Model Informatiebeveiligingsbeleid SCIPR

Onderdeel van het SCIPR Framework Informatiebeveiliging

SCIPR-community: werken aan betere informatiebeveiliging

Informatiebeveiligers en Privacy Officers in het hoger onderwijs werken samen in SCIPR (SURF Community voor Informatiebeveiliging en Privacy). We stellen daar met elkaar onder andere beleid en leidraden op om de informatiebeveiliging en privacy van jouw instelling te verbeteren.

Dit document is tot stand gekomen in samenwerking met:

- Helma de Boer, Deltion College
- Ludo Cuijpers, Vista College
- Jan Evers, Universiteit Twente
- Bart van den Heuvel, Universiteit Maastricht
- Remon Klein Tank, Wageningen Universiteit en Research
- Elma Middel, Hanze Hogeschool
- Frans Pingen, Wageningen Universiteit en Research
- Miranda van der Ploeg-Cools, Tilburg University
- Anita Polderdijk, Hogeschool Windesheim
- Raoul Vernède, Universiteit Utrecht

Versie 3.0, maart 2020

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

Gebruikswijzer van dit model

Verwijder deze pagina en de opmerkingen in de kantlijn uit het document.

Deze gebruikswijzer is bedoeld als toelichting op het gebruik van dit model voor het informatiebeveiligingsbeleid (en niet als leeswijzer voor het beleid zelf). Het model helpt slechts als richtlijn voor de CISO om te komen tot een specifiek IB-beleid voor de eigen instelling. Met de zoek- en vervang functie kan bijvoorbeeld wel snel de instellingsnaam worden ingevuld, maar daarmee is het document nog niet geschikt om aan een bestuur voor te leggen.

De opzet van dit model is om alle elementen van informatiebeveiliging te benoemen die de SCIPR-community adviseert op te nemen in het IB-beleid van de instelling, compleet met tekstaanbevelingen.

Uiteraard is de invulling van het IB-beleid per instelling op onderdelen anders. Van invloed kunnen zijn:

- Grootte van de instelling (bijvoorbeeld niet voldoende personen om alle taken en rollen zuiver te scheiden).
- De politieke werkelijkheid binnen een instelling (een organisatieverandering is niet altijd wenselijk, of niet op dit moment. Of er is een specifieke mandatenregeling die bepaalde verantwoordelijkheden anders belegt).
- Volwassenheid van IB in de instelling (het beleid is b.v. te veelomvattend als onderliggende taken, rollen en functies vooralsnog niet zijn ingevuld en niet snel kunnen worden ingevuld).
- Als een instelling meer of minder onderliggende documenten beschikbaar heeft om aan te refereren.
- Vormgevingseisen.

De instelling kan afhankelijk van bovenstaande situaties vervolgens kiezen om:

- Elementen weg te laten
  (als er b.v. geen Business Continuity Manager is, of geen CSIRT).
- Elementen naar een bijlage te verplaatsen of enkel te refereren aan een onderliggend document, of juist in plaats van een bijlage tekst in het hoofddocument op te nemen.
- Elementen verder uit te schrijven als/omdat er geen onderliggende documenten zijn.

Specifiek maken van dit document

Opmerking	In dit document is op een aantal plaatsen met een opmerking een aanwijzing gegeven.
<tekst1/tekst>	Vervang dit door tekst die passend is bij de eigen situatie, bijvoorbeeld <naam onderwijsinstelling> wordt 'Hogeschool X'.

Commented [L.C.1]: Dit is een voorbeeld van een opmerking waarin een aanwijzing wordt gegeven. Verwijder uiteindelijk alle opmerkingen uit het document.

[tekst] Neem deze tekst alleen op als dit in de eigen instelling van toepassing is.

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 <naam instelling> voorziet in adequate informatiebeveiliging en daarmee voldoet aan de relevante wet- en regelgeving.
Met het informatiebeveiligingsbeleid (IB-beleid) wil <naam instelling> ook bijdragen aan een betere kwaliteit van de informatievoorziening en zorgen voor een juiste balans tussen functionaliteit, veiligheid en privacy.

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

Vijf beleidsprincipes zijn leidend, namelijk:

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

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

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

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

1. Inleiding

Het succes van <naam instelling> 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 <naam instelling>-diploma(certificaat), behaalde cijfers of de legitimiteit van onderzoekconclusies ondermijnen. Ook de privacy[2] van studenten, medewerkers en gasten en de reputatie van <naam Instelling> kunnen worden geschaad. Informatiebeveiliging is daarom van cruciaal belang.
[“Protect and Comply” is dan ook een van de drie pijlers in de in 2018 vastgestelde I-Strategie van <naam instelling>.]

Commented [L.C.2]: Dit is een voorbeeld zin mbt aanvullende informatie van een specifieke instelling, in dit geva de UM

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

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

Informatieveiligheid is niet te bereiken door alleen een aantal technische en organisatorische maatregelen vast te stellen. Door de veranderende wereld is het een dynamisch proces. In dit document zijn om die reden vijf hoofdprincipes leidend voor informatiebeveiliging binnen <naam instelling>. De vast te stellen maatregelen, procedures en richtlijnen kunnen getoetst worden aan de vijf hoofdprincipes die in hoofdstuk 4 zijn beschreven.

Er is een belangrijke relatie tussen informatiebeveiligingsrisico's en risico's op andere gebieden, zoals privacy, safety[3] (arbowetgeving), veiligheid in onderwijs en onderzoek, fysieke beveiliging en business-continuïteit. Soms overlappen ze elkaar gedeeltelijk. [Dit beleidsdocument is een onderdeel van het Beleid Integrale Veiligheid van <naam instelling>].

Commented [L.C.3]: Eventueel aanpassen naar eigen situatie

2. Wet- en regelgeving

<naam instelling> streeft ernaar om in al haar processen en procedures te voldoen aan de relevante wet- en regelgeving. Dit doet zij op basis van het principe “Pas toe of leg uit”, waardoor <naam instelling> altijd kan verantwoorden waarom zij wel of niet voldoet. In bijlage D is een overzicht opgenomen van de relevante wet- en regelgeving.

[1] Zie toelichting paragraaf 3.1 over verschillen in de definities ‘informatieveiligheid’ en ‘informatiebeveiliging’
[2] Voor het specifieke Privacy beleid van <Naam Instelling> zie <URL>
[3] *Safety* wordt als verzamelterm gebruikt voor de verschillende aspecten van personele veiligheid: Arbo en milieu, sociale veiligheid, bedrijfshulpverlening e.d.

3. Definitie, doelstelling, doelgroep en reikwijdte

3.1 Informatieveiligheid en Informatiebeveiliging

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

De eindverantwoordelijkheid voor informatieveiligheid ligt bij het bestuur van <naam instelling>.

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 <naam instelling> 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.

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

Commented [L.C.4]: Hier kan ook al een specifiek niveau genoemd worden: bv CMM niveau 3 zoals vastgesteld in het SURF normenkader

Het IB-beleid, en de opvolging daarvan, moet <naam instelling> in staat stellen 'in control' en compliant te zijn. Op basis daarvan kunnen de betrokken <decanen/directeuren> samen met <het College/de Raad van Bestuur> verantwoording afleggen aan de Raad van Toezicht (RvT). De uitvoering van het beleid is ook de basis is om te voldoen aan wettelijke voorschriften.

Randvoorwaarden

Om deze doelstellingen te kunnen bereiken zijn de volgende randvoorwaarden voor <naam instelling> van belang:

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

Uitgangspunten

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

- *Kader*
  Het beleid biedt een kader om (toekomstige) maatregelen in de informatiebeveiliging te toetsen aan de vastgestelde beveiligingsprincipes (hoofdstuk 4), best practices en normen. Daarnaast biedt het een kader om de taken, bevoegdheden en verantwoordelijkheden in de instelling te beleggen.
- *Normen*
  Specifiek voor de SURF gemeenschap[4] is het 'SURF Normenkader Informatie Beveiliging Hoger Onderwijs' (IBHO) vastgesteld. Het IBHO is gebaseerd op de normen die zijn vastgelegd in de ISO-27000-serie. Het IBHO vormt samen met dit beleidsdocument de basis voor een informatie-beveiligingsmanagementsysteem (ISMS[5], zie bijlage A) van <naam instelling>. Het ISMS is ingericht op basis van de internationale standaard ISO 27001. Formele certificering, bijvoorbeeld volgens de norm ISO 27001, wordt niet als noodzakelijk gezien voor <naam instelling>. [<naam instelling> streeft er wel naar om voor specifieke onderdelen van de informatievoorziening een formele certificering te behalen om daarmee de kwaliteit aan te kunnen tonen[6].]
- *Volwassenheid*
  IBHO omschrijft een norm voor de volwassenheid van de Informatiebeveiliging volgens het Capability Maturity Model (CMM)[7]. <naam instelling> streeft naar een volwassenheidsniveau volgens de SURF-richtlijnen.
- *Maatregelen*
  <naam instelling> 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 <naam instelling> zijn te vinden op ……..].

3.3. Doelgroep

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

3.4. Reikwijdte van het beleid

Bij <naam instelling> 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 <naam instelling> kan aanspreken.

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

Onder apparaten en applicaties vallen:

[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] Denk bv. aan een ISO-27001 certificaat voor opslagvoorzieningen ten behoeve van Onderzoek.
[7] https://nl.wikipedia.org/wiki/Capability_Maturity_Model

- 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[8]-devices, zoals bewakingscamera's en sensoren.
- Alle op deze apparaten beschikbare (web/cloud)services en applicaties ('apps').

<Naam instelling> faciliteert het gebruik van privéapparaten (BYOD[9]) <in beperkt mate / ….>. Het gebruik van BYOD op het <Instellings>-netwerk voor toegang tot applicaties of informatie van de instelling valt onder dit IB-beleid.

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

4. Beleidsprincipes informatiebeveiliging

4.1. Inleiding

<Naam Instelling> is een instelling met een open karakter. Vanuit het onderwijs- en onderzoeksperspectief is de insteek "*Open waar mogelijk, gesloten waar nodig*". [Dat past ook bij de FAIR[10] doelstellingen in het onderzoekdomein.] Adequate beveiliging van informatie is steeds een randvoorwaarde en het openstellen van informatie moet een bewuste keuze zijn.

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

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

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

De uiteindelijk door de instelling vastgestelde maatregelen zijn niet altijd 1-op-1 toepasbaar in alle situaties. Soms zijn er bijvoorbeeld processen die afwijken of bestaan er technische of organisatorische beperkingen. In die gevallen moeten er vervangende maatregelen worden genomen waarmee het achterliggende principe tot zijn recht komt en de risico's voldoende worden afgedekt, volgens het uitgangspunt "Pas toe of leg uit"[11].

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

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

4.2. Beleidsprincipes

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

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

- Het ISMS (bijlage A).
- Richtlijnen voor projectmatig werken, werkinstructies en awareness-programma's.
- Classificatie (bijlage C) waarmee een risicoanalyse kan worden uitgevoerd als basis voor technische en organisatorische maatregelen.

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

De vijf door <naam instelling> vastgestelde beleidsprincipes zijn:

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

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

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

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

4	**Security by Design** Integrale aanpak informatiebeveiliging 
Kern	Informatiebeveiliging is vanaf de start een integraal onderdeel van ieder project of iedere verandering mbt informatie, processen en IT-faciliteiten.
Achtergrond	Security by design betekent dat al tijdens de start van een project, het ontwerp van een nieuwe applicatie of ICT-omgeving en bij technische of functionele veranderingen rekening wordt gehouden met de beveiliging van gegevens en de continuïteit van de processen. Dit voorkomt (vaak dure) herstelwerkzaamheden achteraf.
Implicaties	Denk hierbij aan het vaststellen en toetsen van beveiligingseisen in projecten en het inregelen van autorisatieschema's. Zie bijlage B voor een overzicht van alle implicaties.

5	**Security by Default** Standaard beperkte toegang en veilige instellingen 
Kern	Gebruikers hebben alleen toegang tot informatie en IT-faciliteiten die zij nodig hebben voor hun werkzaamheden. Het openstellen van informatie is een bewuste keuze.
Achtergrond	Security by default betekent dat in elke configuratie die wordt geïmplementeerd de aanwezige security opties standaard aan staan. Dit voorkomt ongewenste en ongecontroleerde toegang tot (persoons)gegevens. Openstellen van informatie is daarmee altijd een bewuste keuze na een zorgvuldige afweging.
Implicaties	Denk hierbij aan het definiëren van standaard rollen en het standaard beperken van autorisaties en het standaard beschermen van alle externe communicatie met SSL-technologie. Zie Bijlage B voor een overzicht van alle implicaties.

5. Governance IB-beleid

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 <naam instelling> op strategisch niveau veel aandacht aan afstemming van informatiebeveiliging, arboveiligheid, fysieke beveiliging, business-continuïteit en privacybescherming [(integrale veiligheid)]. Waar mogelijk en nodig vertaalt deze afstemming zich ook naar het tactische en operationele niveau. [De governance rondom informatiebeveiliging wordt daarom binnen Integrale Veiligheid in gezamenlijkheid opgepakt.]

Commented [L.C.5]: Als er geen "integrale veiligheid" is in de instelling dan deze zin dus weglaten

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

5.2. Rollen en hun inpassing in <IB-Governance>

Deze paragraaf beschrijft hoe de <IB-Governance> is georganiseerd, wie waarvoor verantwoordelijk is en aan wie wordt gerapporteerd. In de diverse rollen is onderscheid gemaakt in richtinggevend (strategisch), sturend (tactisch) en uitvoerend (operationeel). [De verantwoordelijkheden die bij de diverse rollen horen, zijn geborgd in de mandaatregeling van < naam instelling >.]

De benaming van de specifieke rollen voor Informatiebeveiliging sluiten zoveel mogelijk aan bij het PvIB[12]:

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

Tabel: rolbenaming conform PvIB

CISO: <Corporate/Central/Chief> Information Security Officer
CISM: <Corporate/Central/Chief> Information Security Manager
[NB: Naast de CISO heeft ook de Compliance Officer (CO) een strategisch Tactische rol mbt Informatieveiligheid]
[Parallel aan de IB-rollen zijn er ook privacy rollen ingevuld: een (Centrale) Privacy Officer ((C)PO) vergelijkbaar met de CISO en Lokale Privacy Officers ((L)PO) bij de <beheerseenheden/faculteiten/servicecentra/…>. Lokaal zijn deze rollen te combineren.]

Commented [L.C.6]: Beschrijf eventueel de specifieke situatie bij de instelling

Commented [L.C.7]: Benoem hier de (voorgenomen) keuzes van de Instelling. Let op. De rollen FG en (C/L)ISO mogen niet gecombineerd worden.

De <IB-Governance> bij <naam instelling> is ingericht volgens het zogenaamde Three Lines of Defence model[13] (ook wel '3LoD'). Dit model wordt algemeen toegepast als model om Governance, Risk en

[12] Beroepsprofielen Informatiebeveiliging: https://www.pvib.nl/kenniscentrum/documenten/beroepsprofielen-informatiebeveiliging-2-0
[13] https://www.icas.com/ca-today-news/internal-audit-three-lines-of-defence-model-explained

Compliance (GRC) te borgen in een operationele organisatie. Het beschrijft niet alleen de rollen binnen de organisatiestructuur, maar ook hun onderlinge samenwerking.

5.2.1 Eerste en tweede lijn

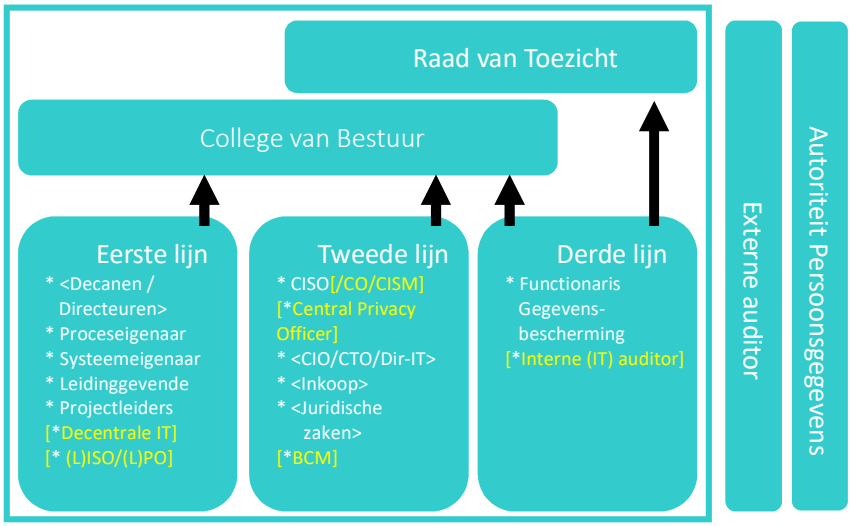
Het 3LoD-model heeft als uitgangspunt dat het lijnmanagement (de business) verantwoordelijk is voor haar eigen processen. De <decanen/directeuren> zorgen ervoor dat beveiligingsmaatregelen ook werkelijk worden geïmplementeerd, dat awareness-programma's worden uitgevoerd, dat personeel wordt opgeleid,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

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

5.2.2 De derde lijn

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

De binnen de AVG verplichte Functionaris Gegevensbescherming (FG) en de <afdeling Internal Audit/ internal auditor> behoren typisch tot de derde lijn. Beiden opereren volledig los van alle andere organisatieonderdelen en rapporteren niet alleen aan <het College/de Raad> van Bestuur, maar ook aan de Raad van Toezicht.



Schema: Three Lines of Defence, vertaald naar Onderwijs

In bijlage E worden de diverse rollen in de <IB-Governance> en het 3LoD-model verder beschreven. De Raad van Toezicht, de externe auditor en de externe toezichthouder (Autoriteit Persoonsgegevens [en/of

/Onderwijsinspectie]) worden verder buiten beschouwing gelaten.

5.2.3 Eindverantwoordelijkheid

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

Commented [L.C.8]: Hier kan ook al meteen gerefereerd worden aan een specifieke regeling in de instelling

5.2.4 Taken, bevoegdheden, verantwoordelijkheden

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

Strategisch niveau	Tactisch niveau	Operationeel niveau
De Corporate Information Security Officer (CISO) is een rol op strategisch (en tactisch) niveau. De CISO is verantwoordelijk voor het beleid en het ISMS-proces. De decentrale [L]ISO's vertalen dat beleid naar hun afdelingen.	De rol van (Corporate) Information Security Manager of (C)ISM is tactisch (en operationeel). De (C)ISM is verantwoordelijk voor de vertaling van de strategie en het beleid naar tactische (en operationele) plannen. Dit doet hij samen met de CISO (vanwege de uniformiteit), de systeem- en proceseigenaren [en de Privacy Officer].	Het operationele niveau is verantwoordelijk voor de implementatie van de informatiebeveiligingsmaatregelen en de afhandeling van incidenten. Dat gebeurt in overleg met de functionele beheerders en relevante IT-functionarissen en waar nodig met de tactische laag.

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

[De actuele invulling voor <naam instelling> van rollen op functies c.q. functionarissen is te vinden in Bijlage F – Actuele invulling rollen Informatiebeveiliging.]

Niveau	Wat?	Wie?	Overleg	Documenten
Richtinggevend (strategisch)	• Bepalen IB-strategie • Organisatie voor IB inrichten • IB planning en control vaststellen • Business continuity management • Communicatie naar management en organisatie	Bestuur (de portefeuillehouder Informatieveiligheid) op basis van advies CISO[/CO] en <CIO/directeur IT/CTO /CFO>	Bestuur stelt vast, <Strategisch IB-overleg> adviseert	• IB beleidsplan • Privacybeleid • Gedrag- en Integriteitscode • ISMS Classificatierichtlijn • [Business continuity plan]
Sturend (tactisch)	Planning & Control IB: • voorbereiden normen en wijze van toetsen • evalueren beleid en maatregelen, ook van externe partijen bij	• Proceseigenaren • Systeemeigenaren • CISO[/CO] • [L]ISO • [Central Privacy Officer]	<Tactisch IB overleg>	• Classificaties/Risico-analyses en audits, inclusief DPIA's en SURFaudit • IB baselines (basismaatregelen) • Jaarplan en-verslag

	contracten • begeleiding interne assessments en externe audits • Communicatie naar proces- en systeem-eigenaren en IT-ondersteuning			
Uitvoerend (operationeel)	• Implementeren IB-maatregelen. • Registreren en evalueren incidenten, inclusief datalekken • Communicatie eindgebruikers	• IT in samenwerking met proces- en systeemeigenaren • Functioneel beheer • (C)ISM • [SOC][14] • [CSIRT[15]] • [Privacy Officer]	<Operationeel IB-overleg> [CSIRT-overleg]	• SLA's (security-paragraaf) • Incidentregistratie inclusief evaluatie • [<CSIRT-charter/ Operationeel Model CSIRT]

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 <naam instelling> gestructureerd overleg gevoerd over het onderwerp informatiebeveiliging op diverse niveaus.

Strategisch	Tactisch	Operationeel
Op strategisch niveau wordt richtinggevend gesproken over governance, re g gaan, zit iisk en compliance, alsmede over doelen, scope en ambitie op het gebied van informatiebeveiliging, in samenhang met privacy. Dit gebeurt in het bestuur, geadviseerd door [<de I[T]-Board/vergelijkbaar overleg> en]de CISO [en de CO][en afgestemd op [de I[T]-strategie en]de risicobereidheid van <naam Instelling>].	Op tactisch niveau wordt de strategie vertaald naar plannen, maatregelen, te hanteren normen, evaluatiemethoden, e.d. Deze plannen en instrumenten zijn sturend voor de uitvoering. Dit tactisch overleg wordt gevoerd tussen de CISO[, CO, CPO, [L]ISO's en (C)ISM('s). Waar nodig in overleg met overige betrokken functionarissen zoals [het CSIRT-coördinator en]proces- of systeemeigenaren.	Op operationeel niveau worden de zaken besproken die de dagelijkse bedrijfsvoering aangaan in de zin van uitvoering en implementatie

Commented [HdB9]: Een volwassen instelling heeft een riskmanagement-proces ingericht en (b.v.) een (Quality &)Risk board als extra toezichthouder/adviesorgaan voor het bestuur. In kleinere instellingen zal het bestuur alleen geadviseerd worden door bv de CIO/CTO en de CISO

Alle drie overlegtypes worden zoveel mogelijk ingepast in bestaande overlegvormen met hetzelfde karakter. Zo bespreekt men op strategisch niveau niet alleen informatiebeveiliging en privacy, maar ook andere risico's waarmee <naam Instelling> te maken kan krijgen, zoals financieel, personeel en commercieel. [Dat betekent bij <naam Instelling> dat informatiebeveiliging op de agenda staat van het <CBB/CVB/IT-board>.] Op tactisch niveau zal het ook gaan over keuze van IT-functionaliteit en-services [op de agenda van het informatiemanagers-overleg <…>]. Op operationeel niveau staat informatiebeveiliging op de agenda van overleggen tussen IT-ondersteuners <…>, functioneel beheerders en IT-beheerders, maar ook op overleggen met key-users en projectteams, <Agile-Sprints/…>.

Documenten

Voor informatiebeveiliging wordt bij <naam Instelling> dezelfde (PDCA-)managementcyclus gevolgd, die ook

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

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

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 <naam Instelling> voor informatiebeveiliging hanteert zoals genoemd in bovenstaande tabel.

5.3. Bewustwording en training

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

Commented [L.C.10]: Eventueel beschrijven hoe campagnes "samengepakt" worden. Bv. gecombineerd via een drieluit bestaande
uit mensen van IT-Privacy-Datamanagement. (Het gaat dan om veilige opslag data gebruik persoonsgegevens in onderzoek en ondersteunende processen/kwaliteitseisen/research datamanagement)

5.4. Controle, oefenen, naleving en sancties

Bij <naam instelling> is de Internal Audit afdeling verantwoordelijk voor de (planning van) interne IT audits en de CISO voor de controle op de uitvoering van de informatiebeveiligingsjaarplannen. De <[L]ISO's en [C]ISM('s)> ondersteunen daarbij. [De uitvoering van de audits is belegd bij <CSIRT/SOC[16]/Internal IT-audit>.]

Commented [L.C.11]: Conform 3LoD model, als een dergelijke afdeling er niet is, dan zou jet ook bij de CISO belegd kunnen zijn.

De interne controles vinden jaarlijks plaats en worden naast de reguliere formele audits aangevuld met diverse incidentele activiteiten, zoals het nemen van steekproeven, het uitvoeren van penetratietesten en het controleren van de feitelijke werking van de vastgestelde beveiligingsmaatregelen. Daarnaast worden vaardigheden en operationele procedures regelmatig getest in brainstormsessies of oefeningen. Voorbeelden hiervan zijn informatiebeveiligings-/CSIRT-firedrills[17].

De informatiesystemen (of-processen) van <naam instelling> worden intern geaudit. De audit richt zich op (1) de classificatie van de in het informatiesysteem vastgelegde gegevens, (2) de inventarisatie van de risico's, (3) de genomen beveiligingsmaatregelen en (4) de samenhang tussen 1, 2 en 3. Voor elk informatiesysteem wordt een audit frequentie vastgesteld aan de hand van de risicoclassificatie. Als een informatiesysteem wordt vervangen of als er belangrijke wijzingen plaatsvinden in de beveiliging, wordt er een audit uitgevoerd op basis van een nieuwe businessimpact en risicoanalyse. De externe controle wordt in een cyclus van vier jaar uitgevoerd door een onafhankelijke partij. Dit is qua planning gekoppeld met het accountantsonderzoek en dit wordt zoveel mogelijk gecombineerd met de normale planning & control-cyclus.

Commented [L.C.12]: Dit is aanvullend op de Jaarlijkse General IT-controls van de accountant, die zich in veel gevallen beperkt tot de onderdelen die in relatie staan met de verantwoording van de jaarrekening. Uiteraard kan een ander schema aangehouden worden, hier speelt ook het kosten aspect.

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

[<Naam instelling> neemt deel aan de SURFaudit selfassessment cyclus en de bijbehorende tweejaarlijkse benchmark. Minimaal eens per <2/4> jaar wordt een SURF Peer review aangevraagd.]

[16] Security Operations Centre (SOC)

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

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

Controle op de naleving vindt plaats door toezicht te houden op hoe in de dagelijkse praktijk met informatiebeveiliging wordt omgegaan. Hierbij is het van belang dat leidinggevenden (inclusief onderwijsverantwoordelijken) de medewerkers en studenten aanspreken op tekortkomingen. Voor het toezicht op de naleving van de AVG is de 'Functionaris Gegevensbescherming' (FG) verantwoordelijk.

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

Commented [L.C.13]: Wordt vastgelegd in de AUP

5.5. Financiering

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

Centraal

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

Decentraal

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

6. Melding en afhandeling van incidenten

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

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

Incidenten kan men bij <naam instelling> melden bij het <CSIRT/CERT>[18]-meldpunt: <...>[19] . <Naam instelling> heeft de contactgegevens van dit meldpunt duidelijk gecommuniceerd naar haar medewerkers, studenten en derden.

[18] <Computer Security Incident Response Team / Computer Emergency Response Team>
[Zie <Bijlage F / het CSIRT Charter/Operational Model] voor meer informatie]

[19] <Servicedesk>@<instelling.nl>, tel. +31 <12345678>

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

De incidenten worden afgehandeld volgens het door <naam instelling> vastgestelde Incident managementproces, waar de afhandeling van datalekken een onderdeel van is. [Het CSIRT <Charter/ Operational Model> beschrijft het proces als het gaat over ernstige incidenten en incidenten buiten reguliere bedrijfstijden] .

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

Commented [L.C.14]: Hier moet dus ook de CPO/FG bij worden aangehaakt indien er persoonsgegevens in het geding zijn.
Refereer eventueel naar een separaat datalekken proces als dat in uw instelling zo geregeld is.

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 < /2/3> jaar geëvalueerd en zo nodig bijgesteld. [Minimaal 1 keer per 4 jaar, of] na een substantiële verandering van het instellingsbeleid of belangrijke ontwikkelingen op cyberveiligheidsgebied, wordt het beleid herzien en opnieuw vastgesteld.

Dit beleid, versie <versienummer>, is vastgesteld door het bestuur van <naam instelling> op <datum> [en kan worden aangehaald als “Informatiebeveiligingsbeleid van <naam Instelling>”].

Commented [L.C.15]: Het beleid voorziet (via de maatregelen) in een vorm van een medewerker volgsysteem (bv door het bijhouden van logfiles). Volgens de WOR is een dergelijk beleid instemmingsplichtig.

Commented [L.C.16]: Bv vaststelling instellings strategisch plan, IT-strategie,....

Commented [L.C.17]: Ook als er relatief weinig wijzigt is dit aan te bevelen. Het zet IB namelijk weer op de agenda, wat belangrijk is voor de bestuurlijke awareness.

Bijlage A- Schematisch overzicht inrichting ISMS

Informatiebeveiliging is een continu proces. Kort gezegd: eerst moet worden vastgesteld wat nodig is, waarna maatregelen worden getroffen. Deze maatregelen worden vastgelegd in een jaarplan. De maatregelen kunnen veranderen (omdat bedreigingen en risico's veranderen, maar ook wet- en regelgeving is aan verandering onderhevig). Controle kan dan aanleiding geven tot bijsturing van de maatregelen. Daarnaast kan ook het totaalpakket van eisen, maatregelen en controle aan een herijking toe zijn en zal dus periodiek geëvalueerd moeten worden. Het gehele proces van informatiebeveiliging volgt dus een Plan-Do-Check-Act (PDCA)-cyclus (zie afbeelding).

De complete set van maatregelen, processen en procedures wordt vastgelegd in een Information Security Management System (ISMS) en biedt daarmee ondersteuning in het doorlopen van de PDCA-cyclus. De jaarlijkse planningen zijn te vinden zijn in de planning/ specifieke planning bij een <Instelling>, en meer in detail in de <I/IT> jaarplannen.

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

Voorbereiding

In de voorbereidende fase komen de volgende zaken aan de orde:

- 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 er onder 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 fasen:

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

Bijlage B – Informatiebeveiligingsprincipes

1	**Risico-gebaseerd** Informatiebeveiliging is risico-gebaseerd 
Kern	We baseren de maatregelen op de mogelijke veiligheidsrisico's van onze informatie, processen en IT-faciliteiten.
Achtergrond	Het delen van kennis (openheid) is een belangrijke kernwaarde van het onderwijs- en onderzoekproces van <naam instelling>. 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[20] uitgevoerd.] • De risico's worden ingeschat en vastgesteld op basis van een risicoclassificatie (**Bijlage <C>**). • <Naam instelling> 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. • Er worden maatregelen getroffen om het vastgestelde risico op Beschikbaarheid, Integriteit en Vertrouwelijkheid te brengen naar het geaccepteerde niveau. • Informatie heeft één eigenaar. • Eigenaren van informatie, informatiesystemen, applicaties en processen zijn verantwoordelijk voor de implementatie en operationele handhaving van maatregelen onder het principe van "Pas toe of leg uit". • Afwijkingen kunnen worden geaccepteerd binnen de risicobereidheid (risk-appetite) van <naam instelling>, uiteindelijk te bepalen door het bestuur. • Voor afwijkingen moet het risico-acceptatieproces worden gevolgd, met acceptatie door de informatie-, proces- of applicatie-eigenaar. • De informatie-eigenaar (of eventueel ook de proces- of applicatie-eigenaar) tekent voor acceptatie van de risico's. • Maatregelen moeten zo worden ingericht dat hun effect controleerbaar is. • De hoogste risico's worden als eerste gemitigeerd. • Op basis van de risicoanalyse kan informatiebeveiliging voor gebruiksgemak kiezen.

Commented [L.C.18]: Deze implicatie dus opnemen als een BCM proces aanwezig is. Als dat niet zo is, dan zal het mee genomen kunnen worden bij de Classificatie (Beschikbaarheid).

Commented [L.C.19]: Dit moet dus deel uitmaken van alle overige processen, bv door te beschrijven in een richtlijn voor projectmatig werken.

[20] 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].

	• 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. • <Naam instelling> blijft verantwoordelijk voor adequate bescherming van informatie bij gebruik van externe diensten voor informatieverwerking. • Waar van toepassing bevatten contracten de veiligheidseisen en de levering van externe toetsing (assurance) die laat zien dat maatregelen effectief zijn.

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

3	**Altijd** Informatiebeveiliging is een continu proces 
Kern	Informatiebeveiliging zit in het DNA van al onze werkzaamheden.
Achtergrond	De omgeving verandert continu; cyberdreigingen nemen toe en af; processen veranderen, medewerkers en studenten veranderen etc. Eenmalig de maatregelen bepalen en implementeren is onvoldoende om een veilig klimaat te behouden. Informatiebeveiliging heeft alleen zin als dit een continu proces is van het nemen van maatregelen, bewustzijn en controles.
Implicaties	• Er wordt een Information Security management Systeem (ISMS, **Bijlage <A>**) ingericht waarmee door middel van een PDCA-cyclus alle aspecten van het IB-beleid adequaat worden opgevolgd. • Periodiek worden audits en assessments uitgevoerd die het mogelijk maken het beleid en de genomen maatregelen te controleren op effectiviteit (controleerbaarheid). • Bij instroom van nieuwe medewerkers en studenten is er aandacht voor de bewustwording van de risico's en de beveiligingsprocedures van <naam instelling> rond toegang en gebruik van IT-middelen. • Periodiek worden accounts met hoge privileges gevalideerd. • <Naam instelling> organiseert regelmatig cybersecurity-awareness activiteiten voor de diverse doelgroepen: studenten, medewerkers, leidinggevenden en partners van <naam instelling>. • Bij aanpassingen in rollen, taken, en verantwoordelijkheden van een persoon worden ook de autorisaties daarmee in overeenstemming gebracht en aangepast. • Er wordt een proces ingericht om het dreigingsbeeld voor <naam Instelling> te bepalen en periodiek bij te stellen. Nieuwe dreigingen leiden waar nodig tot aanpassing van maatregelen.

Commented [L.C.20]: Dit kan bv. georganiseerd worden door het instellen/inhuren van een Security Operations Center (SOC).

4	**Security by Design** Integrale aanpak informatiebeveiliging 
Kern	Informatiebeveiliging is vanaf de start een integraal onderdeel van ieder project of iedere verandering mbt informatie, processen en IT-faciliteiten.
Achtergrond	Security by design betekent dat al tijdens de start van een project, het ontwerp van een nieuwe applicatie of ICT-omgeving en bij technische of functionele veranderingen rekening wordt gehouden met de beveiliging van gegevens en de

	continuïteit van de processen. Dit voorkomt (vaak dure) herstelwerkzaamheden achteraf.
Implicaties	• Voor elk nieuw project/software-inkoop/innovatie worden de security-eisen (non-functional requirements) vanaf de start meegenomen. • Voor de livegang wordt de toepassing van de security-eisen getoetst en/of getest. • Bij elk IT-systeem of inrichting wordt ter bevordering van informatiebeveiliging het principe van 'minste rechten' gehanteerd. Dat betekent dat ernaar wordt gestreefd om niet meer rechten te verlenen dan nodig zijn voor adequate functie- en bedrijfsuitoefening. • Toegang tot systemen is gebaseerd op autorisatieschema's. • Scheiding van verantwoordelijkheden wordt toegepast in processen en procedures. • In het ontwerp wordt meegenomen dat het gebruik van informatie en IT-voorzieningen herleidbaar is tot een verantwoordelijke gebruiker. • Er wordt een richtlijn "security in projecten" vastgesteld, gebaseerd op de maatregelen die voortkomen uit de risicoclassificatie en maatregelen die mogelijk voortvloeien uit de gegevensbeschermingseffectbeoordeling (DPIA) in het kader van de AVG. • Bij procesontwerp worden maatregelen meegenomen die de continuïteit van het proces afdoende kunnen waarborgen.

5	**Security by Default** Standaard beperkte toegang en veilige instellingen 
Kern	Gebruikers hebben alleen toegang tot informatie en IT-faciliteiten die zij nodig hebben voor hun werkzaamheden. Het openstellen van informatie is een bewuste keuze.
Achtergrond	Security by default betekent dat in elke configuratie die wordt geïmplementeerd de aanwezige security opties standaard aan staan. Dit voorkomt ongewenste en ongecontroleerde toegang tot (persoons)gegevens. Openstellen van informatie is daarmee altijd een bewuste keuze na een zorgvuldige afweging.
Implicaties	• De beveiligingsbaseline van de standaardconfiguratie moet worden vastgelegd. (bv. het standaard beschermen van alle externe communicatie met SSL-technologie) • Het principe bij initiële inrichting van een informatiesysteem of een infrastructuur is "*gesloten, tenzij*". • Afwijking van de initiële inrichting volgt het principe "Pas toe of leg uit." • Security wordt geborgd in een changemanagementproces. • Toegang tot informatie is rol-gebaseerd, waardoor gebruikers alleen toegang hebben tot informatie en IT-faciliteiten die zij nodig hebben voor hun werkzaamheden (vastgelegd in een autorisatieschema)

	• Er worden enkele hoofdrollen geïdentificeerd op basis waarvan baseline-autorisaties worden toegekend. Te denken valt aan de hoofdrol student, medewerker, leverancier etc. Gebruikers krijgen standaard alleen deze rollen. • Logging- en auditprocessen worden zodanig ingeregeld dat toegang tot informatie en IT-faciliteiten herleidbaar is tot een verantwoordelijke gebruiker.

Bijlage C – 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.
<Naam instelling> volgt een risico gestuurde aanpak. De RvB/CvB stelt eens per jaar vast wat de risicobereidheid van de instelling is en hoe de bijbehorende schade categorieën er uit zien.
Voor alle data die verwerkt wordt, wordt het risico bepaald door impact die een incident kan hebben en de kans dat een incident zich voordoet. De impact wordt bepaald door de schade die een bepaalde dataset kan veroorzaken, door bijvoorbeeld de data te verliezen. De schade wordt vastgesteld door de data eigenaar die de data in een bepaalde categorie indeelt.
De risicobereidheid en de schade zijn een gegeven. De kans wordt bepaald door de maatregelen die genomen zijn om de data te beschermen. Aanvullende maatregelen verkleinen de kans. De security officer bepaald welke maatregelen geïmplementeerd moeten zijn zodat de kans en daarmee het restrisico naar een acceptabel laag niveau kan worden gebracht.

Procesweergave

Periodiek

1.
Vaststellen risico bereidheid
RvB / CvB

Per dataset

2.
Vaststellen schadecategorie
Data eigenaar

Per verwerkend system

3.
Bijstellen kans
Security officer

1. Risico bereidheid

Met een risicoanalyse kan de mogelijke schade worden geëvalueerd die een dreiging kan toebrengen aan

Commented [VR(21]: In kader kwetsbaarhedenmanagement hebben we risico acceptatie opgedeeld naar niveaus van verantwoordelijkheden. Dus beperkte risicos kunnen lager in de organisatie geaccepteerd worden en grotere en bredere risico's moeten door CvB geaccepteerd worden.

Commented [RKT22]: Expliciet voorleggen aan RvB / CvB

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. <Naam instelling> 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 <naam instelling> is in onderstaand schema weergegeven.

Tabel 1: Risicobereidheid

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

Schade categorieën

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 <naam instelling> zijn als volgt bepaald:

Tabel 2: Indicatie schade categorieën

INDICATIE SCHADE CATEGORIEËN

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	Langdurige verstoring van een groot deel van het onderwijs op een of meer	Publicatiebeperkingen, reputatieschade aan onderzoeker of instelling, patenten of contractuele afspraken	Directe schade tussen €250.000 en €1.500.000

Commented [RKT23]: Template. Voorleggen aan onderwijs, onderzoek en bedrijfsvoering in eigen instelling. Zo wordt betrokkenheid vergroot.

Commented [RKT24]: Bedragen moeten nog worden bijgesteld

	maatschappelijk gevoelige werkzaamheden (zoals dierproeven).	instituten.		
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

Voor gedefinieerde waarde

De organisatie heeft voor enkele type data een voor gedefinieerde waarde gegeven die de standaard is voor de hele organisatie. Dit is een waarde voor de hele set, of een waarde per uniek voorkomen. Zo is een applicatie waar 10 reguliere persoonsgegevens in voorkomen minder waardevol dan een applicatie waar van alle medewerkers de persoonsgegevens in staan.

Tabel 3: voor gedefinieerde waarde

Datatype	Waarde per uniek voorkomen	Waarde/schade dataset
Reguliere persoonsgegeven naam, telefoonnummer en/of e-mail adres	€10,00	-
Overige reguliere persoonsgegevens	-	Ernstige schade (door boetes)
Bijzondere persoonsgegevens		Ernstige schade (door boetes)
Kopie identiteitsbewijs / rijke set aan gegevens van elke persoon	-	Ernstige schade (identiteitsfraude individuen)
Herleidbaarheid personen naar zeer gevoelig werk (bv dierproef)	-	Ontwrichtende schade (voor individuen)

Commented [RKT25]: Voorzet, inhoud tabel moet nog worden bepaald. We zouden hier ook geld aan kunnen koppelen. Een kleine dataset is voor een derde meer waard dar een grote? Of maakt dat voor de boetes niet uit?

1. 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.

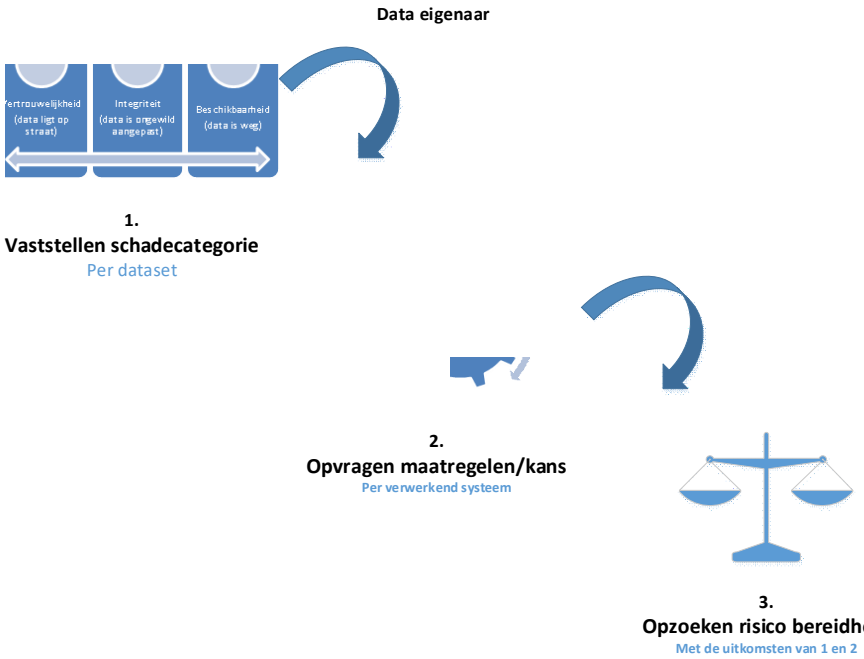
- **Integriteit**: We kunnen niet meer garanderen dat de data niet is aangepast.
- **Vertrouwelijkheid**: De data is in handen van derden en deze kunnen er mee doen wat ze willen.

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

Tabel 4: 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, 4 en 4 de categorie waarin zijn data valt.
2. De data eigenaar vraagt bij de security 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 hij op zoek naar een ander systeem of overlegt met de systeem eigenaar en de security 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 officer voor een maatwerk risico analyse.

2. Bepalen maatregelen / kansen

De (C)ISO 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[21], 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[22]. 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

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

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

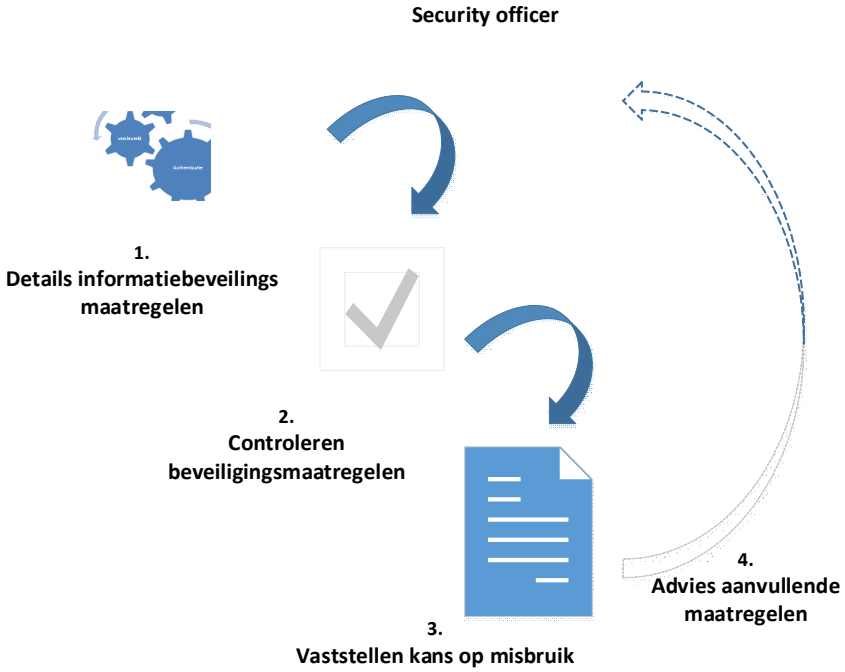
technische eisen die gesteld worden aan het systeem dat de dienst levert. Implementatie van de maatregelen voor 'laag' en 'midden' of compenserende maatregelen die hetzelfde doel halen geeft een systeem een goede weerbaarheid.

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 GEIMPLEMENTEERD	KANS
GEEN/ONBEKEND	Hoog
STITCH	Reëel
STITCH + NORMENKADER	Beperkt
RISICOANALYSE	Minimaal

Proces gezien vanuit security officer en systeem eigenaar



1. De maatregelen die zijn genomen voor de informatiebeveiliging van een bepaald systeem worden

aangeleverd of uitgevraagd.
2. De security officer toetst of het systeem voldoet aan (een van) de twee sets aan maatregelen.
3. Op basis van de uitkomst van 2 koppelt hij de kans op misbruik aan het systeem, overeenkomstig tabel 5 hierboven. Deze uitkomst kan intern in de organisatie gepubliceerd worden zodat een volgende dataeigenaar de geconstateerde kans op kan zoeken.
4. Indien een systeem niet voldoet komt de security 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 <naam instelling>.

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

2. **Algemene Verordening Gegevensbescherming (AVG)**
   [De instelling heeft een separaat gegevensbeschermingsbeleid vastgesteld waarin naleving van de AVG wordt geborgd. Naleving van het informatiebeveiliging<s/- en gegevensbeschermings>beleid inclusief de daarin vermelde technische en organisatorische maatregelen zorgen samen voor het voldoen aan de AVG.

   Commented [L.C.26]: Voor instellingen die deze template gebruiken en geen geïntegreerd IBP beleid hebben)

3. **Wettelijke Bewaartermijnen/Archiefwet**
   <Naam instelling> 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. <Naam instelling> hanteert daarbij het Basisselectiedocument[23] van de sector <universiteiten/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.

   Commented [L.C.27]: Wellicht voor Onderzoeksinstituten resp. academische ziekenhuizen een ander document

4. **Auteurswet**
   <Naam instelling> respecteert auteursrechten en handelt daarnaar.

   Commented [L.C.28]: De Auteurswet is enigszins arbitrair om te noemen.
   Ook de Rijksoctrooiwet enz. zouden genoemd kunnen worden.
   Let op: In het kader van Open Sourceis er nogal een ontwikkeling aan de hand die de auteursrechtenkwestie behoorlijk dynamisch zal gaan maken

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

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

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

   Commented [L.C.29]: De <CSIRT-coördinator/CISO/…> adviseren hierover, samen met <Juridische Zaken> aan het bestuur. Alleen het bestuur kan aangifte doe en is daartoe feitelijk verplicht.

[23] <referentie VH-document /referentie VSNU-document (wordt per 1-1-2020? opnieuw vastgesteld)>

7. **Overige codes en landelijke afspraken**

   Het informatiebeveiligingsbeleid bij <naam instelling> is gebaseerd op het SURF Normenkader en de instelling is deelnemer in de <VSNU/VH[24]> . <Naam instelling> is in dit kader gehouden aan de volgende codes en landelijke afspraken:

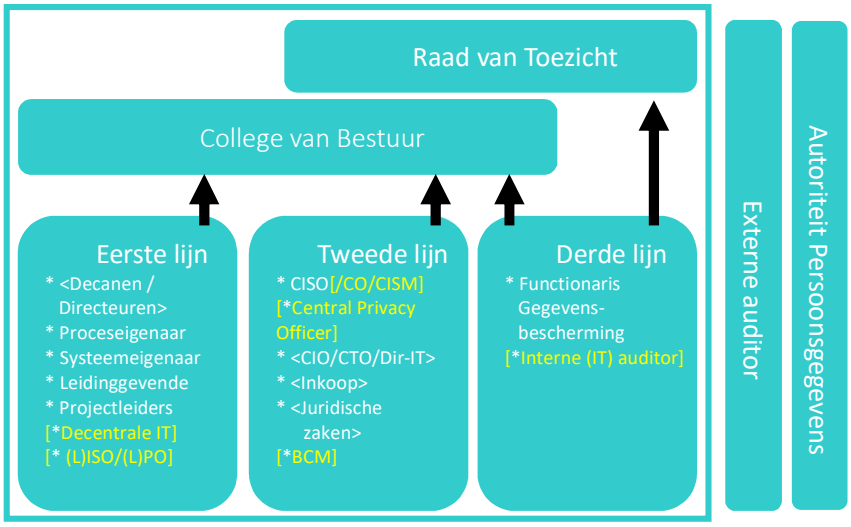
   - Code goed bestuur universiteiten.
   - Nederlandse gedragscode wetenschappelijke integriteit.
   - Juridisch Normenkader Hoger Onderwijs.
   - Basisselectie document <WO/UMC/HO/…>.
   - …

Commented [L.C.30]: Actualiseren en aanvullen met referenties naar behoefte en situatie

[24] Vereniging Samenwerkende Nederlandse Universiteiten, resp. Vereniging van Hogescholen

Bijlage E- Rollen in de IB-governance

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



Schema: Three Lines of Defence, vertaald naar Onderwijs

<College/Raad> van Bestuur
Het bestuur is verantwoordelijk voor de informatiebeveiliging binnen <naam instelling> en stelt het beleid en de governance op het gebied van informatieveiligheid vast. Informatieveiligheid komt zo vaak als nodig en minimaal <1x/2x> per jaar op de agenda van het bestuur. Het bestuur wijst een van haar leden aan als portefeuillehouder informatieveiligheid.

De inhoudelijke verantwoordelijkheid voor zover het de digitale informatiebeveiliging betreft is door de portefeuillehouder <belegd bij/gemandateerd aan> de CISO. Deze heeft de opdracht om op de digitale informatiebeveiliging van de gehele instelling toe te zien. De niet-digitale informatiebeveiliging is belegd bij <de compliance officer/de proceseigenaren>.

Functionaris Gegevensbescherming (FG of Data Protection Officer)
De FG houdt binnen <naam instelling> toezicht op de toepassing en naleving van de AVG, zoals beschreven in het privacybeleid van < naam instelling >[25]. De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie in de instelling.

[Interne (IT-)auditor
De interne IT-auditor is onderdeel van de interne audit-organisatie en controleert jaarlijks het goed en

Commented [L.C.31]: Dat is best practice en wordt ook sterk aangeraden door SCIPR. De CISO rapporteert dan rechtstreeks aan CvB.
1) Het kan zijn dat deze rol bij een instelling wordt ingevuld door CIO of CTO/Dir. IT of vergelijkbaar.
2) Het kan ook zijn dat CIO/CTO of de IV-manager aan CvB rapporteert en de CISO zelf alleen direct aan CIO/CTO/IV-manager, dat wordt afgeraden maar dan moet deze zin aangepast worden.

Commented [L.C.32]: informatieveiligheid betreft niet uitsluitend hetgeen via de digitale (snel)weg loopt. Steeds meer universiteiten haken aan bij de idee om de compliance officer een rol te geven.
De CISO staat wellicht niet voor het geheel aan de lat. Denk dus aan niet digitale informatie en bv. ook aan datamanagement.

[25] Referentie aan het beleid (staat wellicht ook in de inleiding)

betrouwbaar functioneren van de interne IT-organisatie. Dit omvat o.a. de structuur en verantwoordelijkheden van de IT-organisatie, de hardware, de software, het interne- en (indien aanwezig) externe netwerk, veiligheids- en calamiteitensystemen. De interne IT-auditor rapporteert aan de interne auditor en aan de belangrijkste stakeholders CIO/CTO/CISO/FG. De interne auditor rapporteert ook aan de opdrachtgever, doorgaans is dit de portefeuillehouder in het bestuur, en aan de Raad van toezicht.]

Commented [L.C.33]: Als er dus een aparte interne IT-auditor is, zal deze meestal aan de Interne auditor en de stakeholders (CIO/CTO/CISO/FG) rapporteren, maar niet rechtstreeks aan CvB/RvT

Corporate Information Security Officer (CISO)

De CISO is een rol op strategisch (en tactisch) niveau. Hij adviseert en rapporteert onafhankelijk en direct aan het bestuur[26]. De CISO stelt het IB-beleid op, helpt bij een juiste vertaling daarvan naar instellingsonderdelen, ziet toe op de (uniforme) naleving ervan en rapporteert over lacunes, inconsistenties en onvolkomenheden. De CISO kan zowel gevraagd als ongevraagd advies geven. < De CIO / CFO> is de hiërarchisch leidinggevende van de CISO. De rol van CISO is belegd bij één persoon, maar er kunnen decentraal meer (Local) Information Security Officers ofwel (L)ISO's zijn, die het beleid in tactisch opzicht decentraal implementeren.

Commented [L.C.34]: De CISO zit dus bij voorkeur niet binnen de IT afdeling om onafhankelijkheid te kunnen borgen.

Commented [L.C.35]: De CIO-rol kan ook ingevuld worden door de CTO (Dir. IT) . De CFO (Chief Financial Officer) wordt minder vaak in deze rol geplaatst.

[De CISO heeft verschillende bevoegdheden. Zo kan hij onderzoek doen, onderzoek laten uitvoeren (audits), informatie opvragen en deze in principe ook krijgen. In het geval de privacy in het geding is (en in alle bijzondere gevallen) beslist het bestuur]. [Binnen <Naam Instelling> vervult de CISO ook de rol van Business Continuity Manager (BCM). Dit is ook een strategisch/tactische rol die tot doel heeft de business continuïteit te bewaken.]

Commented [L.C.36]: Als er geen aparte BCM is

[Compliance Officer (CO)

De CO is een rol op strategisch (en tactisch) niveau. De CO rapporteert rechtstreeks aan het bestuur. De CO zorgt voor de naleving van governance-aspecten en wet- en regelgeving binnen de instelling.]

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

De CISM vervult een rol bij de vertaling van de strategie naar tactische (operationele) en technische plannen en maatregelen. Dit doet hij samen met de CISO en met de systeem- en proceseigenaren. Tevens adviseert de CISM over specifieke informatiebeveiligingsmaatregelen, bijvoorbeeld in projecten, bij acquisities van software of hardware, etc. De CISM heeft < Directeur IT/ CTO> als hiërarchisch leidinggevende. [Naast de CISM zijn er decentraal meer functionarissen met de rol (Local) Information Security Manager. Deze functionarissen vertalen de centraal vastgestelde maatregelen en operationele plannen door naar de decentrale organisatie.]

[(Corporate of Local) Privacy Officer (<(C/L)>PO)

De Privacy Officer houdt zich binnen <naam instelling> centraal of decentraal bezig met de toepassing en naleving van de AVG. In sommige gevallen in samenwerking met de (C/L)ISM en (C/L)ISO, bijvoorbeeld bij het analyseren van (mogelijke) datalekken. Andere voorbeelden hiervan zijn bij het beoordelen van risico's en maatregelen in het geval van een Gegevensbeschermingseffectbeoordeling (DPIA) of bij het afsluiten van verwerkersovereenkomsten in het kader van de AVG.]

[Business Continuity Manager (BCM)

De BCM draagt zorg voor het definiëren, opzetten en controleren van processen en middelen die de continuïteit van de instelling waarborgen in brede zin. Dus techniek, procedures, mensen, etc. De BCM coördineert de IT-beveiliging met de CISO.]

Proceseigenaar

Een proceseigenaar is iemand die verantwoordelijk is voor een van de primaire of ondersteunende processen, al dan niet gebruikmakend van meerdere systemen.

---

[26] Bij overgang naar "Integrale Veiligheid" kan de adviesrol naar het bestuur vervangen worden door CSO of "Chief Security Officer" – die dan zowel over informatiebeveiliging, fysieke beveiliging en safety gaat.]

Vaak is de proceseigenaar van een primair proces ook formeel intern verantwoordelijk voor de gegevens die in dat proces en de daarvan afgeleide processen worden verwerkt (informatie- of broneigenaar).

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

Leidinggevende (inclusief onderwijsverantwoordelijken)
Naleving van het IB-beleid is onderdeel van het integrale bedrijfsproces. Iedere leidinggevende heeft de taak om:

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

[CSIRT-coördinator
Een specifieke rol op het gebied van informatiebeveiliging is het CSIRT[27]-coördinator. De CSIRT-coördinator wordt benoemd door <het bestuur> en is verantwoordelijk voor information security incident management binnen de instelling. In dat kader is het CSIRT-coördinator ook bevoegd om tijdelijk computersystemen of netwerksegmenten te laten isoleren. Het CSIRT-coördinator werkt voor het uitvoeren van deze taken samen met andere, formeel benoemde, CSIRT-leden volgens het door het bestuur vastgestelde <CSIRT-charter / CERT-operational-model / …>.]

Commented [L.C.37]: Kan dus ook weggelaten worden. Dit gaat over high prio incident proces en inrichting CERT, maar als mandaaten zwaar zijn ingeregeld wordt ook direct aan CvB gerapporteerd, meestal vanuit de 2-de LoD

Commented [L.C.38]: Deze rol is soms belegd bij de CISO, soms bij de CISM

Commented [L.C.39]: Doorgaans zal het worden opgesteld door de CISO

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

[Bijlage F - Actuele Invulling rollen informatiebeveiliging]

Rollen uit informatiebeveiligingsbeleid	Gewenste invulling
Bestuur	
Binnen bestuur: portefeuillehouder Informatiebeveiliging	
Business Continuity Manager = BCM	
Information Security Officer = CISO	
Compliance Officer = CO	
Information Security Manager = CISM	
Privacy Officer = PO	
Functionaris Gegevensbescherming	
Interne IT-auditor	
CIO	
CTO/Directeur IT	
CSIRT-coördinator	
Belangrijkste proceseigenaren	
Decanen/directeuren	

Commented [L.C.40]: Dit model beleid is het eenvoudigst toe te passen door de generieke rollen die in het beleid zijn benoemd in deze bijlage te vertalen naar de voor uw instelling geldende rollen/namen: daarbij kunnen desgewenst ook meerdere rollen aan één functionaris gegund worden. Natuurlijk is het ook mogelijk om deze vertaalslag direct in het beleid zelf te doen, en deze bijlage leeg te laten – het nadeel daarvan is dat versie management lastiger is wanneer functionarissen van rol veranderen en wanneer het Instellingsbeleid in de nabije toekomst wordt aangepast: met de lokale vertaalslag in deze bijlage F is dat eenvoudiger. Geheel weglaten van deze bijlage met al of niet een referentie naar operationeel document is ook een optie

Bijlage G - Documenten informatiebeveiliging

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

In het kader van informatiebeveiliging hanteert <naam instelling> de volgende documenten:

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

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

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

4. *Jaarplan/verslag*
   De CISO levert, in lijn met de PDCA-cyclus, jaarlijks een verslag over het afgelopen jaar en een jaarplan voor het volgende jaar op aan het bestuur. Het jaarverslag is mede gebaseerd op de resultaten van de periodieke controles/audits. Er wordt o.a. ingegaan op incidenten, resultaten van risicoanalyses (inclusief genomen maatregelen) en andere initiatieven die het afgelopen jaar hebben plaatsgevonden. Het jaarplan wordt in ieder geval afgestemd met het Privacy jaarplan wat door de FG wordt opgesteld. [De verslagen worden geconsolideerd in de bestuurlijke Planning & Control-cyclus.] Waar nodig wordt apart aandacht besteed aan specifieke systemen/applicaties.
   Het jaarplan moet getoetst worden op de beschikbaarheid van resources (mensen en middelen), afgezet tegen de risico's die gemitigeerd moeten worden.

5. *<Baseline van informatiebeveiligingsmaatregelen /basisniveau maatregelen/maatregelen database>*
   Deze baseline beschrijft de maatregelen die minimaal nodig zijn om het voor <naam instelling> vastgestelde minimale niveau van informatiebeveiliging te kunnen waarborgen. Dit vloeit voort uit het beleid of uit aanvullende besluiten die door het bestuur genomen zijn. Deze basismaatregelen moeten overal in de instelling worden genomen. De baseline wordt gemaakt door de (C)ISM('s) in overleg met de CISO en vastgesteld in het tactisch IB-overleg. Wanneer er processen of systemen zijn die na een classificatie of andere risicoanalyse (bijvoorbeeld een DPIA) hogere beveiligingseisen nodig hebben, dan worden er aanvullende maatregelen genomen.

6. *Policies*
   Gedragscodes en richtlijnen op het gebied van informatiebeveiliging voor medewerkers, studenten en derden (al dan niet voor specifieke doelgroepen), zoals:
   - Acceptable Use Policy, voor het veilig gebruik van IT-voorzieningen, e-mail en internetgebruik door medewerkers, studenten en derden.
   - [RFC-2350 voor de lokale CSIRT (zie hoofdstuk 6. Melding en afhandeling van incidenten (CSIRT))].
   - [<Charter/Operational model> van het CSIRT].
   - Privacy Beleid.
   - [Richtlijn Authenticatie (inclusief wachtwoordbeleid].
   - [Richtlijn Autorisatie].
   - [Toepassing van cryptografische hulpmiddelen].
   - [Richtlijn responsible disclosure].

Commented [L.C.41]: Actualiseren en aanvullen met referenties naar behoefte en situatie

- [IT Lifecycle management[28]].
- Integriteits-/gedragscode voor ICT-functionarissen.

Daarnaast is informatiebeveiliging een vast onderdeel van de volgende documenten:

7. *Dienstenovereenkomsten (DVO's, SLA's), inhuur- en uitbestedingscontracten en eventueel bijbehorende verwerkersovereenkomsten*
   Bij de inhuur van personeel en bij de inkoop van middelen (met name hardware, software, applicatie/cloud platforms en diensten), wordt expliciet aandacht aan informatiebeveiliging besteed. Dit wordt gedaan door o.a. het IB-beleid toe te passen op externen en door beveiliging standaardonderdeel van de inkoopvoorwaarden te maken. Afspraken worden in een contract(en) met de leverancier vastgelegd. Het contract bevat standaard een informatiebeveiligingsparagraaf waarin de verantwoordelijkheden van de leverancier zijn opgenomen. De basis hiervoor is het SURF Juridisch Normenkader Cloudservices Hoger Onderwijs[29] die een informatiebeveiliging bijlage bevat.

8. *[Business Continuity Plan]*
   Het Business Continuity Plan wordt opgesteld op initiatief van de Business Continuity Manager en in samenwerking met het bestuur, de CISO, de proceseigenaren, het hoofd IT en < CIO/hoofd Facilitaire Zaken.>]

[28] Bijvoorbeeld: bij de aanschaf van hard/software dient beveiliging tijdens de hele *lifecycle* van aanbesteding, via testen en implementatie, en wijzigingsbeheer tot aan afvoer en vernietiging meegenomen te worden.
29 https://www.surf.nl/binaries/content/assets/surf/nl/kennisbank/2013/juridisch-normenkader-cloudservices-hoger-onderwijs.pdf

[Bijlage H - Inrichting van CSIRT]

Commented [L.C.42]: Deze bijlage kan geheel vervallen indien er geen CSIRT is, of wordt voorzien.
CSIRT wordt ook wel CERT- Computer Emergency Response Team- genoemd. Of specifiek <instelling->CERT
Gebruik de afkorting die gewenst is .

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

De leden van het CSIRT zijn in die rol benoemd door het bestuur en opereren in haar opdracht. [De leden van het CSIRT zijn tevens onderdeel van het SOC van <naam instelling>.]

Het CSIRT stelt een handvest op waarin doelgroep, opdracht, bevoegdheden, escalaties, werkwijze (inclusief omgang met vertrouwelijkheid) en samenstelling zijn uitgewerkt. Daarin wordt o.a. vastgelegd dat het CSIRT voor <naam instelling> als geheel werkzaam is en haar opdracht direct van het bestuur van <naam instelling> krijgt. Ook worden directe escalaties naar het bestuursniveau (via de CISO) vastgelegd. Dit is [onderdeel van het algemene calamiteitenprotocol van <naam instelling>]. Ook worden directe contacten vastgelegd met de afdelingen c.q. personen die binnen <naam instelling> zorg dragen voor juridische kwesties en contacten met de pers.

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

Incidentbeheer en-registratie hebben betrekking op de wijze waarop medewerkers, studenten en derden inbreuken op de informatiebeveiliging melden en de wijze waarop deze worden afgehandeld. Van incidenten kan worden geleerd. Incidentregistratie en periodieke rapportage over opgetreden incidenten horen dan ook thuis in een volwassen informatiebeveiligingsomgeving. Incidenten kunnen bij <naam instelling> worden gemeld bij het <CSIRT/CERT>[30]-meldpunt: <...>[31]. <Naam instelling> heeft de contactgegevens van dit meldpunt duidelijk gecommuniceerd naar haar medewerkers, studenten en derden.

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

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

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

Commented [L.C.43]: Als er een SOC functie aanwezig is, dan zullen trends (ook) vanuit deze functie worden geconstateerd. Eventueel deze passage hierop aanpassen.

[30] <Computer Security Incident Response Team / Computer Emergency Response Team>
[Zie <Bijlage F / het CSIRT Charter/Operational Model] voor meer informatie]

[31] <Servicedesk>@<instelling.nl>, tel. +31 <12345678>