Fontys

› FOR SOCIETY

INFORMATIE BEVEILIGINGSBELEID

FONTYS HOGESCHOLEN

INFORMATION SECURITY & PRIVACY OFFICE

Dit beleid, versie V1.0, is vastgesteld door het College van Bestuur van Fontys Hogescholen op 14 juni 2022.
Dit beleid is opgesteld door het ISP-Office en tot stand gekomen met medewerking van de ISP-werkgroep binnen het IM-netwerk, meerdere directeuren, Northwave security en alle ISP-Office medewerkers.

INHOUDSOPGAVE

SAMENVATTING

Het succes van een organisatie hangt steeds meer af van informatie, nieuwe technologieën en computersystemen. Die informatie moet goed worden beveiligd, zeker als er persoonsgegevens worden opgeslagen. In dit document is verwoord op welke manier Fontys voorziet in adequate informatiebeveiliging en daarmee voldoet aan de relevante wet- en regelgeving. Met het informatiebeveiligingsbeleid (IB-beleid) wil Fontys 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 is complex en zit verweven in alle lagen van de organisatie. Naast de reikwijdte van het beleid worden de verantwoordelijkheden van de betrokken functionarissen beschreven. Het lijnmanagement is verantwoordelijk voor haar eigen processen, de directie zorgt ervoor dat beveiligingsmaatregelen daadwerkelijk worden geïmplementeerd. Eindverantwoordelijkheid ligt bij het College van Bestuur.

Gelet op de ransomware aanvallen, gestart bij de Universiteit Maastricht in december 2019, zal geen manager in het hoger onderwijs het nog in zijn hoofd halen om het belang van cybersecurity te bagatelliseren. Door de Inspectie van het onderwijs, het ministerie van OCW en de Autoriteit Persoonsgegevens zijn rapporten en brieven geschreven die aandringen op een verhoogde digitale weerbaarheid in het onderwijs. De schaamteloosheid van cybercriminelen is niet gering met enorme herstelkosten als gevolg. Investeren in cybersecurity is niet alleen een kostenpost maar inmiddels een verdienmodel: Return on Security Investment (ROSI).

Informatiebeveiliging en privacybescherming dragen bij aan:
- Waardecreatie: door het ontwikkelen van kennis en talent en het daartoe faciliteren van samenwerking en flexibiliteit in een eigentijdse en veilige digitale leer-, onderzoeks- en werkomgeving.
- Waardebehoud: door het waarborgen van data-integriteit en veiligheid van informatie en ontwikkelde kennis, met voorspelbare kwaliteit en compliant aan wet- en regelgeving.

Zeven strategische beleidsprincipes zijn binnen Fontys leidend, namelijk:
1. **Return on Security Investment**
   Informatiebeveiliging en privacybescherming bij Fontys dragen bij aan waardecreatie en waardebehoud.
2. **Risico-gebaseerd**
   We baseren maatregelen op de mogelijke risico's voor Fontys; wet- en regelgeving is naast de Fontys Strategiekaart en het cyberdreigingsbeeld in het hoger onderwijs, de basis voor het identificeren van risico's.
3. **Iedereen**
   De verantwoordelijkheid voor informatiebeveiliging en privacybescherming ligt bij iedereen en het management stuurt hierop.
4. **Altijd**
   Informatiebeveiliging en privacybescherming zijn cyclische processen die verankerd zijn in exploratie, verandering, exploitatie en beëindiging.
5. **Security by Design**
   Fontys verankert informatiebeveiliging en privacybescherming in processen en management in denken en doen.
6. **Security by Default**
   Toegang tot informatie is afgeschermd en wordt alleen specifiek voor gebruikers opengezet op basis van het 'need to know'-principe ("Gesloten waar nodig en open waar mogelijk")
7. **Samenwerking**
   Vanuit het perspectief van macrodoelmatigheid kijkt en volgt Fontys wat "sector overstijgend samen" en "sectorspecifiek aanvullend" gedaan kan worden.

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 Fontys 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 nooit klaar. Het is een continu proces, waarbij we steeds kijken naar mogelijke verbeteringen. Dit gebeurt onder andere door jaarplannen, controles en bijsturing. Naast security & privacy officers kunnen ook de Functionaris Gegevensbescherming (FG) en de interne auditors hier adviezen voor geven.

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

1. INLEIDING

Het succes van Fontys 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[1]. 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 Fontys-diploma(certificaat), behaalde cijfers of de legitimiteit van onderzoekconclusies ondermijnen.

Ook de privacy[2] van studenten, medewerkers en relaties en de reputatie van Fontys kunnen worden geschaad. Informatiebeveiliging is daarom van cruciaal belang. Borgen van veiligheid is dan ook opgenomen in de strategie Fontys for Society 2021-2025. Dit wordt onder andere bereikt door alle ondersteunende processen Fontysbreed te harmoniseren en te verbeteren.

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 relaties van Fontys 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 complex en dynamisch proces. In dit document zijn om die reden zeven hoofdprincipes leidend voor informatiebeveiliging binnen Fontys. De vast te stellen maatregelen, procedures en richtlijnen kunnen getoetst worden aan de zeven hoofdprincipes die in hoofdstuk 4 zijn beschreven.

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

---

1 Zie toelichting paragraaf 3.1 over verschillen in de definities 'informatieveiligheid' en 'informatiebeveiliging'

2 Voor het specifieke Privacy beleid van Fontys zie **https://fontys.nl/Over-Fontys/Nieuws-tonen-op/Privacybeleid.htm**

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

2. WET- EN REGELGEVING

Fontys streeft ernaar om in al haar processen en procedures te voldoen aan de relevante wet- en regelgeving. Dit doet Fontys op basis van het principe “Pas toe of leg uit”, waardoor Fontys altijd kan verantwoorden waarom Fontys wel of niet voldoet. Fontys is **risico avers** als het gaat om wetgeving en de SURF regelgeving informatiebeveiliging. In bijlage D is een overzicht opgenomen van de relevante wet- en regelgeving.

3. DEFINITIE, DOELSTELLING, DOELGROEP EN REIKWIJDTE

3.1 Informatieveiligheid en Informatiebeveiliging

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

De eindverantwoordelijkheid voor informatieveiligheid ligt bij het bestuur van Fontys.

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 Fontys 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.

Fontys heeft de ambitie om met behulp van dit beleidsdocument de informatieveiligheid structureel naar een hoog niveau te brengen en daar te houden. Dit doet Fontys door het beschrijven van verantwoordelijkheden, taken en bevoegdheden en naleven van wet- en regelgeving. Fontys volgt voor informatiebeveiliging het meest actuele SURF normen- en toetsingskader informatiebeveiliging hoger onderwijs.

Het IB-beleid, en de opvolging daarvan, moet Fontys in staat stellen ‘in control’ en compliant te zijn. Op basis daarvan kunnen de betrokken directeuren samen verantwoording afleggen aan het college van bestuur; het College van Bestuur legt verantwoording af aan de Raad van Toezicht. De uitvoering van het beleid is ook de basis is om te voldoen aan wettelijke voorschriften.

3.2.1 Randvoorwaarden

Om deze doelstellingen te kunnen bereiken zijn de volgende randvoorwaarden voor Fontys 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.

- **Werken onder architectuur**
  Het onderwijs kent een autonome besturingsfilosofie, ook binnen de instellingen zelf. Dit heeft geleid tot een grote hoeveelheid aan oplossingen, weinig samenhang en veel koppelingen. Binnen Fontys ook IT-spaghetti genoemd. Het harmoniseren van ondersteunende processen zoals beschreven in Fontys for Society 2021-2025 en werken onder architectuur moet leiden tot goed zicht en grip op de informatievoorziening. Dit is namelijk cruciaal voor de informatieveiligheid. Werken onder architectuur leidt tot maximale samenhang en minimale koppelingen. Hierdoor komt Fontys beter in control, ook voor wat betreft informatieveiligheid en privacybescherming.
- **Eigenaarschap**
  Fontys for Society 2021-2025 schrijft: ''Alle ondersteunende processen gaat Fontys bedrijfsbreed harmoniseren en verbeteren, onder proceseigenaarschap van één van de diensten en in nauwe samenwerking met betrokken professionals in de instituten.'' Het naleven van de door het cvb goedgekeurde notitie over proceseigenaarschap behoort tot een van de randvoorwaarden voor informatieveiligheid op het juiste niveau.
- **(Centrale) regie op digitalisering**
  Zorgdragen voor een voor de organisatie passende portfolio aan veranderopgaven in lijn met Fontys for Society 2021-2025, waarbij programma's en projecten gestuurd worden op kwaliteit en risico's.
- **Houding en gedrag ten aanzien van veiligheid**
  Goed gedrag is het juiste doen ook als niemand kijkt. Medewerkers zijn altijd in staat om beveiligingsmaatregelen te omzeilen. Voldoen aan dit IB-beleid betekent een groot bewustzijn van veiligheid- en informatierisico's, waarbij leidinggevenden het goede voorbeeld geven (tone at the top). Veiligheid is een integraal onderdeel van ons denken en handelen.

3.2.2 Uitgangspunten

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

- **Kader**
  Het beleid biedt een kader om (toekomstige) maatregelen in de informatiebeveiliging te toetsen aan de vastgestelde beveiligingsprincipes (hoofdstuk 4), best practices en normen. Daarnaast biedt het een kader om de taken, bevoegdheden en verantwoordelijkheden in de instelling te beleggen.
- **Normen**
  Specifiek voor de SURF gemeenschap[4] is het 'SURF Normenkader informatie Beveiliging Hoger Onderwijs' (IBHO) vastgesteld. Het IBHO is gebaseerd op de normen die zijn vastgelegd in de ISO-27000-serie. Het IBHO vormt samen met dit beleidsdocument de basis voor een informatie-beveiligingsmanagementsysteem (ISMS[5], zie bijlage A) van Fontys. Het ISMS van Fontys is ingericht op basis van het SURF normen- en toetsingskader.
- **Volwassenheid**
  SURF omschrijft een norm voor de volwassenheid van de informatiebeveiliging volgens het Capability Maturity Model (CMM)[6]. Fontys volgt de SURF baseline, die CMM niveau 3 voorschrijft.
- **Maatregelen**
  Fontys 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 Fontys zijn te vinden in het Fontys ISMS tool.

---

4 De actuele documenten zijn te vinden op **https://www.surf.nl/informatiebeveiliging** en **https://www.surf.nl/surfaudit-inzicht-in-je-informatiebeveiliging-en-privacy** en voor SCIPR-leden op de ondersteunende wiki's **https://wiki.surfnet.nl/display/SCIPR/SCIPR+Home** en **https://wiki.surfnet.nl/display/SA/SURFaudit+Home**

5 ISMS: Information Security Management System.

6 **https://nl.wikipedia.org/wiki/Capability_Maturity_Model**

3.3. Doelgroep

Het IB-beleid is primair bestemd voor medewerkers op strategisch en tactisch niveau, waaronder het bestuur, directeuren en managers. Zij zien toe dat uiteindlijk iedereen die – intern of extern – te maken heeft met de informatievoorziening van Fontys zich houdt aan dit beleid. Het beleid is van toepassing op alle medewerkers, docenten, studenten, gasten, bezoekers en externe relaties.

3.4. Reikwijdte van het beleid

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

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

Onder apparaten en applicaties vallen:

- Alle fysiek op het netwerk aangesloten apparaten zoals servers, werkstations, laptops, gebouwbeheerssystemen.
- Alle draadloos op het netwerk aangesloten mobiele apparaten, zoals notebooks, tablets, smartphones, smartwatches.
- IoT[7]-devices, zoals bewakingscamera's en sensoren.
- Alle op deze apparaten beschikbare (web/cloud)services en applicaties ('apps').

Meerdere regelingen geven een verdere invulling aan dit beleid. Dit zijn regelingen over bijvoorbeeld gedragscodes, authenticatie, patchen, mobiele apparatuur en beeldopnamen. Diensten en instituten kunnen zelf invulling geven aan specifieke regelingen, echter altijd in lijn met dit beleid en ISP-kaders.

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

7 Internet of Things

4. BELEIDSPRINCIPES INFORMATIEBEVEILIGING

4.1. Inleiding

Fontys is een instelling met een open karakter. Wanneer het aankomt op wet- en regelgeving zijn wij risico-avers. Vanuit het onderwijs- en onderzoeksperspectief is de insteek ''Gesloten waar nodig, open waar mogelijk''. Dat past ook bij de FAIR doelstellingen in het onderzoekdomein. Adequate beveiliging van informatie is steeds een randvoorwaarde en het openstellen van informatie moet een bewuste keuze zijn.

Fontys heeft zeven 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 zeven 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 een-op-een 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''[8].

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

4.2. Beleidsprincipes

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

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.

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

Fontys wil beschikken over een eigentijdse en veilige digitale leer-, onderzoeks- en werkomgeving. Informatiebeveiliging en privacybescherming zijn essentieel voor het bereiken van deze doelstelling en dus voor het risicomanagement bij Fontys. De volgende principes vormen een leidraad voor de informatiebeveiliging en privacybescherming binnen Fontys:

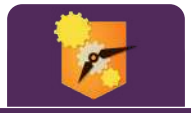
De zeven door Fontys vastgestelde strategische en tactische informatiebeveiligingsprincipes zijn:

1. Return on Security Investment
2. Risico-gebaseerd
3. Iedereen
4. Altijd
5. Security by Design
6. Security by Default
7. Samenwerken

> 1	**Return on Security Investment** Informatieveiligheid is een enabler voor vele digitale diensten
Kern	Informatiebeveiliging en privacybescherming bij Fontys dragen bij aan waardecreatie en waardebehoud.
Achtergrond	Informatiebeveiliging en privacybescherming dragen bij aan: • Waardecreatie: door het ontwikkelen van kennis en talent en het daartoe faciliteren van samenwerking en flexibiliteit in een eigentijdse en veilige digitale leer-, onderzoeks- en werkomgeving. • Waardebehoud: door het waarborgen van data-integriteit en veiligheid van informatie en ontwikkelde kennis, met voorspelbare kwaliteit en compliant aan wet- en regelgeving. Onderwijsinstellingen die weerbaar zijn tegen cybercrime en de privacy van studenten goed beschermen, hebben een streepje voor op de concurrentie.
Implicaties	Denk hierbij aan een veilige digitale leer-, onderzoeks- en werkomgeving en compliant aan wet- en regelgeving. Zie Bijlage B voor een overzicht van alle implicaties.

> 2	**Risico-gebaseerd** Informatiebeveiliging is risico-gebaseerd
Kern	We baseren maatregelen op de mogelijke risico's voor Fontys; wet- en regelgeving is naast de Fontys Strategiekaart en het cyberdreigingsbeeld in het hoger onderwijs, de basis voor het identificeren van risico's.
Achtergrond	Het delen van kennis (openheid) is een belangrijke kernwaarde van het onderwijs- en onderzoekproces van Fontys. 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.

> 3	**Iedereen** Informatiebeveiliging is een verantwoordelijkheid van iedereen
Kern	De verantwoordelijkheid voor informatiebeveiliging en privacybescherming ligt bij iedereen en het management stuurt hierop.
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.



> 4	**Altijd** Informatiebeveiliging is een continu proces
Kern	Informatiebeveiliging en privacybescherming zijn cyclische processen die verankerd zijn in exploratie, verandering, exploitatie en beëindiging.
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.

> 5	**Security by Design** Integrale aanpak informatiebeveiliging
Kern	Fontys verankert informatiebeveiliging en privacybescherming in processen en management in denken en doen.
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.

> 6	**Security by Default** Standaard beperkte toegang en veilige instellingen
Kern	Toegang tot informatie is afgeschermd en wordt alleen specifiek voor gebruikers opengezet op basis van het need to know-principe (‘‘Gesloten waar nodig en open waar mogelijk’’).
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.
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.

> 7	**Samenwerken** Binnen de sector als sector overstijgend samenwerken
Kern	Vanuit het perspectief van macrodoelmatigheid kijkt en volgt Fontys wat ‘‘sector overstijgend samen’’ en ‘‘sectorspecifiek aanvullend’’ gedaan kan worden.
Achtergrond	Structureel samenwerken met partijen buiten en binnen het hoger onderwijsstelsel en kennis delen met als doel elkaar bewust en scherp te houden op het gebied van cyberveiligheid.
Implicaties	Denk hierbij aan het samenwerken binnen SURF, zoals normenkaders, model IB-beleid, gezamenlijk inkopen en de SURFsoc dienstverlening. Zie Bijlage B voor een overzicht van alle implicaties.

5. GOVERNANCE INFORMATIEBEVEILIGINGSBELEID

5.1. Afstemming met samenhangende risico's

Bij governance moet aandacht zijn voor alle soorten risico's en hun onderlinge samenhang. Om die reden besteedt Fontys op strategisch niveau veel aandacht aan afstemming om de verschillende thema's binnen Integrale Veiligheid: Crisismanagement, Information Security en Privacy, Kennisveiligheid, Internationalisering, Gebouwveiligheid en BHV, Sociale veiligheid, Integriteit, Arbo en milieu in gezamenlijkheid op te pakken. Waar mogelijk en nodig vertaalt deze afstemming zich ook naar het tactische en operationele niveau.

5.2. Organisatie van de informatiebeveiliging

Deze paragraaf beschrijft hoe de governance van informatiebeveiliging is georganiseerd, wie waarvoor verantwoordelijk is en aan wie wordt gerapporteerd. De governance van informatiebeveiliging bij Fontys is ingericht volgens het zogenaamde IAA's Three Lines Model[9]. 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 De eerste lijn: directeuren, managers, ISP-contactpersonen, projectleiders

Het Three-lines-model heeft als uitgangspunt dat het lijnmanagement (de business) verantwoordelijk is voor haar eigen informatie risicomanagement. De directeuren van onderwijsinstituten en ondersteunende diensten zijn verantwoordelijk voor de implementatie en naleving van het informatiebeveiligingsbeleid. Zij zorgen ervoor dat beveiligingsmaatregelen ook werkelijk worden geïmplementeerd, dat awareness-programma's worden uitgevoerd, dat personeel wordt opgeleid, etc. De ISP-contactpersonen bewaken namens de gemandateerde directeur het informatiebeveiligingsbeleid binnen hun eigen onderwijsinstituut of dienst. Zij vormen de eerste lijn als het gaat om informatiebeveiligingsrisico's te signaleren en om hiervoor de juiste maatregelen te nemen om het risico te reduceren tot een acceptabel niveau. Hierbij worden zij ondersteund door o.a. managers en projectleiders. Dit is de eerste lijn.

5.2.2 De tweede lijn: het Information Security and Privacy Office van Fontys

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, integrale risicoanalyses, self-assessments en het opstellen van jaarplannen en rapportages zijn taken van de tweede lijn. De tweede lijn rapporteert rechtstreeks aan het bestuur.

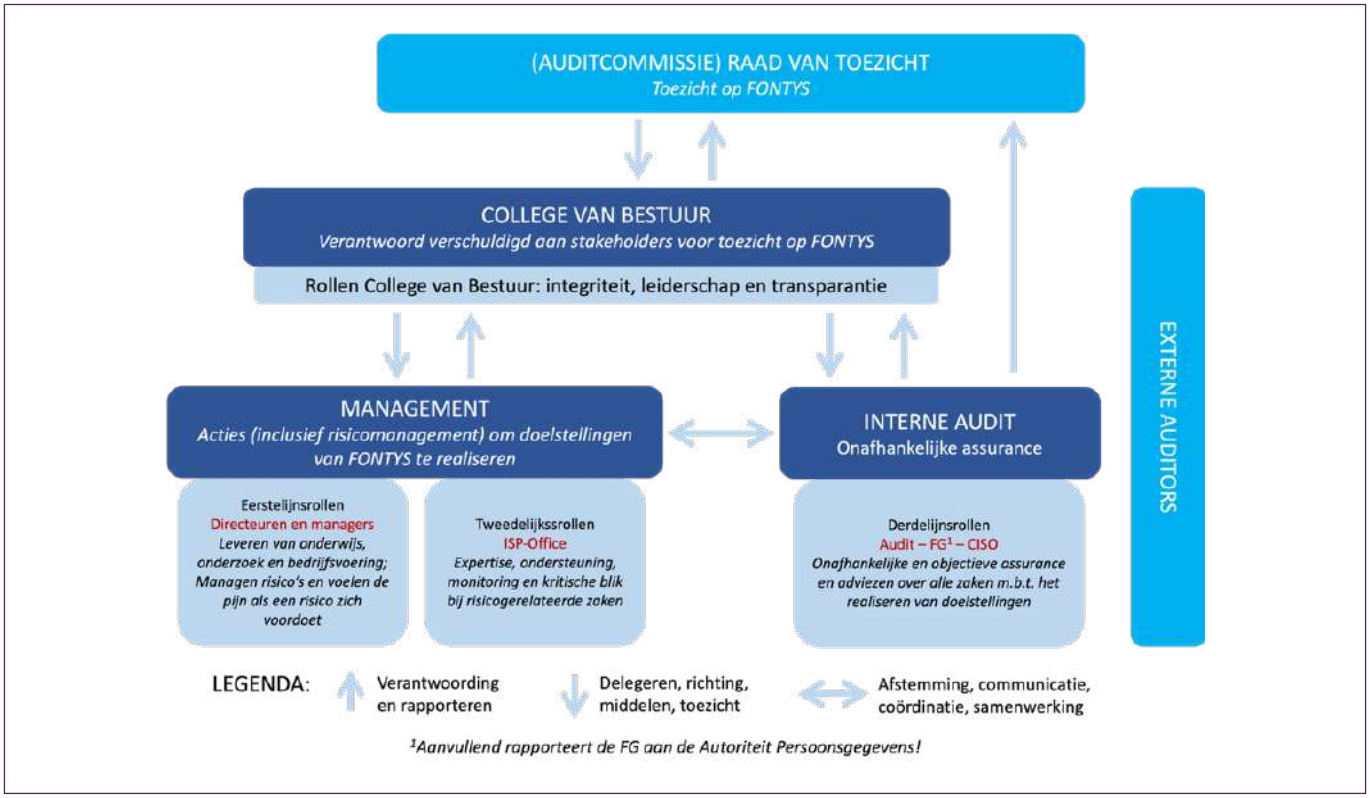
Experts op het gebied van informatiebeveiliging en privacybescherming (information security & privacy officers) werken samen binnen het Information Security and Privacy Office (ISP-office). Zij vormen de second line of defense. Het ISP-office monitort de toepassing en naleving van het informatiebeveiligings- en privacybeleid, adviseert over informatiebeveiliging en privacybescherming en ondersteunt de ISP-contactpersonen.
Het ISP-office wordt geleid door de Corporate Information Security Officer (CISO). De CISO geeft functioneel leiding aan de werkzaamheden van de Information Security & Privacy Officers.

9 https://na.theiia.org/translations/PublicDocuments/Three-Lines-Model-Updated-Dutch.pdf

5.2.3 De ‘derde lijn’: Functionaris Gegevensbescherming (FG) en Auditors

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 auditors behoren typisch tot de derde lijn. Zij opereren volledig los van alle andere organisatieonderdelen en rapporteren niet alleen aan het College van Bestuur, maar ook aan de Raad van Toezicht.



Figuur 1 IIA’s Three Lines Model, vertaald naar de Fontys organisatie

IIA staat voor Instituut van Internal Auditors. In bijlage E wordt de invulling van het IIA’s Three lines model binnen Fontys geschetst en staan de rollen gericht op informatiebeveiliging en privacy binnen Fontys omschreven.

5.2.4 Eindverantwoordelijkheid

Juridisch gezien is het College van Bestuur (CvB) eindverantwoordelijk voor informatieveiligheid en daarmee ook voor Informatiebeveiliging van de instituten en ondersteunende diensten. Specifieke onderdelen van deze verantwoordelijkheid worden via de mandaatregeling[10] bij de directeuren binnen de instituten en diensten verder belegd.

10 Uitvoeringsregeling artikel 16 lid 1 van het Bestuurs- en beheersreglement Stichting Fontys

5.2.5 Taken, bevoegdheden, verantwoordelijkheden

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

De actuele invulling voor Fontys van rollen op functies c.q. functionarissen is te vinden in Bijlage E - Actuele invulling rollen Informatiebeveiliging.

Niveau	Wat?	Wie?	Documenten
Richtinggevend (strategisch)*	• Bepalen IB-strategie • Organisatie voor IB inrichten • IB planning en control vaststellen • Business continuity management • Communicatie naar management en organisatie	• College van Bestuur (de portefeuillehouder IB) op basis van advies van CISO en directeur Dienst-IT/CIO	• De informatie-beveiligingsstrategie maakt integraal deel uit de van de Fontys digitaliserings-strategie • Informatie-beveiligingsbeleid • Privacybeleid • Gedrag- en Integriteitscode • ISMS-proces • Classificatie-richtlijn
Sturend (tactisch)*	• PDCA-cyclus • Voorbereiden normen en wijze van toetsen • Monitoren en evalueren beleid en maatregelen, ook van externe partijen bij contracten • Begeleiden self assessments en in- en externe audits • Communicatie naar data-, proces- en systeem-eigenaren (business security) • Communicatie naar Manager ICT (cybersecurity)	• Data-, proces- en systeemeigenaren • CISO • Manager ICT • Security & Privacy officers • Compliance officer • Directeuren op basis van advies ISP-contactpersonen	• Jaarplan FG • Jaarplan ISP-Office • Classificaties/Risico-analyses en audits, inclusief DPIA's en SURFaudit • IB baselines (basismaatregelen) • IB-paragraaf in MARAPs • ISP MARAP • ISP Nieuwsbrief • Bedrijfscontinuïteits-plan
Uitvoerend (operationeel)*	• Implementeren IB-maatregelen. • Registreren en evalueren van informatiebeveiligings-incident • Registreren en evalueren van datalekken • Communicatie naar eindgebruikers • Opvolging van voorschriften en maatregelen. Melding incidenten.	• IT in samenwerking met data-, proces- en systeemeigenaren • ISP-contactpersonen • Functioneel beheerders • Teamleiders • Fontys CERT • Key-gebruikers (optie)	• SLA's (security-paragraaf) • informatiebeveiligings-incident registratie en evaluatie • Datalek registratie en evaluatie • Geprioriteerde kwestsbaarheden • Handboek Fontys CERT

Tabel 2 Taken, bevoegdheden verantwoordelijkheden incl. rollen, functies en documenten op strategisch, tactisch en operationeel niveaus

* Strategisch, Tactisch en Operationeel IB overleg zijn generieke namen voor de op deze niveaus ingerichte overleg vormen.

5.2.6 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 Fontys gestructureerd overleg gevoerd over het onderwerp informatiebeveiliging op diverse niveaus.

Strategisch	Tactisch	Operationeel
Op strategisch niveau wordt richtinggevend gesproken over governance en compliance, alsmede over doelen, scope en ambitie op het gebied van informatiebeveiliging, in samenhang met privacy. Dit gebeurt in verschillende samenstellingen: • In lijn met de MARAP-cyclus geeft de CISO een toelichting op de ISP-MARAP aan het voltallig CvB. • Elke 6 weken is er een overleg tussen de portefeuillehouder IB, de CISO, de FG en de CIO. • Maandelijks komt de enterprise architecture board bij elkaar, bestaande uit CIO, enterprise architect en CISO. • Op ad-hoc basis zijn de CISO en FG te gast in het Dienst directeuren overleg. • Elke 4 weken heeft de CISO en de FG een overleg met Audit CvB waarin de uitkomsten van audits, risico's en maatregelen worden besproken. • Elke twee weken heeft de CISO een overleg met de CIO over de lopende IB-zaken.	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 vindt plaats op de volgende momenten: • Het wekelijke Integraal Informatiemanagement (IM)-advies-overleg. Hieraan neemt een ISP-Office medewerker deel. Tijdens dit overleg worden vernieuwings- of onderhoudsprojecten integraal beoordeeld vanuit Inkoop, Informatiemanagement, architectuur, informatie-beveiliging en privacy. • Elke twee weken heeft de CISO een overleg met de Manager ICT over de stand van zaken m.b.t. technische beheersmaatregelen. • Iedere zes weken worden de ISP-contactpersonen door het ISP-Office bijgepraat over de plannen en voortgang m.b.t. informatiebeveiliging en privacy. Daar waar nodig wordt er overleg gevoerd met overige betrokken functionarissen zoals ISO Dienst-IT, projectleiders, proces-, gegevens- of systeemeigenaren.	Op operationeel niveau worden de zaken besproken die de dagelijkse bedrijfsvoering aangaan in de zin van uitvoering en implementatie. Operationele overleggen die structureel plaatsvinden zijn: • Twee keer per week is het operationeel Fontys CERT overleg. In dit overleg worden de SURFsoc meldingen en security incidenten geprioriteerd en besproken welke technische maatregelen nodig zijn. De ISO van het ISP-Office neemt hier wekelijks aan deel en de CISO op ad-hoc basis. • Operationeel integraal veiligheidsoverleg. Eén keer per maand wordt dit overleg georganiseerd door de coördinator integrale veiligheid. Als vertegenwoordiging vanuit informatiebeveiliging en privacy neemt de CISO deel.

Tabel 3 Overlegstructuren op strategisch, tactisch en operationeel niveaus

5.2.7 Documenten

Voor informatiebeveiliging wordt bij Fontys dezelfde (PDCA-)management¬cyclus 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 G is een uitgebreider overzicht opgenomen van de documenten die Fontys 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 is de zwakste schakel en creëert de grootste risico's. Bij Fontys werken we daarom voortdurend aan de vergroting van het bewustzijn bij medewerkers om kennis van cyber- en privacy 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 functioneel beheerders.

Dit alles laat onverlet dat elke beveiliging faalt als deze niet gedragen wordt door de medewerkers – elke Fontysmedewerker en student is medeverantwoordelijk voor goede beveiliging. Dit is een cruciaal onderdeel van bewustwording en wordt randvoorwaardelijk ondersteund in het personeelsbeleid. Bewustwording is een onderdeel van het introductieprogramma voor nieuwe medewerkers en studenten. Verhoging van dit bewustzijn (naast kennis ook houding en gedrag) is primair de verantwoordelijkheid van alle Fontys directeuren.

5.4. Controle, oefenen, naleving en sancties

Bij Fontys is de afdeling Audit & Control (3e lijn) verantwoordelijk voor de (planning van) interne audits zoals beschreven is in het auditcharter. Binnen Fontys zijn o.a. de volgende uitgangspunten leidend voor het aanbrengen van focus en keuzes in de auditplanning:

- De auditfunctie richt zich op de operationele activiteiten én de verandering daarin, en sluit daarbij aan op de strategische agenda.
- De Fontys Enterprise Architectuur (FEA) geeft het speelveld weer voor de auditor in een kennisinstelling, en vormt daarmee een goed bruikbaar aanknopingspunt voor het identificeren van primaire, ondersteunende of besturingsprocessen met een hoog risicoprofiel.
- De focus ligt op processen, op de informatievoorziening, en - bij verandering - op projecten of programma's met een hoog risicoprofiel.
- Actualiteiten en externe ontwikkelingen die spelen.

Audit doet jaarlijks een voorstel voor de auditplanning. Mogelijke risico's en onderwerpen worden vooraf besproken met belangrijke stakeholders, waaronder de CISO en de Functionaris Gegevensbescherming. Audits op informatievoorziening, informatiebeveiliging en privacy vlak kunnen onderdeel uitmaken van de planning. De uiteindelijke planning ligt ter goedkeuring voor aan het college van bestuur. Indien urgente bevindingen op het vlak van informatievoorziening, informatiebeveiliging en privacy tijdens een audit naar voren komen worden ze door de auditors gerapporteerd, echter deze onderwerpen zijn niet automatisch in scope bij elke audit en worden niet standaard getoetst. Indien specialistische kennis noodzakelijk is voor een audit en niet voorhanden is in het bestaande auditteam, dan zal deze expertise extern ingehuurd worden.
De CISO is samen met het ISP office (beide 2e lijn) verantwoordelijk voor de controle op de uitvoering van de informatiebeveiligings¬jaarplannen van instituten en diensten (1e lijn). Alle Fontys directeuren, in samenspraak met de eigen ISP-contactpersoon, beschrijven in de informatiebeveiligingsparagraaf van de MACON de speerpunten voor informatiebeveiliging en privacy voor dat kalenderjaar. De ISP-contactpersoon vertaalt dit naar een informatiebeveiligingsjaarplan. Vervolgens rapporteert de directeur in de MARAP-cyclus aan het CvB over de voortgang van het eigen informatiebeveiligingsjaarplan. Daar waar nodig adviseert het ISP-office over het op te stellen instituutsjaarplan.

De interne controles vanuit ISP office vinden jaarlijks plaats en worden 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 oefeningen. Voorbeelden hiervan zijn cybercrisisoefeningen of incidentoefeningen. Fontys neemt elk jaar deel aan de SURF cybercrisisoefening NOZON/OZON voor het Hoger Onderwijs.

Als een informatiesysteem wordt vervangen of als er belangrijke wijzingen plaatsvinden in de beveiliging, wordt er een quality assurance onder verantwoordelijkheid van het project- of programmamanagement uitgevoerd op basis van een nieuwe businessimpact en risicoanalyse.

De externe controle wordt tweejaarlijks uitgevoerd door een onafhankelijke partij (4e lijn). De focus van IT auditwerkzaamheden door de externe accountant is beperkt tot de (delen van de) geautomatiseerde omgeving die relevant is voor de jaarrekeningcontrole. Dit wordt zoveel mogelijk gecombineerd met de normale planning & control-cyclus.

Het SURF normen- en toetsingskader Informatiebeveiliging Hoger Onderwijs (IBHO), dat is gestoeld op ISO 27001/27002 en het NBA/NOREA Volwassenheidsmodel Informatiebeveiliging[11] wordt gebruikt als uitgangspunt voor interne en externe controles. Fontys neemt deel aan de SURFaudit self-assessment cyclus en de bijbehorende tweejaarlijkse benchmark.

De bevindingen van de interne en externe controles/audits en mogelijke externe eisen met betrekking tot beveiliging, zijn input voor de nieuwe jaarplannen van Fontys. 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 en privacy wordt omgegaan (verantwoordelijkheid van de 1e en 2e lijn o.a. ISP-Office en ISP-contactpersonen). Hierbij is het van belang dat leidinggevenden (inclusief onderwijsverantwoordelijken) de medewerkers en studenten aanspreken op tekortkomingen.

Als uit de controles blijkt dat de naleving ernstig tekortschiet, dan kan Fontys de betrokken verantwoordelijke medewerkers of studenten een sanctie opleggen. De sanctie wordt opgelegd binnen de kaders van de cao, arbeidsovereenkomsten, ICT gedragscode en de wettelijke mogelijkheden in bijvoorbeeld de Wet op het Hoger Onderwijs en wetenschappelijk onderzoek (WHW). Primair is dit een verantwoordelijkheid van het cvb, maar dit kan in sommige gevallen worden gemandateerd aan de verantwoordelijke leidinggevenden.

5.5. Financiering

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

Centraal
Het ISP-Office heeft een jaarlijks eigen budget voor het Fontys ISMS-systeem, gevraagd en ongevraagd onderzoek (e.g. penetration testing en red teaming), extra ISP-Office capaciteit, Fontysbrede bewustwordingscampagnes en vakspecifieke opleidingen. Algemene zaken, zoals het uitvoeren van interne en externe audits, worden uit de algemene middelen betaald.

Decentraal
Cybersecurity
Technische beheersmaatregelen vallen onder de Dienst-IT. De kosten voor SURFsoc, Fontys Operation Center, Fontys CERT, 24x7 CERT, technische beheersmaatregelen voor het netwerk, de servers en 'endpoints' vallen binnen deze dienst.

Business security
De beveiliging van informatiesystemen en processen, inclusief de kosten daarvan, zijn integraal onderdeel van verantwoord beheer van het betreffende informatiesysteem of proces. Er is altijd een eigenaar (veelal een dienstdirecteur) hiervoor verantwoordelijk. Programma's en projecten gericht op het onderhoud of de vernieuwing van de informatievoorziening dienen een apart budget op te nemen voor informatiebeveiliging en privacy. Voorlichting en training voor specifieke toepassingen of doelgroepen worden uit decentrale middelen betaald.

11 https://www.nba.nl/intern-en-overheidsaccountants/volwassenheidsmodel-informatiebeveiliging/

6. MELDING EN AFHANDELING VAN INCIDENTEN EN DATALEKKEN

Een incident is een gebeurtenis die de bedrijfsvoering negatief kan beïnvloeden. Incidentbeheer en -registratie gaat over het detecteren, vastleggen en afhandelen van incidenten. Een informatiebeveiligingsincident is een enkele of serie van ongewenste of onverwachte gebeurtenissen die een significante kans hebben op het veroorzaken van een ramp, het compromitteren van de bedrijfsprocessen en een bedreiging vormen ten aanzien van de beveiliging. Belangrijk hierbij is dat medewerkers, studenten en derden herkennen wanneer er sprake is van een incident of informatiebeveiligingsincident en dit ook melden.

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

Incidenten en inbreuken op de informatiebeveiliging kan men bij Fontys melden bij de IT Servicedesk: Telefonisch: +31 8850 77777; e-mail: **it-servicedesk@fontys.nl**. Fontys heeft de contactgegevens van dit meldpunt duidelijk gecommuniceerd naar haar medewerkers, studenten en derden.

Iedere medewerker, student en derde is ook verantwoordelijk voor het signaleren van datalekken. Datalekken dienen direct gemeld te worden aan het ISP-Office en worden onder coördinatie van het ISP-Office afgehandeld. Datalekken kan men bij Fontys melden via het online meldformulier datalek: **https://intern.fontys.nl/Meldformulier-Datalek** Fontys heeft de contactgegevens van dit meldformulier duidelijk gecommuniceerd naar haar medewerkers, studenten en derden. Voor ondersteuning bij het melden van een datalek kunnen medewerkers en studenten terecht bij de ISP-contactpersoon.

Dienst-IT heeft een stand-by dienst als het gaat over ernstige incidenten buiten reguliere bedrijfstijden.

Voor ernstige informatiebeveiligingsincidenten is er de binnen Dienst-IT de High Impact procedure. Indien een ernstig incident leidt tot een crisis, komt het Fontys Centraal Crisis Team (CCT) in actie: **https://connect.fontys.nl/diensten/HenF/Paginas/Crisismanagement.aspx**

Zodat Fontys leert van haar incidenten worden alle ernstige informatiebeveiligingsincidenten en datalekken geëvalueerd onder coördinatie van het ISP-Office. Hierbij zijn altijd aanwezig, de direct betrokken medewerker, de directeur, de ISP-contactpersoon, de CISO en de FG. Doel is wat Fontys kan leren van het incident en/of datalek, zodat maatregelen worden bedacht en geïmplementeerd om herhaling te voorkomen.

Iedere medewerker, student en derde kan kwetsbaarheden bij Fontys melden via het online meldformulier Responsible Disclosure: **https://fontys.nl/Over-Fontys/Onze-organisatie-1/Responsible-disclosure-Fontys-Hogescholen.htm**. Daarmee geeft Fontys mogelijke melders van kwetsbaarheden in de informatiesystemen een garantie dat Fontys, onder voorwaarden, geen juridische stappen tegen hen onderneemt.


Lenovo

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. Het wordt 1x per 2 jaar geëvalueerd en zo nodig bijgesteld. 1 keer per 5 jaar, of na een substantiële verandering van het instellingsbeleid of belangrijke ontwikkelingen op cyberveiligheidsgebied, wordt het beleid herzien en opnieuw vastgesteld.

Dit beleid, versie 2021, is vastgesteld door het bestuur van Fontys op <datum> en kan worden aangehaald als het ''Informatiebeveiligingsbeleid van Fontys''.


Easy Scan
Dat is zo gebleven!
ASTRO WORLD

BIJLAGE A - SCHEMATISCH OVERZICHT INRICHTING FONTYS ISMS

Waarom een Fontys Information Security Management Systeem (ISMS)?

Een ISMS is ondersteunend aan de doelstelling om informatieveiligheid over een langere periode op een steeds hoger volwassenheidsniveau uit te voeren. Het hebben van een ISMS is geen eenmalige activiteit of een project. Het is een voortdurend kwaliteitsproces dat binnen Fontys uitgevoerd wordt. Het hoofddoel van een ISMS is het verbeteren van de effectiviteit van informatiebeveiliging en privacy door een procesmatige aanpak, die wordt ondersteund door de Fontys organisatie.

Voor het effectueren van informatiebeveiliging en privacy wordt binnen het ISMS gewerkt met een verbetercyclus, zoals de PDCA-cyclus. Deze PDCA-cyclus sluit aan bij de Planning & Control-cyclus, oftewel de MACON/MARAP-cyclus van Fontys. Na het uitvoeren van risicoanalyses en vaststellen van wat nodig is om de gevonden risico's te beheersen, worden maatregelen getroffen en vervolgens wordt gecontroleerd of die maatregelen het gewenste effect hebben (controle). Risico's kunnen in de tijd gezien veranderen (omdat de omgeving en bedreigingen ook veranderen) en daarom worden er periodiek controles uit te voeren. Via een vastgesteld auditplan van Audit & Control, in afstemming met het ISP-office, worden jaarlijks keuzes gemaakt voor welke systemen welk soort beveiligingsaudits worden uitgevoerd. Deze controles kunnen dus aanleiding geven tot bijsturing in de maatregelen. Daarnaast kan het totaalpakket van eisen, maatregelen en controle aan een herijking toe zijn (evaluatie). Het goed doorlopen van de stappen kan op elk moment zorgen voor een passend beveiligingsniveau.

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. De jaarlijkse planning en de voortgang ervan zijn bij Fontys te vinden in de MACON respectievelijk MARAP-rapportages van diensten en instituten in de paragraaf 'Informatiebeveiliging'.

Door herhaling van de PDCA-cyclus werkt de organisatie doorlopend aan het verbeteren van het ISMS en is daardoor meer 'in control'.

Stappen in de ISMS

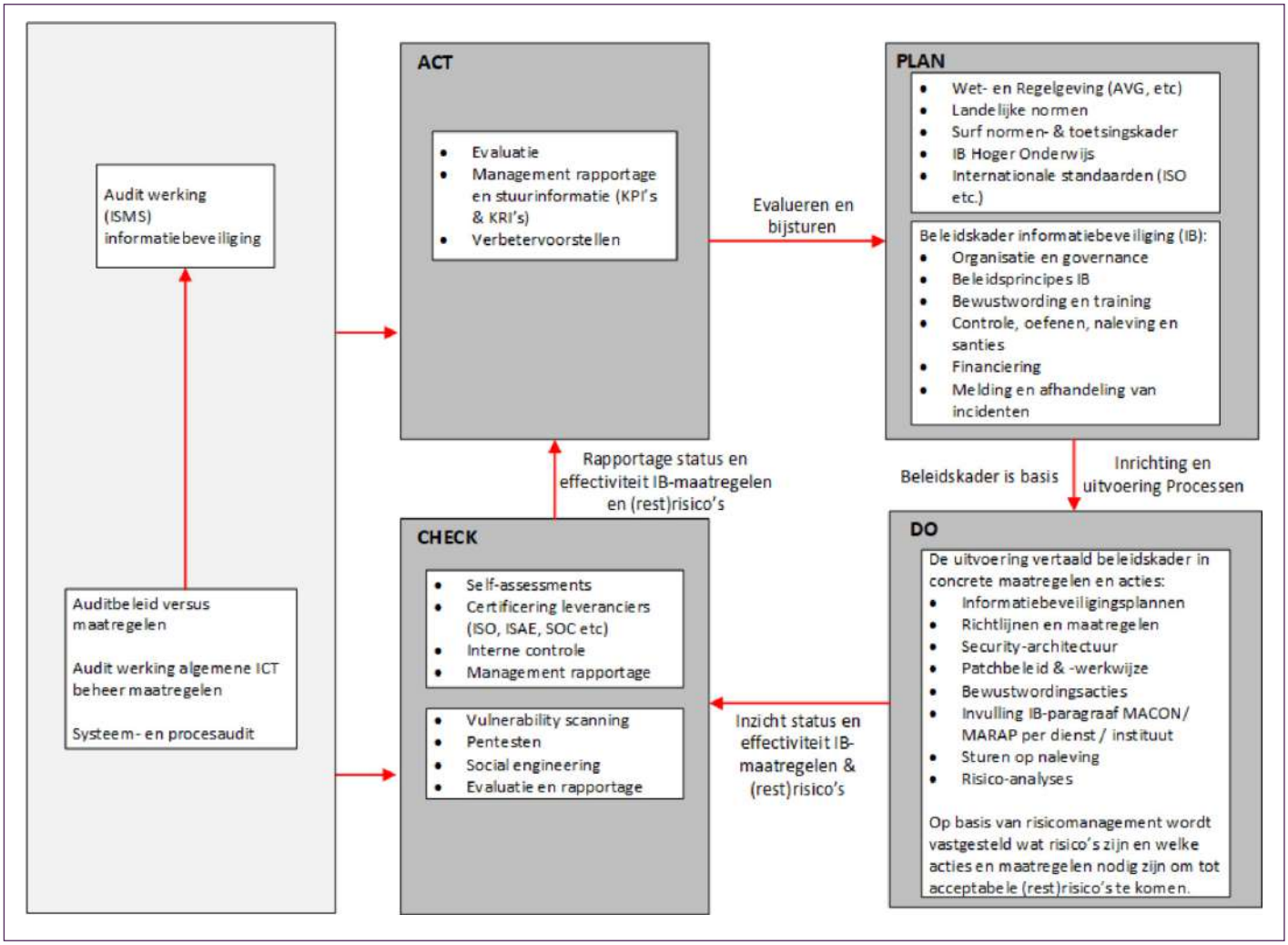
Voor de inrichting van het ISMS zijn allerlei vereisten gesteld:

- Begrip van de context van de organisatie: externe en interne omgeving;
- Begrip van de behoeften en verwachtingen van belanghebbende partijen;
- Een goede beschrijving van de scope van het ISMS: wat valt eronder en wat doet niet mee;
- Leiderschap en commitment, zonder welke informatiebeveiliging in een organisatie niet serieus genomen kan worden.

Vervolgens moet het ISMS opgesteld worden.
De PDCA-cyclus omvat de volgende vier fasen:

1. Plan	2. Do	3. Check	4. Action
In de planfase worden de volgende zaken gedefinieerd: • beleid • scope • bedrijfsmiddelen (assets) • risico's en kansen • middelen • competenties • bewustzijn • communicatie • gedocumenteerde informatie	Bij de uitvoering van het ISMS gaat het om: • de operationele planvorming en beheersing • risicobeoordeling(en) • risicobehandeling	De checkfase omvat de evaluatie van de werking van het ISMS: • bewaking, meting, analyse en evaluatie • interne audit • management review	Op basis van de uitkomsten van de checkfase worden verbeteringen doorgevoerd

Onderstaande figuur geeft de werking van het ISMS binnen Fontys aan.



Figuur 1 Werking van het ISMS binnen Fontys

BIJLAGE B - INFORMATIEBEVEILIGINGSPRINCIPES

1	**Return on Security Investment** Informatieveiligheid is een enabler voor vele digitale diensten
Kern	Informatiebeveiliging en privacybescherming bij Fontys dragen bij aan waardecreatie en waardebehoud.
Achtergrond	Informatiebeveiliging en privacybescherming dragen bij aan: • Waardecreatie: door het ontwikkelen van kennis en talent en het daartoe faciliteren van samenwerking en flexibiliteit in een eigentijdse en veilige digitale leer-, onderzoeks- en werkomgeving. • Waardebehoud: door het waarborgen van data-integriteit en veiligheid van informatie en ontwikkelde kennis, met voorspelbare kwaliteit en compliant aan wet- en regelgeving. Onderwijsinstellingen die weerbaar zijn tegen cybercrime en de privacy van studenten goed beschermen, hebben een streepje voor op de concurrentie.
Implicaties	• Een eigentijdse en veilige digitale leer-, onderzoeks- en werkomgeving • Risico gebaseerd ontwikkelen van kennis en talent • Waarborgen van data-integriteit • Waarborgen van veiligheid van informatie • Waarborgen van ontwikkelde kennis • Waarborgen van bescherming van persoonsgegevens • Zorgdragen voor voorspelbare kwaliteit • Compliant aan wet- en regelgeving.

2	**Risico-gebaseerd** Informatiebeveiliging is risico-gebaseerd
Kern	We baseren maatregelen op de mogelijke risico's voor Fontys; wet- en regelgeving is naast de Fontys Strategiekaart en het cyberdreigingsbeeld in het hoger onderwijs, de basis voor het identificeren van risico's.
Achtergrond	Het delen van kennis (openheid) is een belangrijke kernwaarde van het onderwijs- en onderzoekproces van Fontys. Voor een goede risicoafweging bij het beschermen van informatie en het treffen van de juiste maatregelen, is het van belang om de waarde van informatie vast te stellen. Als de waarde van informatie bekend is, kan ook de juiste mate van beveiliging worden bepaald, één die past bij de risico's. Proportionaliteit daarin is gewenst, ook om de beschikbare financiële middelen efficiënt te gebruiken ('Fit for purpose').

Implicaties	• Voor alle processen en/of applicaties wordt een Business Impact Analyse[12] uitgevoerd. • De risico's worden ingeschat en vastgesteld op basis van een risico¬classificatie. Zie bijlage C. • Fontys stelt een Classificatie Richtlijn vast. • Een gegevensbeschermingseffectbeoordeling (DPIA – Data Protection Impact Assessment) in het kader van de AVG maakt waar nodig onderdeel uit van de risicoanalyse. • Waar nodig worden maatregelen getroffen om het vastgestelde risico op Beschikbaarheid, Integriteit en Ver¬trouwe¬lijk¬heid 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 Fontys, uiteindelijk te bepalen door het bestuur. • Voor afwijkingen moet het risico-acceptatieproces worden gevolgd, met acceptatie door de informatie-, proces- of applicatie-eigenaar. • De proces-eigenaar (en/of data-eigenaar) tekent voor acceptatie van de risico's. • Maatregelen moeten zo worden ingericht dat hun effect controleerbaar is. • De hoogste risico's worden als eerste gemitigeerd. • Op basis van de risicoanalyse kan informatiebeveiliging voor gebruiks¬gemak kiezen. • Maatregelen moeten (qua kosten) in balans zijn met de vermindering van risico's (proportionaliteitsprincipe). • Informatie heeft één bron, waardoor eigenaarschap en ''single point of truth'' goed te duiden is. Hierdoor ontstaat ook een extra ketenverantwoordelijkheid voor de consequenties van wijzigingen bij de bron. • Fontys blijft verantwoordelijk voor adequate bescherming van informatie bij gebruik van externe diensten voor informatieverwerking. • Waar van toepassing bevatten contracten de veiligheidseisen en de levering van externe toetsing (assurance) die laat zien dat maatregelen effectief zijn.

> 3	**Iedereen** Informatiebeveiliging is een verantwoordelijkheid van iedereen
Kern	De verantwoordelijkheid voor informatiebeveiliging en privacybescherming ligt bij iedereen en het management stuurt hierop.
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.

12 Een BIA wordt in het kader van het Business Continuity Management (BCM) gebruikt om de kritieke processen van de niet-kritieke processen te scheiden [Wikipedia].

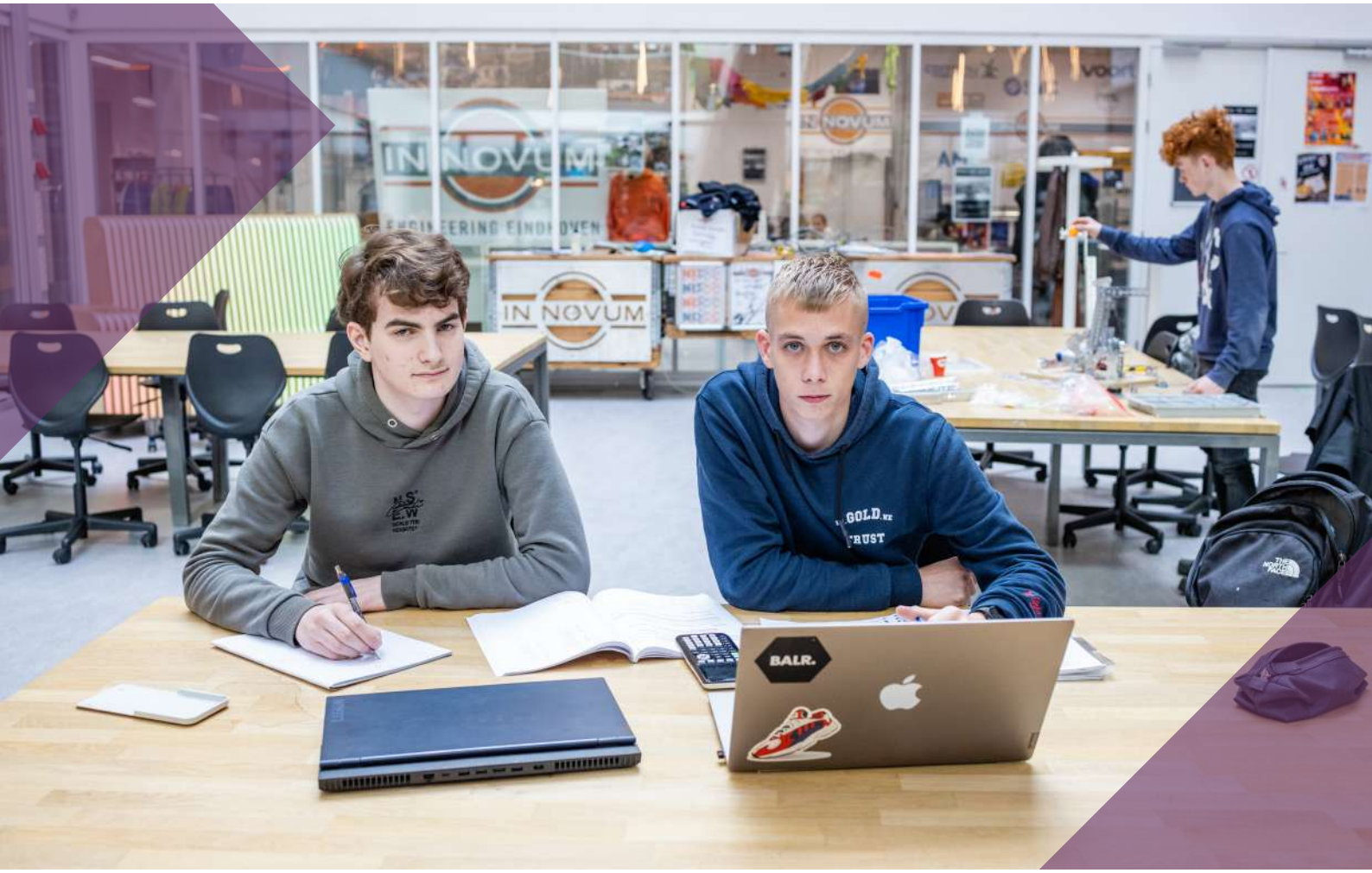
Implicaties	• Directie en management stuurt op informatiebeveiliging en privacybescherming en zorgt voor de juiste 'tone-at-the-top'. • Directie en management zorgt dat de medewerkers de kans krijgen verantwoordelijkheid te nemen voor informatiebeveiliging en privacybescherming. • Voor alle gebruikers van digitale informatievoorzieningen van Fontys is een zogenaamde Gedragscodes ICT beschikbaar die is gepubliceerd via de website van Fontys. Er is een aparte gedragscode voor studenten en voor medewerkers. • 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 het ISP-Office of via het online meldformulier Responsible Disclosure • Schending van wetgeving, voorschriften en regels op gebied van informatiebeveiliging kan leiden tot sanctionerende maatregelen, door of namens het CvB, zoals vastgelegd in de gedragscodes.

> 4	**Altijd** Informatiebeveiliging is een continu proces
Kern	Informatiebeveiliging en privacybescherming zijn cyclische processen die verankerd zijn in exploratie, verandering, exploitatie en beëindiging.
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, zie 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 Fontys rond toegang en gebruik van IT-middelen. • Periodiek worden accounts met hoge privileges gevalideerd. • Zowel centraal als decentraal organiseert Fontys regelmatig cybersecurity-awareness activiteiten voor de diverse doelgroepen: studenten, medewerkers, leidinggevenden en partners van Fontys. • Bij aanpassingen in rollen, taken, en verantwoordelijkheden van een persoon worden ook de autorisaties daarmee in overeenstemming gebracht en aangepast. • De Fontys strategiekaart en het cyberdreigingsbeeld van SURF zijn leidend voor het dreigingsbeeld voor Fontys. Beiden worden periodiek bijgesteld. Nieuwe dreigingen leiden waar nodig tot aanpassing van maatregelen.

> 5	**Security by Design** Integrale aanpak informatiebeveiliging
Kern	Fontys verankert informatiebeveiliging en privacybescherming in processen en management in denken en doen.
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) herstel¬werkzaamheden 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 gegevens¬beschermings¬¬effectbeoordeling (DPIA) in het kader van de AVG. • Bij procesontwerp worden maatregelen meegenomen die de continuïteit van het proces afdoende kunnen waarborgen.

> 6	**Security by Default** Standaard beperkte toegang en veilige instellingen
Kern	Toegang tot informatie is afgeschermd en wordt alleen specifiek voor gebruikers opengezet op basis van het 'need to know'-principe (Gesloten waar nodig en open waar mogelijk).
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 autorisatie¬schema) • 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.

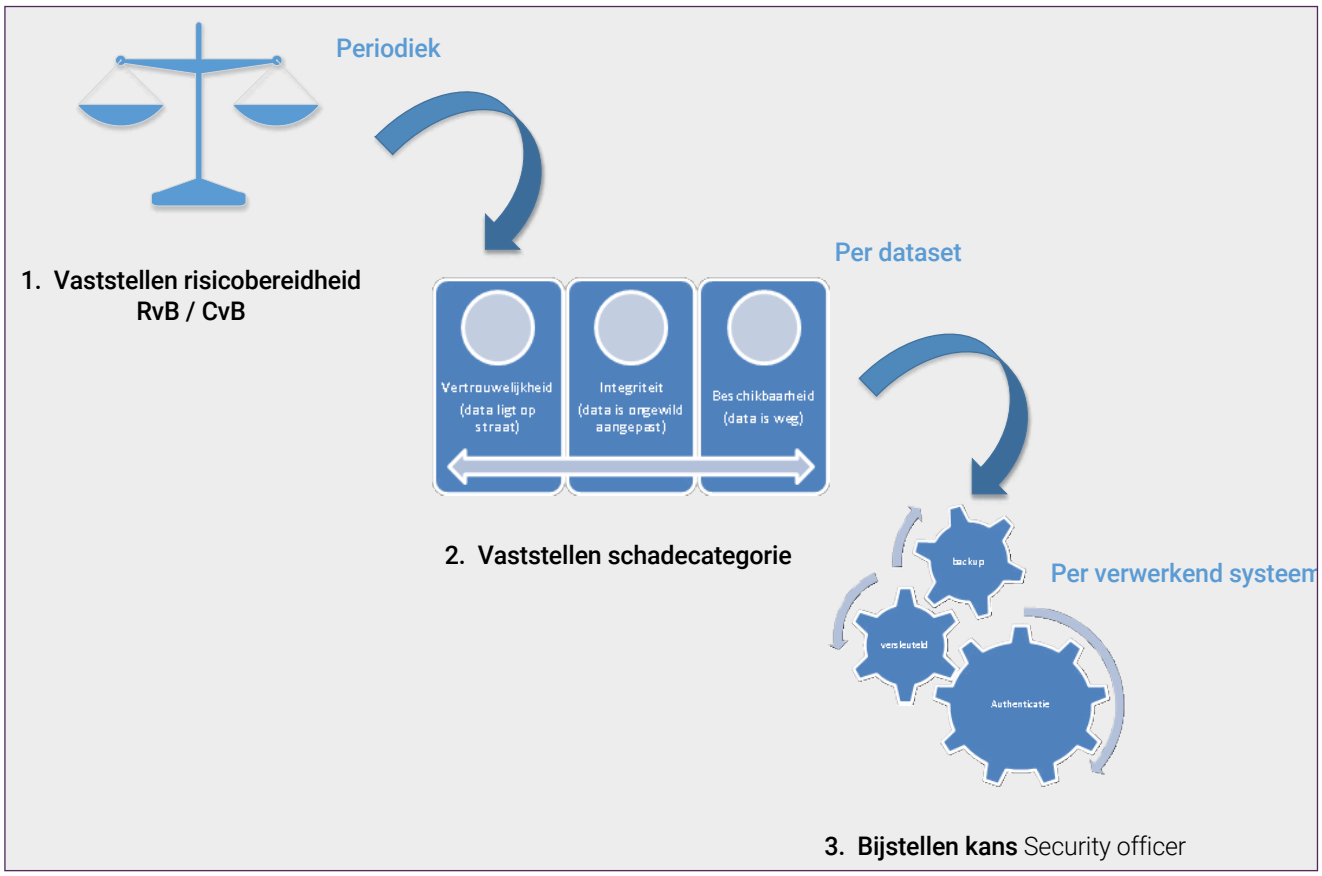
> 7	**Samenwerken** Binnen de sector als sector overstijgend samenwerken
Kern	Vanuit het perspectief van macrodoelmatigheid kijkt en volgt Fontys wat sector overstijgend samen en sectorspecifiek aanvullend gedaan kan worden.
Achtergrond	Structureel samenwerken met partijen buiten en binnen het hoger onderwijsstelsel en kennis delen met als doel elkaar bewust en scherp te houden op het gebied van cyberveiligheid.
Implicaties	• Goed sturen op stelselniveau (digitale veiligheid stevig op de bestuursagenda). • Elkaar bewust en scherp houden op het gebied van cyberveiligheid. • Structureel samenwerken en kennis actualiseren. • Informatie delen en gezamenlijk actief blijven leren en vernieuwen. • Partnership met een strategisch securitypartner. • Intensief samenwerken in SURF verband. • Samenwerken met SURF SCIPR (strategisch/tactisch). • Samenwerken met SURF SCIRT (operationeel). • Samenwerken met SURFcert (incident response). • Samenwerken in HBO-CISO en HBO-FG verband. • Samenwerken met partnerinstellingen in de regio (TUe, Avans, Zuyd HS). • Een normen- en toetsingskader informatiebeveiliging voor het hoger onderwijs. • Een model IB-beleid en een model privacy-beleid. • Gezamenlijk inkopen van informatiebeveiligingsdiensten, e.g. de SURFsoc dienstverlening. • Samenwerken binnen de IT-Circle (sector overstijgend).



BIJLAGE C - CLASSIFICATIE

Classificatie geeft een inschatting van de gevoeligheid en het belang van informatie om tot een juiste mate van beveiliging te komen. Niet alle informatie is even vertrouwelijk of hoeft bij een incident even snel weer beschikbaar te zijn. Het is niet erg efficiënt of gebruiksvriendelijk om niet-vertrouwelijke informatie op dezelfde manier te beschermen als vertrouwelijke informatie.
Fontys volgt een risico gestuurde aanpak. De risicobereidheid van Fontys voor wat betreft wet- en regelgeving (AVG respectievelijk SURF normenkader informatiebeveiliging hoger onderwijs) is avers. Voor alle data die verwerkt wordt, wordt het risico bepaald door impact die een incident kan hebben en de kans dat een incident zich voordoet. De impact wordt bepaald door de schade die een bepaalde dataset kan veroorzaken, door bijvoorbeeld de data te verliezen. De schade wordt vastgesteld door de data-eigenaar die de data in een bepaalde categorie indeelt.
De risicobereidheid en de schade zijn een gegeven. De kans wordt bepaald door de maatregelen die genomen zijn om de data te beschermen. Aanvullende maatregelen verkleinen de kans of reduceren de impact. De security & privacy officer adviseert welke maatregelen geïmplementeerd moeten zijn zodat het restrisico naar een acceptabel niveau kan worden gebracht.

Procesweergave



1. 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. Het gebruik van standaard risicoanalysehulpmiddelen is vaak een tijdrovend en abstract traject.
Niet alle risico' s hoeven gemitigeerd te worden. Fontys 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 Fontys is in onderstaand schema weergegeven.

Tabel 1: Risicobereidheid

Risico		**Schade**			
		Verwaarloosbaar	Enig	Ernstig	Ontwrichtend
Kans	Minimaal	Acceptabel	Acceptabel	Bespreekbaar	Niet acceptabel
	Klein	Acceptabel	Bespreekbaar	Bespreekbaar	Niet acceptabel
	Reëel	Bespreekbaar	Bespreekbaar	Niet acceptabel	Niet acceptabel
	Hoog	Bespreekbaar	Niet acceptabel	Niet acceptabel	Niet acceptabel

Schade 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 veiligheid terugdringen tot een voor de organisatie acceptabel niveau. De schade categorieën bij Fontys zijn als volgt bepaald:

Tabel 2: Indicatie schade categorieën

Indicatie schade categoriën				
Impact	**Imago**	**Onderwijs**	**Onderzoek**	**Financieel**
Verwaarloosbaar	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 €250.000
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.	Publicatie-beperkingen, reputatieschade aan onderzoeker of instelling, patenten of contractuele afspraken	Directe schade tussen €250.000 en €1.500.000
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 €1.500.000

2. Bepalen schade / waarde

De eigenaar van de data heeft de eindverantwoordelijkheid voor de uitvoering van het inschatten van de waarde/ schade en het selecteren van een gepast systeem om de data te verwerken. Schade kan worden veroorzaakt door de data kwijt te raken, maar ook door dat de data onbetrouwbaar is geworden of boetes vanwege onzorgvuldige omgang. De waarde van de data is het financiële gewin voor een derde als ongeautoriseerde toegang tot de data kan krijgen. De eigenaar bepaalt de schade categorie op basis van de maximale schade/waarde van de data. De waarde van een aantal datatypen is al vastgesteld voor de hele organisatie (tabel 2).

De eigenaar houdt bij het bepalen rekening met drie hoofdscenario's:

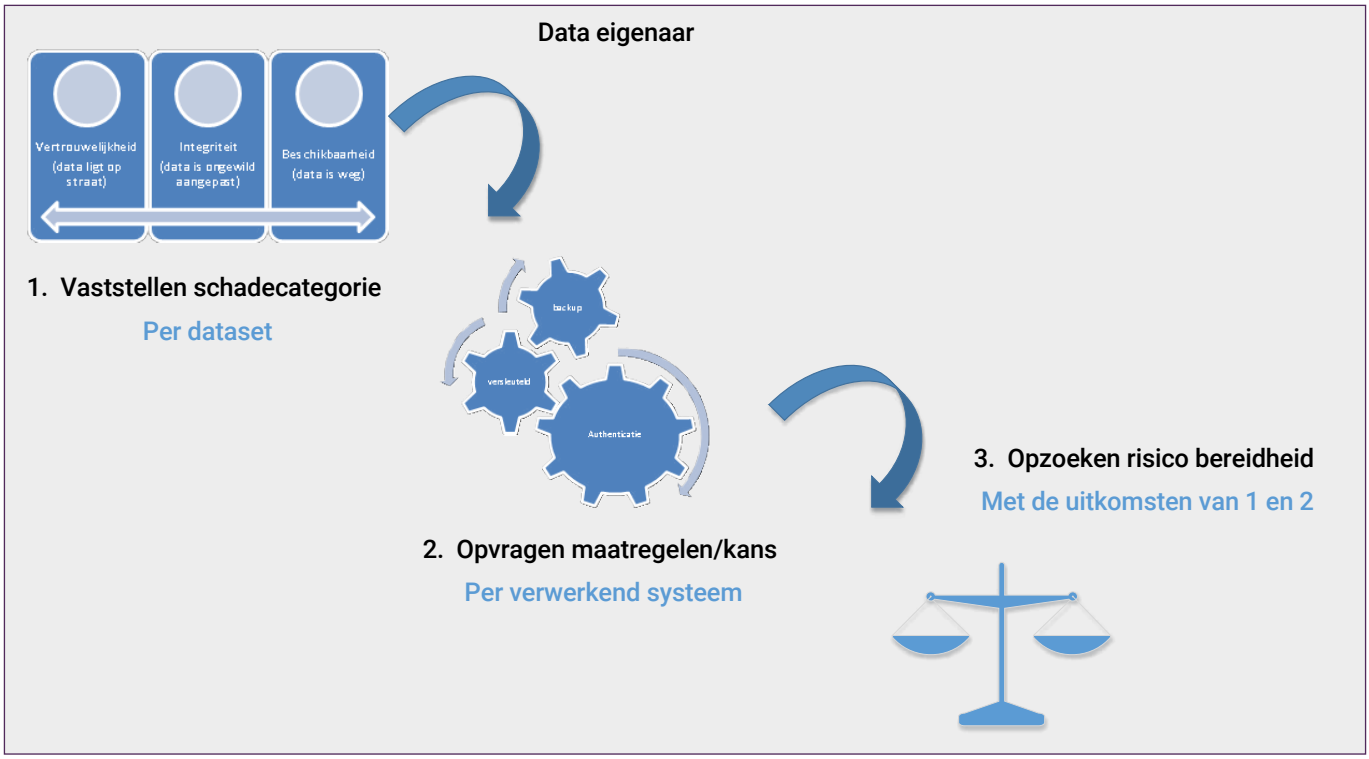
- **Beschikbaarheid**: De data is weg door een fout, storing of kwaadwillende.
- **Integriteit**: We kunnen niet meer garanderen dat de data niet is aangepast.
- **Vertrouwelijkheid**: De data is in handen van derden en deze kunnen er mee doen wat ze willen.

Onderstaande tabel geeft een handvat voor het inschatten van de schade:

Tabel 3: Inschatten van de schade

Categorie	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 1 dag 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 1 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.

Proces gezien vanuit de data-eigenaar



1. De data-eigenaar selecteert met behulp van de gegevens in tabel 2, 3 en 4 de categorie waarin zijn data valt.
2. De data-eigenaar vraagt bij de security & privacy officer op wat de vastgestelde kans op BIV-schade (tabel 4) van een bepaald systeem is.
3. De data-eigenaar controleert of de data door het systeem verwerkt kan worden door de risicobereidheid in tabel 1 te raadplegen. Zo niet, dan gaat de data-eigenaar op zoek naar een ander systeem of overlegt met de systeemeigenaar en de security & privacy officer of er extra maatregelen getroffen kunnen worden om de kans op misbruik verder terug te dringen. In het geval dat de dataset in de hoogste waarde/schade categorie valt neemt de data-eigenaar altijd contact op met de security & privacy officer voor een maatwerk risico analyse.

3. Bepalen maatregelen / kansen

De ISP-contactpersoon al dan niet met ondersteuning van de security & privacy officer toetst aan welke eisen de digitale omgeving voldoet.
SURF heeft twee standaard sets aan maatregelen beschreven om risico's voor een bepaald systeem te beperken:

- **STITCH**[13], dit is een set met een beperkt aantal technische eisen die eisen eenvoudig te meten zijn. Implementatie van deze maatregelen geeft een systeem een basis weerbaarheid.
- **Normenkader**[14]. Bijlage C van het SURF juridisch normenkader (cloud)diensten bevat de Handreiking Beveiligingsmaatregelen. Deze handreiking bevat voornamelijk maatregelen uit ISO 27002 die zowel gaan over de governance van bij de leverancier van de dienst, als technische eisen die gesteld worden aan het systeem dat de dienst levert. Implementatie van de maatregelen voor 'laag' en 'midden' of compenserende maatregelen die hetzelfde doel halen geeft een systeem een goede weerbaarheid.

13 De Security Technical IT Checklist: **https://www.surf.nl/files/2019-04/SCIRT-STITCH1.0_1.pdf**

14 SURF juridisch normenkader (cloud)diensten: **https://www.surf.nl/files/2019-01/surf_c-handreiking-beveiligingsmaatregelen---bijlage-c---versie-mei-2018.pdf**

Een risicoanalyse geeft het meest realistische beeld van het risico dat een bepaald systeem loopt. Dit is echter vrij arbeidsintensief en niet realistisch om voor alle systemen uit te voeren. We koppelen daarom in het algemeen de kans aan een set van maatregelen, waarbij een risicoanalyse alleen wordt uitgevoerd (en alle voortvloeiende maatregelen geïmplementeerd) als de kans minimaal moet zijn:

Tabel 5 maatregelen -> kans tabel

Maatregel geïmplementeerd	Kans
Geen/onbekend	Hoog
Stitch	Reëel
Stitch+ normenkader	Beperkt
Risicoanalyse	Minimaal

Proces gezien vanuit security & privacy officer en systeemeigenaar

1. De maatregelen die zijn genomen voor de informatiebeveiliging van een bepaald systeem worden aangeleverd of uitgevraagd.
2. De security & privacy officer toetst of het systeem voldoet aan (een van) de twee sets aan maatregelen.
3. Op basis van de uitkomst van 2 koppelt de security & privacy officer de kans op misbruik aan het systeem, overeenkomstig tabel 5 hierboven. Deze uitkomst kan intern in de organisatie gepubliceerd worden zodat een volgende data-eigenaar de geconstateerde kans op kan zoeken.
4. Indien een systeem niet voldoet komt de security & privacy officer met een advies voor de maatregelen die genomen moeten worden om het systeem naar het gewenste niveau te krijgen. Optioneel: als het een dataset is die zeer waardevol is of grote schade kan aanrichten dan zal de eigenaar vragen om een risicoanalyse van de verwerkende systemen.

Risicoanalyse

Voor systemen die data verwerken die ernstige of ontwrichtende schade kunnen toebrengen wordt een maatwerk analyse van het systeem uitgevoerd. Hierbij wordt eerst vastgesteld wat de dreigingen voor een systeem zijn die de vastgestelde schade kunnen veroorzaken. Voorbeelden van dreigingen zijn

- Beschikbaarheidsverlies van gegevens
- Integriteit cijferadministratie aangetast
- Vertrouwelijkheid Intellectueel eigendom aangetast

Per dreiging wordt vervolgens gekeken welke verschijningsvormen deze hebben. Voorbeelden van verschijningsvormen zijn:

- Identiteitsdiefstal
- Misbruik kwetsbaarheden in systemen
- Ransomware
- IT verstoring

Per verschijningsvorm wordt gekeken welke mitigerende maatregelen er geïmplementeerd kunnen worden die de dreiging of de gevolg schade kunnen inperken. Voorbeelden zijn:

- Multi factor authenticatie
- Pentest, monitoring
- Backup

Als alle noodzakelijke maatregelen zijn geïmplementeerd, dan krijgt het systeem de kans ‘minimaal’ toegewezen.

BIJLAGE D - WET- EN REGELGEVING

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

1. Wet op het Hoger onderwijs en Wetenschappelijk onderzoek (WHW)

Fontys 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) en UAVG

Fontys heeft een separaat privacybeleid vastgesteld waarin naleving van de AVG en de Uitvoeringswet AVG (UAVG) wordt geborgd. Naleving van het informatiebeveiligings en privacybeleid inclusief de daarin vermelde technische en organisatorische maatregelen zorgen samen voor het voldoen aan de AVG.

3. Wettelijke Bewaartermijnen/Archiefwet

Fontys 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. Fontys hanteert daarbij het Basisselectiedocument[15] van de sector hogescholen. 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

Fontys respecteert auteursrechten en handelt daarnaar.

5. Telecommunicatiewet

Omdat de doelgroep van Fontys voldoende afgebakend is worden de netwerkvoorzieningen van Fontys niet aangemerkt als een openbaar netwerk in de zin van de Telecommunicatiewet.

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

15 Referentie VH-document: Selectielijst hogescholen 2013, actualisatie 2019 Versie 1.1, april 2019

7. Overige codes en landelijke afspraken

Het informatiebeveiligingsbeleid bij Fontys is gebaseerd op het SURF Normenkader en de instelling is deelnemer in de VH[16]. Fontys is in dit kader gehouden aan de volgende codes en landelijke afspraken:

- Code goed bestuur universiteiten.
- Nederlandse gedragscode wetenschappelijke integriteit.
- SURF Normen- en toetsingskader Informatiebeveiliging Hoger Onderwijs.
- Basisselectie document Hoger Onderwijs.

16 Vereniging van Hogescholen

BIJLAGE E - ROLLEN DE IB-GOVERNANCE

Voor informatierisicomanagement hanteert Fontys het IIA Three lines model risk management. In deze bijlage wordt de invulling van het IIA's Three lines model binnen Fontys geschetst.

IIA Three lines model risk management – Information security & privacy (ISP) risico's

1ste lijn
Instituten en diensten (directeur)
- Verantwoordelijk voor eigen business unit (uitvoeren onderwijs en onderzoek of bedrijfsvoering) en doelen in lijn met de Fontys strategie
- Verantwoordelijk voor de naleving van het IB-beleid en de AVG
- Verantwoordelijk voor eigen risico's op data en processen en (persoons)gegevensbescherming incl. het inrichten ervan
- Geeft zelf invulling aan dienst- of instituut specifieke regelingen in lijn met de ISP-kaders
- Dragen de consequenties als deze risico's zich voordoen
- Managen ISP risico's door
  - Identificeren van risico's
  - Beoordelen van risico's door het uitvoeren van security- en privacy toetsen en DPIA's.
  - Definiëren en implementeren beheersmaatregelen om risico's te mitigeren tot een acceptabel niveau
  - Monitoren of de beheersmaatregelen werken zoals beoogd
- Uitvoeren jaarlijkse risicoanalyse en opstellen van (eigen) ISP-jaarplan
- Screenen nieuwe medewerkers op betrouwbaarheid en integriteit
- Trainen, adviseren en motiveren (nieuw) personeel, docenten en studenten zodat kennis, houding en gedrag m.b.t. ISP en de ICT-gedragscode wordt vergroot en onderhouden.
- Zorgen voor zicht en grip op data, processen, systemen en autorisaties (business security) en het onderhouden ervan (o.a. voorkomen legacy, naleven bewaartermijnen en leveranciersmanagement)
- Classificeren van data en informatiesystemen
- Zorgen voor afdoende beveiliging van digitale en fysieke toegang tot vertrouwelijke informatie en ruimten
- Opstellen en onderhouden van bedrijfscontinuïteitsplan
- Opstellen en onderhouden van registers van verwerkingsactiviteiten en (laten) afsluiten van verwerkersovereenkomsten
- Onderzoeken en analyseren van datalekken en security-incidenten
- Afhandelen van rechten van betrokkenen onder coördinatie van ISP-Office
- Bewaken voortgang door invullen ISP KPI-dashboard en verantwoorden via ISP-paragraaf in MARAP

2de lijn
ISP Office
- Verantwoordelijk voor Informatiebeveiligings- & privacy beleid en standaard ISP taal
- Opstellen van ISP kaders, richtlijnen en werkwijzen (templates)
- Fontysbreed organiseren van ISP
- Kritische blik bij risico gerelateerde zaken
- Expertise in informatiebeveiliging en privacy
- Opleiden, adviseren, faciliteren en controleren de eerste lijn
- Adviseren van de 1e lijn over privacy en security by design & by default.
- Communicatie (e.g. portal, nieuwsbrief, Bron) en voorlichting (e.g. presentaties, seminars, workshops)
- Gevraagd en ongevraagd adviseren en onderzoeken
- Controleren en registreren op naleving ISP-compliance conform AVG en SURF-Toetsingskader-IB
- Controleren van de Dienst-IT op de werking van technische maatregelen (e.g. pentesten)
- Jaarlijks Surfaudit benchmark (self-assessment), oneven jaren op information security en even jaren op privacy
- Organiseren van cybercrisisoefeningen
- Coördineren en adviseren van de 1ste lijn bij informatiebeveiligingsincidenten, datalekken en rechten van betrokkenen
- Samenwerken met Integrale Veiligheid (Dienst-HF) en strategisch ISP-partner (Northwave)
- Onafhankelijk verzorgen van integrale ISP MARAP aan directeuren, CvB en RvT

3de lijn
Functionaris Gegevensbescherming
- Onafhankelijk toezicht op de toepassing en naleving van de AVG en het privacy beleid
- Informeert en stimuleert de organisatie om zich bewust te worden van privacy risico's
- Adviseert (gevraagd en ongevraagd) over verplichtingen die uit de AVG voortvloeien
- De FG doet namens het CvB de datalek meldingen aan de AP
- De FG is het aanspreekpunt bij klachten hoe Fontys persoonsgegevens behandelt
- De FG werkt samen en is hét contactpunt van de Autoriteit Persoonsgegevens (AP)
- Rapporteren bevindingen en aanbevelingen aan CvB en RvT
- Opstellen FG-jaarplan

Audit
- Jaarlijks opstellen van een auditjaarplan i.o.m. belangrijkste stakeholders (o.a. cvb, CISO en FG) en zoals beschreven is in het auditcharter.
- Uitvoeren van audits conform planning. Audits op informatievoorziening, informatiebeveiliging en privacy vlak kunnen onderdeel uitmaken van de planning.
- Rapporteren van bevindingen op informatievoorziening, informatiebeveiliging en privacy vlak die als 'bijvangst' bij audits met een ander onderwerp (niet ISP) geconstateerd worden.
- Audit bevindingen en aanbevelingen aan cvb en rvt rapporteren.

Externe audit
- Tweejaarlijks externe security audit (VH)

De verantwoordelijkheden en taken aangaande informatie risicomanagement staan in onderstaande tabel vermeld.
Zie tabel in het document "Three lines model Fontys v1.0
Hieronder worden de rollen gericht op informatiebeveiliging en privacy binnen Fontys nader omschreven.

Raad van Toezicht (RvT)

De Raad van Toezicht ziet erop toe dat het College van Bestuur (CvB) adequaat bestuurt. De taken, bevoegdheden en profielkenmerken van de RvT zijn vastgelegd in de statuten en het Bestuurs- en Beheersreglement. Het Toetsingskader, dat opgesteld is volgens de Branchecode goed bestuur hogescholen, draagt bij aan een systematische invulling van de toezichthoudende rol. De RvT is zo samengesteld dat de leden ten opzichte van elkaar, het CvB en welk deelbelang dan ook, onafhankelijk en kritisch kunnen opereren. De RvT bestaat uit zeven personen en wordt ondersteund door de secretaris van het CvB.

College van Bestuur (CvB)

Het CvB is eindverantwoordelijk voor de informatiebeveiliging binnen Fontys en stelt het beleid en de governance op het gebied van informatieveiligheid vast. Informatieveiligheid komt zo vaak als nodig en minimaal 3 per jaar (één keer per trimester) op de agenda van het CvB. Het CvB wijst één van haar leden aan als portefeuillehouder Integrale Veiligheid, waar informatiebeveiliging en privacy deel van uitmaakt.
De inhoudelijke verantwoordelijkheid voor zover het de digitale en fysieke informatiebeveiliging betreft is door de portefeuillehouder belegd bij de CISO. Deze heeft de opdracht om op de digitale informatiebeveiliging van heel Fontys toe te zien.

Interne (IT-)auditor

De interne auditor is onderdeel van de afdeling Audit CvB en controleert jaarlijks het goed en betrouwbaar functioneren van de informatievoorziening, informatiebeveiliging en privacy. Dit door onafhankelijk en objectief te toetsen. De interne auditor controleert het samenspel tussen de 1ste en 2de lijn op effectiviteit en efficiency. Tot de taken behoren onder andere het opstellen van auditplanning en het rapporteren van bevindingen en aanbevelingen aan het CvB, Auditcommissie RvT, de CIO en CISO.

Corporate Information Security Officer (CISO)

De CISO is een functie op strategisch en tactisch niveau. De CISO is de leidinggevende van het Information Security & Privacy Office (ISP-office). De CISO werkt nauw samen met de CIO, de Enterprise architect, de FG en de portefeuillehouder in het CvB. De CISO adviseert en rapporteert *onafhankelijk* en direct aan het voltallig CvB. De CISO stelt het IB-beleid op, helpt bij een juiste vertaling daarvan naar instituten en diensten, ziet toe op de (uniforme) naleving ervan en rapporteert over lacunes, inconsistenties en onvolkomenheden. De CISO kan zowel gevraagd als ongevraagd advies geven. De rol van CISO is belegd bij één persoon, echter de CISO wordt binnen het ISP-office ondersteund door de Information Security & Privacy Officers. Daarnaast werkt de CISO nauw samen met de eerste lijn, zijnde de Manager ICT (cybersecurity) en de ISP-contactpersonen bij instituten en diensten (business security). De contactpersonen in de eerste lijn implementeren het beleid binnen het eigen instituut of dienst.
De CISO heeft verschillende bevoegdheden en zijn eigen budget. Zo kan de CISO gevraagd en ongevraagd onderzoek (laten) doen, denk aan audits en pentests en informatie opvragen en deze in principe ook krijgen.

Functionaris Gegevensbescherming (FG)

De FG houdt binnen Fontys toezicht op de toepassing en naleving van de AVG, zoals beschreven in het privacybeleid van de Fontys Hogescholen. De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie binnen Fontys.
De FG kan zowel gevraagd als ongevraagd advies geven. De rol van FG is belegd bij één persoon, echter de FG wordt binnen het ISP-office ondersteund door de Information Security & Privacy Officers.

Risk & Compliance Officer ISP (RCO-ISP)

De RCO-ISP is een rol op tactisch niveau. De RCO ISP is werkzaam binnen het ISP-Office en rapporteert rechtstreeks aan de CISO (IB) en de FG (Privacy). Compliance resultaten worden door de CISO gerapporteerd aan het CvB. De RCO-ISP controleert en registreert de naleving van governance-aspecten, AVG en het SURF normen- en toetsingskader informatiebeveiliging hoger onderwijs.

Security & Privacy Officer (S&PO)

De Security & Privacy Officer (S&PO) houdt zich binnen Fontys bezig met de toepassing en naleving van het informatiebeveiligingsbeleid en de AVG. Zij zijn werkzaam binnen het ISP-Office. Zij stellen de kaders en de werkwijzen (privacytoets, DPIA, risicoanalyse, dataclassificatie, e.d.) op en adviseren en faciliteren de eerste lijn. Ook zorgen zij dat medewerkers en in het bijzonder ISP-contactpersonen zijn opgeleid in informatiebeveiliging en privacy. Het ISP-Office werkt ook operationeel voor wat betreft het afhandelen van datalekken en uitoefenen van rechten van betrokkenen.

ISP-contactpersonen

Ieder instituut en dienst is verplicht een ISP-contactpersoon te hebben. Veelal is deze rol belegd bij de (decentrale) informatiemanager. Zoals eerder aangegeven is het lijnmanagement van instituten en diensten operationeel

verantwoordelijkheid voor informatiebeveiliging en privacybescherming.
Voor de ISP-contactpersoon betekent dit om binnen de afgesproken kaders sturing te geven aan het gebruik en de ontwikkeling van de informatiebeveiliging en privacybescherming in onderwijs, onderzoek en bedrijfsvoering voor het eigen instituut of dienst. De rapportagelijn van ISP-contactpersonen over de Informatiebeveiliging en privacybescherming is zowel naar de directeur van het instituut/dienst als ook naar het ISP-Office (tweede lijn).

ISO Dienst-IT

De ISO (Information Security Officer) Dienst-IT geeft tactisch en operationeel advies over de benodigde technische securitymaatregelen, zodat Fontys onder andere weerbaar is tegen cyberaanvallen.
De ISO Dienst-IT is tevens voorzitter van het Fontys CERT (zie bijlage H). In die rol, ook wel CERT- of CSIRT-coördinator genoemd.

Medewerkers

Informatieveiligheid begint bij het individu. Dit houdt in dat medewerkers verantwoordelijk zijn voor hun eigen informatiebeveiliging en privacybescherming. Medewerkers dienen de door Fontys voorgeschreven beveiligingsmiddelen en informatiebeveiligingsmaatregelen te gebruiken en de ICT-gedragscode na te leven. Zij zijn zich bewust van relevante wet- en regelgeving en signaleren tijdig (potentiële) beveiligingsincidenten en datalekken.

Lijnmanagement (directeuren en managers)

Informatiebeveiliging en privacy is in de eerste plaats de verantwoordelijkheid van de lijnmanager (leidinggevende). De lijnmanager zit in de eerste lijn binnen het Three lines model van risicomanagement. De lijnmanager maakt de afwegingen in hoeverre risico's acceptabel zijn. De lijnmanager kent het te beveiligen werkproces en de te beschermen informatie uiteindelijk het best.
Naleving van het IB-beleid is onderdeel van het integrale bedrijfsproces. In die zin is het beschermen van data niet anders dan andere risico's voor de bedrijfsvoering waar de lijnmanager ook verantwoordelijk voor is. Iedere lijnmanager heeft de taak om:

- Ervoor te zorgen dat hun medewerkers en studenten op de hoogte zijn van (de voor hen relevante aspecten van) het beveiligingsbeleid en de ICT-gedragscode;
- 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.

De directeuren van instituten en diensten plannen en rapporteren via de MACON respectievelijk MARAP over de risico's en maatregelen met betrekking tot informatiebeveiligings- en privacy onderwerpen. Dit in lijn met de Fontys MARAP cyclus (PDCA-cyclus).

Specifieke rollen in de lijn

CIO
De chief information officer (CIO) is ook binnen Fontys de hoogste verantwoordelijke op het gebied van de Informatie Voorziening. De CIO rapporteert aan de portefeuillehouder IV binnen het CvB. De CIO is binnen Fontys tevens de directeur van de Dienst-IT.

Manager ICT
De Manager ICT zorgt samen met zijn teamleiders voor de vertaling van informatiebeveiliging op tactisch niveau naar operationele plannen en technische maatregelen. Dit doet de Manager ICT in goed overleg met de CISO en met de systeem- en proceseigenaren. Onder zijn verantwoordelijke adviseren zijn specialisten (waaronder de ISO Dienst-IT) over specifieke technische informatiebeveiligingsmaatregelen, bijvoorbeeld in projecten, bij acquisities van software of hardware, etc. De manager ICT heeft Directeur IT als hiërarchisch leidinggevende.

Proceseigenaar
De proceseigenaar is verantwoordelijk voor het goed functioneren van de primaire of ondersteunende processen, al dan niet gebruikmakend van één of meerdere informatiesystemen. Daarbij is de proceseigenaar verantwoordelijk voor de inbedding en toepassing van IB-maatregelen in het proces.

Dataeigenaar
De dataeigenaar zorgt ervoor dat studenten, medewerkers en relaties op het juiste moment over de juiste gegevens van voldoende kwaliteit kunnen beschikken. De datamanager heeft een rol in het zorgdragen voor consistentie en integriteit van data.

Systeemeigenaar
Een systeemeigenaar is verantwoordelijk voor het juist functioneren van het informatiesysteem, waarmee een of meerdere processen worden ondersteund. Uit bovenstaande definities volgt dat de systeemeigenaar, de data- en proceseigenaar als klant heeft. De data- en de proceseigenaar bepalen hoe de gegevens en de processen eruitzien. Vervolgens dient de systeemeigenaar het informatiesysteem hierop in te richten.

Projectleider
De projectleider draagt zorg dat in de beginfase, gedurende en tijdens de afronding van een project, gericht op de vernieuwing of het onderhoud van de Fontys informatievoorziening (IV), dat informatiebeveiliging en privacy is geborgd door middel van 'security & privacy by design'.

BIJLAGE F - DOCUMENTEN INFORMATIEBEVEILIGING

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

In het kader van informatiebeveiliging hanteert Fontys de volgende documenten:

1. Het Informatiebeveiligings-beleid (IB-beleid)

Het IB-beleid ligt ten grondslag aan de aanpak van de (digitale) informatiebeveiliging binnen Fontys. Het IB-beleid worden de randvoorwaarden en uitgangspunten vastgelegd en wordt richting gegeven aan de vertaling van het beleid in concrete maatregelen. Om ervoor te zorgen dat het beleid gedragen wordt binnen de instellingen & diensten en er ook naar handelt wordt het uitgedragen door (of namens) het CvB. Het beleid wordt, onder verantwoordelijkheid van de CISO opgesteld en vastgesteld door het CvB.

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

Voor het ISMS wordt verwezen naar bijlage A.

3. Classificatie Richtlijn

Voor het classificeren wordt verwezen naar bijlage C.

4. Jaarplan/verslag

De CISO rapporteert de voortgang ieder trimester, in lijn met de MACON/MARAP-cyclus, aan het CvB. De CISO stelt elk jaar een jaarplan op, dat wordt voorgesteld aan en goedgekeurd door het CvB. Het jaarplan wordt gebaseerd op de resultaten van de periodieke controles (pentest), de stand van zaken t.o.v. het SURF normenkader IBHO, risicoanalyses, interne- en externe audits. Naast de voortgang van het jaarplan staat in de rapportage in hoeverre Fontys voldoet aan het SURF volwassenheidsmodel IBHO en wordt ingegaan op security incidenten die zich hebben voorgedaan en wat Fontys hiervan leert. In dezelfde lijn wordt ook de voortgang m.b.t. privacy meegenomen in de rapportage. Voor meer informatie over het FG-jaarplan en de voortgangsrapportages wordt verwezen naar het Privacy beleid.

5. Baseline van informatiebeveiliging maatregelen

De Baseline van informatiebeveiliging maatregelen voor het hoger onderwijs is het SURF normen- en toetsingskader informatiebeveiliging hoger onderwijs (IBHO). Met gezamenlijke inspanning onder leiding van SURF is er één baseline voor het hoger onderwijs. Sinds kort is ook het MBO hierbij aangesloten. Het gebruik van één normen- en toetsingskader voor het gehele middelbaar en hoger onderwijs biedt een aantal voordelen:

- Het versterken van de informatieveiligheid door betere afstemming binnen ketens van onderwijs en andere partijen;
- Administratieve lastenverlichting bij zowel afnemers als leveranciers, door uniforme beveiligingsnormen bij het onderwijs;
- Aansluiting bij internationale regelgeving en standaarden;
- Vermindering van onderhoudskosten.

De meest recente versie van het Normenkader is in 2015 gepubliceerd. Het toetsingskader is gebaseerd op de Handreiking bij Volwassenheidsmodel Informatiebeveiliging van de Nederlandse Beroepsorganisatie voor Accountants (NBA). De meest actuele versie van het toetsingskader dateert uit 2019.

De VH is voornemens om tweejaarlijks een externe audit te verplichten voor iedere HBO-instelling op basis van het toetsingskader. Hierbij wordt net als bij ISO 27001 en ISO 27002 het principe van 'pas toe of leg uit' gehanteerd. SURFaudit draagt zorg voor het onderhoud op het normen- en toetsingskader en stelt dit om de paar jaar bij. Begin 2022 staat de introductie van de nieuwe versie van de ISO 27002 gepland. Vanuit SURFaudit wordt onderzoek uitgevoerd naar de impact van deze nieuwe versie op het huidig normenkader. Zodra de nieuwe ISO-versie door de NEN-organisatie wordt gepubliceerd, zal de aanpassing van het normenkader worden opgepakt.

6. Policies

- Privacy beleid
- Gedragscode ICT voor het veilig gebruik van IT-voorzieningen, e-mail en internetgebruik door medewerkers, studenten en derden, inclusief clear desk and clear screen beleid.
- Beleid over informatieveilig software ontwikkelen: Security Baseline Microsoft Azure t.b.v. Business Intelligence (BI) en Data Integratie (DI)
- Beleid over Fontys generieke toepassingen: Security Baseline Microsoft 365, veilig internetten (eduVPN) en voldoen aan veilige e-mail coalitie
- Sourcing beleid
- Backup beleid
- Patch beleid
- IT lifecycle management beleid
- Identity & Access Management beleid (inclusief wachtwoordbeleid en MFA)
- Logging en monitoring beleid (SURFsoc)
- Beleid van cryptografische hulpmiddelen
- Beleid over informatie-uitwisseling
- Beleid voor mobiele apparaten
- Bewaartermijnen
- Checklist veilige tooling
- Richtlijn responsible disclosure

Daarnaast is informatiebeveiliging een vast onderdeel van de volgende documenten:

7. Dienstenovereenkomsten (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 met de leverancier vastgelegd. Het contract bevat standaard een informatie¬beveiligingsparagraaf waarin de verantwoordelijkheden van de leverancier zijn opgenomen. De basis hiervoor is het SURF Juridisch Normenkader Cloudservices Hoger Onderwijs[17] die een informatiebeveiliging bijlage bevat. De leverancier neemt zijn verantwoordelijkheid als deze gecertificeerd is op ISO 27001, ISO27017 of ISAE 3000.

8. Business Continuity Plan

Het Business Continuity Plan en het Centraal Crisis Team valt onder de verantwoordelijkheid van Integrale Veiligheid, onderdeel van de Dienst H&F.

17 https://www.surf.nl/surf-juridisch-normenkader-cloudservices

BIJLAGE G - FONTYS CERT

Het Fontys CERT (Computer Emergency Response Team), ook wel aangeduid met CSIRT (Computer Security Incident Response Team), heeft als doel bij een beveiligingsincident schade te reduceren en snel herstel van de dienstverlening te bevorderen. Naast reactie op incidenten richt het Fontys CERT zich ook op preventie en preparatie. Het Fontys CERT binnen de Dienst-IT bestaat uit een gespecialiseerd team van ICT-professionals, dat in staat is snel te handelen in het geval van een beveiligingsincident met computers of netwerken.

De leden van het Fontys CERT zijn in die rol benoemd door de Manager ICT in overleg met de CISO. Fontys CERT-leden zijn aangesloten bij de SURF Community van Incident Response Teams (SCIRT). Het Fontys CERT is zowel operationeel verantwoordelijk voor incident response als het binnen acceptabele termijn oplossen van kwetsbaarheden in de IT-infrastructuur.

Als er door SURFsoc (Security Operations Center) of andere vertrouwde bronnen verontrustende trends worden geconstateerd, dan speelt Fontys hierop in door het nemen van extra maatregelen of het creëren van bewustwording binnen de organisatie. Voor het detecteren van aanvallen maakt Fontys gebruik van de dienstverlening SURFsoc. Het door het SURFsoc gedetecteerde (mogelijke) aanvallen worden opgevolgd door het Fontys CERT. Het Fontys CERT is gerechtigd om tijdelijk computersystemen of netwerksegmenten te laten isoleren om haar taak goed te kunnen uitvoeren. Het Fontys CERT houdt zich ook bezig met beveiligingsincidenten buiten Fontys als daar eigen medewerkers in enige rol bij betrokken zijn. Om incidenten of kwetsbaarheden op de juiste manier te kunnen afhandelen, worden ze in het structureel Fontys CERT overleg besproken en geprioriteerd.

In het geval het bedrijfsproces, financiën of de goede naam van Fontys in gevaar zijn wordt het Fontys CERT bijgestaan door de strategisch securitypartner van Fontys. Hiervoor is een Incident Response Plan (24x7) afgesloten. Ook SURFcert zal Fontys ondersteunen bij ernstige beveiligingsincidenten. SURFcert staat via het NCSC (Nationaal Cyber Security Center) wereldwijd in verbinding met andere CERT's en CSIRT's.

Er is een handboek Fontys CERT, waarin doelgroep, opdracht, bevoegdheden, escalaties, werkwijze en samenstelling zijn uitgewerkt. High impact Indicenten worden binnen de Dienst-IT geëscaleerd richting het Crisisteam Dienst-IT, dat op haar beurt kan escaleren naar het **Centraal Crisis Team (CCT)** op Fontys-niveau.