heeft de volgende opdracht:
- het signaleren en registreren van alle beveiligingsincidenten, het coördineren van de bestrijding en het toezien op de oplossing van problemen die tot incidenten hebben geleid of door de incidenten zijn veroorzaakt (of het bieden van ondersteuning daarbij);
- het geven van voorlichting en het doen van algemene aanbevelingen aan netwerkbeheerders, systeembeheerders, ontwikkelaars en eindgebruikers door het verspreiden van informatie;
- het leveren van managementrapportages aan directeur ICTS en CIO (Informatiemanagement) over de beveiligingsincidenten en het doen van voorstellen tot betere preventie van of curatie op incidenten.

De CERT bij de UM levert de volgende diensten:
- afhandelen van binnenkomende e-mails;
- afhandelen van binnenkomende telefoons;
- inrichten en operationeel houden van een meldpunt voor alle beveiligingsincidenten (Servicedesk-ICTS) en het coördineren en bewaken van een adequate afhandeling daarvan (oplosgroep Security). De bereikbaarheid van de CERT (tijden/middelen) worden bekend gemaakt aan alle betrokkenen;

- geven van voorlichting aan IT-gebruikers, –ontwikkelaars en –beheerders over preventie van incidenten en actuele bedreigingen;
- adviseren over instellingsbrede beveiligingsaspecten;
- periodiek opstellen van managementrapportages.

De CERT bij de UM behandelt meldingen vertrouwelijk en verstrekt alleen informatie over beveiligingsincidenten als dat noodzakelijk en relevant is voor de oplossing van een incident.

De dienstverlening van de CERT bij de UM is gedocumenteerd en door het College van Bestuur bekrachtigd.