Raamwerk Strategisch Informatiebeveiligingsbeleid

Universiteit Leiden

Versie	1.0
Datum vastgesteld	2 april 2020
Auteur	Aram Segaar- *CISO Universiteit Leiden*

Verantwoording en gebruik

Het is bij verantwoordelijken van dit raamwerk strategisch bekend wat de actiepunten zijn ten behoeve van het verder ontwikkelingen van dit raamwerk. Het opnemen en verwerken van de actiepunten moet resulteren in een afgerond informatiebeveiligingsbeleid voor de Universiteit Leiden.

De actiepunten zijn opgenomen in een apart document dat wordt beheerd door het team security/privacy van de Universiteit Leiden. Het betreffende document is opgeslagen op de interne j-schijf waartoe medewerkers van de afdeling informatiemanagement toegang hebben.

SURF (SCRIPR)

Dit document kent zijn basis op het format van Strategisch Informatiebeveiligingsbeleid dat door SURF is ontwikkeld voor hogescholen en universiteiten. SURF biedt hiermee de mogelijkheid om een allesomvattend document op te stellen waarin alle facetten van informatiebeveiligingsbeleid zijn opgenomen. In het document zijn verwijzingen naar verschillende SURF documenten opgenomen. Het inzien van het SURF format informatiebeveiligingsbeleid is mogelijk.

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

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

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 Universiteit Leiden voorziet in adequate informatiebeveiliging en daarmee voldoet aan de relevante wet- en regelgeving. Met informatiebeveiliging wil Universiteit Leiden ook bijdragen aan een betere kwaliteit van de informatievoorziening en zorgen voor een juiste balans tussen functionaliteit, veiligheid en privacy.

Dit raamwerk voor strategische informatiebeveiliging geeft invulling aan het strategisch beleid dat voor de universiteit van toepassing is. Naast onderliggend strategisch beleid zal het raamwerk bestaan uit een tactisch- operationele toepassing op de universitaire organisatie met faculteiten en eenheden, een meerjarenprogramma en een business continuity plan.

In dit strategische deel wordt beschreven op wie, op welke onderdelen van de instelling en op welke apparaten en applicaties het beleid van toepassing is. Informatiebeveiliging werkt door in alle lagen van de organisatie. Naast de reikwijdte van het beleid worden de verantwoordelijkheden van de betrokken functionarissen beschreven. Het lijnmanagement is verantwoordelijk voor haar eigen processen, de directie zorgt ervoor dat beveiligingsmaatregelen daadwerkelijk worden geïmplementeerd. Eindverantwoordelijkheid ligt bij het College van Bestuur (CvB).

Vijf beleidsprincipes zijn leidend, namelijk:

Risico-gebaseerd
We baseren de maatregelen op de mogelijke veiligheidsrisico's van onze informatie, processen en IT-faciliteiten.

Iedereen
Iedereen is en voelt zich verantwoordelijk voor een juist en veilig gebruik van middelen en bevoegdheden.

Altijd
Informatiebeveiliging zit in het DNA van al onze werkzaamheden.

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.

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 Universiteit Leiden 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

Dit raamwerk voor strategische informatiebeveiliging legt de basis van het strategisch beleid dat voor de universiteit van toepassing is en dient als kader voor de tactisch- operationele toepassing op de universitaire organisatie met faculteiten en eenheden, een meerjarenprogramma en een business continuity plan. Dit raamwerk geeft een solide basis voor de verdere invulling het gehele informatiebeveiligingsprogramma. Met recente voorbeelden zoals de Maastricht aanval en de grote continuïteitsdruk ontstaan gedurende de COVID-19 pandemie is het des te meer van belang dit raamwerk te adopteren.

Het succes van Universiteit Leiden 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 schaden de beschikbaarheid, integriteit en vertrouwelijkheid van informatie beïnvloeden. Voorbeelden van bedreigingen zijn kwetsbaarheden in systemen of ongeautoriseerde toegang tot informatie. Dit kan bijvoorbeeld de waarde van een Universiteit Leiden diploma, behaalde cijfers of de legitimiteit van onderzoekconclusies ondermijnen. Ook de privacy[2] van studenten, medewerkers en gasten en de reputatie van Universiteit Leiden worden geschaad. Informatiebeveiliging is daarom van cruciaal belang.

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 Universiteit Leiden zich ook bewust worden van de risico's en hun handelen daarop afstemmen.

Informatieveiligheid is niet te bereiken door alleen een aantal technische en organisatorische maatregelen vast te stellen. Door de veranderende wereld is het een dynamisch proces. In dit document zijn om die reden vijf hoofdprincipes leidend voor informatiebeveiliging binnen de Universiteit Leiden. De vast te stellen maatregelen, procedures en richtlijnen kunnen getoetst worden aan de vijf hoofdprincipes die in hoofdstuk 3 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 heeft daarom nauwe samenhang met het Beleid Integrale Veiligheid, plan ISSC, positionpaper Privacy, Jaarbeeld 2019 en cyber actieplan 2020 van de Universiteit Leiden.

2. Wet- en regelgeving

Universiteit Leiden 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 Universiteit Leiden 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] Informatie over privacy en gegevensbescherming Universiteit Leiden zie:
https://www.medewerkers.universiteitleiden.nl/ict/privacy-en-gegevensbescherming?cf=bestuursbureau-expertisecentra&cd=bestuursbureau
[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.

Aangezien de eindverantwoordelijkheid voor informatieveiligheid bij het CvB rust, is in lijn daarmee dit raamwerk informatiebeveiligingsbeleid opgesteld.

3.2 Doelstelling, randvoorwaarden en uitgangspunten

Informatiebeveiliging heeft de volgende doelen:

- Het waarborgen van de beschikbaarheid van informatie van het onderwijs, onderzoek en de bedrijfsvoering.
- Het waarborgen dat informatie juist, volledig en actueel is (integriteit) en alleen toegankelijk is voor personen die vanuit hun rol/functie daar toegang tot mogen hebben (beschikbaarheid, integriteit en vertrouwelijkheid).
- Het voorkomen van beveiligings- en privacy-incidenten en de eventuele gevolgen hiervan verminderen.

Met het informatiebeveiligingsbeleid (IB-beleid) wil de Universiteit Leiden 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.

Universiteit Leiden heeft de ambitie om met behulp van dit beleidsdocument de informatieveiligheid structureel naar een hoger niveau te brengen waarbij niveau 3 van de SURF-normenkader als eerste referentiepunt dient. Dit doet zij door het beschrijven van verantwoordelijkheden, taken en bevoegdheden en wet- en regelgeving. Daarnaast is er de samenhang met een beleidscyclus en wordt dit tevens gewaarborgd en gecontroleerd in een Information Security Management System (ISMS).

Het IB-beleid, en de opvolging daarvan, moet Universiteit Leiden in staat stellen 'in control' en compliant te zijn. Op basis daarvan kunnen de betrokken decanen samen met het College van Bestuur verantwoording afleggen aan de Raad van Toezicht. 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 Universiteit Leiden 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. Hierbij vormt het 3 Lines of Defence (3LoD) model de basis voor de beveiligingsorganisatie. Met een juiste organisatorische inrichting worden beveiligingsfunctionarissen effectief in stelling gebracht voor het uitvoeren van hun werkzaamheden. Hiermee komt dus ook de CISO op een positie van waaruit effectief informatieveiligheid gerealiseerd kan worden.

- *Procesbenadering*
  Informatiebeveiliging is een continu proces. Periodiek worden er risicoanalyses en interne/externe audits uitgevoerd. De resultaten hiervan worden opgenomen in vastgestelde jaarplannen met duidelijke keuzes in beveiligingsmaatregelen. De uitvoering van deze beveiligingsmaatregelen wordt periodiek gecontroleerd in cyclische vorm. Hiervoor zijn de juiste mensen en middelen beschikbaar. Zo wordt het proces aangestuurd en in-control gehouden.

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 informatiebeveiligingsmanagementsysteem (ISMS[5], zie bijlage A) van Universiteit Leiden. 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 Universiteit Leiden. Universiteit Leiden 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]. Universiteit Leiden streeft naar een volwassenheidsniveau niveau 3 volgens de SURF-richtlijnen.
- *Maatregelen*
  Universiteit Leiden 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. Ook de eerder vastgestelde minimale maatregelen worden hierbij gehanteerd in lijn met ISO 27002.

3.3. Doelgroep

Het IB-beleid is bestemd voor iedereen die – intern of extern – te maken heeft met de bedrijfsprocessen van de Universiteit Leiden. Het beleid richt zich in eerste instantie op het bestuur, hoger management, de beveiliging van faculteiten en overige universiteitseenheden. 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 Universiteit Leiden wordt informatieveiligheid breed geïnterpreteerd. Het gaat over alle vormen van formeel vastgelegde informatie (dus niet alleen digitale informatie) zowel fysiek als logisch, 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 Universiteit Leiden kan aanspreken.

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

Voor onderzoek geldt dit ook. Aangeschafte middelen zoals onder anderen hardware en software als ook het gebruik hiervan zal aan de universiteit brede standaard moeten voldoen.

Universiteit Leiden faciliteert het gebruik van privéapparaten. Het gebruik van eigen apparatuur op onze netwerken voor toegang tot applicaties of informatie van de instelling valt ook onder dit IB-beleid.

---

[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

Het beleid is locatie-onafhankelijk: het geldt ook als men op een andere locatie dan op het terrein van Universiteit Leiden met informatie of informatievoorzieningen van Universiteit Leiden werkt (zoals thuis, in de trein of bij een andere onderwijsinstelling). Ook bij werken in het buitenland is dit beleid van toepassing, rekening houdend met lokale wet- en regelgeving en een eventueel ander dreigingsbeeld.

3.5. Kritieke processen en systemen

Een zevental processen en onderliggende systemen zijn vanwege hoge afhankelijkheid en kwetsbaarheid voor de operaties (functioneren) van de Universiteit Leiden aangewezen als kritieke processen en systemen. Ondanks dat deze processen in grote mate onveranderd blijven, blijft het essentieel om periodiek, gemeten op basis van Beschikbaarheid, Integriteit en Vertrouwelijkheid, risicoanalyses uit te voeren. Zowel de risicobereidheid als de dreigingen wordt op deze wijze bepaald en geborgd. De onderstaande tabel geeft de zeven kritieke processen weer in relatie tot de bijbehorende (highlevel) ondersteunende systemen.

Kritiek Proces	Ondersteunend Systeem
Onderwijs Logistiek	Student Informatie Systeem
Onderwijsondersteuning	Learning Management System
(Specifieke) Onderzoeksprocessen	Onderzoek specifieke Invulling
HR-processen	Personeelssysteem
Identiteitenbeheer	Indentitymanagement systeem
ICT-beheer processen	ICT-Basisinfrastructuur
Informatiebeveiligingsprocessen	Governance, Risk & Compliance-Tooling

4. Beleidsprincipes informatiebeveiliging

4.1. Inleiding

Universiteit Leiden 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[8] doelstellingen in het onderzoekdomein.] Adequate beveiliging van informatie is steeds een randvoorwaarde en het openstellen van informatie moet een bewuste keuze zijn. Het is van belang dat men binnen de Universiteit Leiden zich ervan bewust is dat het investeren in informatiebeveiliging geld kost.

Universiteit Leiden 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"[9].

Om tot een goede afweging te komen of vervangende maatregelen inderdaad tot een acceptabel restrisico leiden, wordt dit aan het IB-beleid van Universiteit Leiden getoetst. Met de beleidsprincipes en hun implicaties voor

[8] Findable – Accessible – Interoperable – Reusable (zie https://nl.wikipedia.org/wiki/FAIR-principes)

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

informatiebeveiliging uit dit hoofdstuk kan die toetsing plaatsvinden, ook al zijn vervangende maatregelen niet uitputtend in het beleid of in baselines vastgelegd.

4.2. Beleidsprincipes

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

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 Universiteit Leiden vastgestelde beleidsprincipes zijn:

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 Universiteit Leiden. 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 op basis van versleuteling.	

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 Universiteit Leiden op strategisch niveau veel aandacht aan afstemming van informatiebeveiliging, arbo-veiligheid, fysieke beveiliging, business-continuïteit en privacybescherming. Waar mogelijk en nodig vertaalt deze afstemming zich ook naar het tactische en operationele niveau. De governance rondom informatiebeveiliging wordt daarom in samenhang met Integrale Veiligheid toegepast (via Platform Veiligheid).

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

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 IB-Governance bij Universiteit Leiden is ingericht volgens het zogenaamde Three Lines of Defence model[10] (ook wel '3LoD'). Dit model wordt algemeen toegepast als model om Governance, Risk en Compliance (GRC) te borgen in een operationele organisatie. Het beschrijft niet alleen de rollen binnen de organisatiestructuur, maar ook hun onderlinge samenwerking.

5.2.1 Eerste en tweede lijn

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

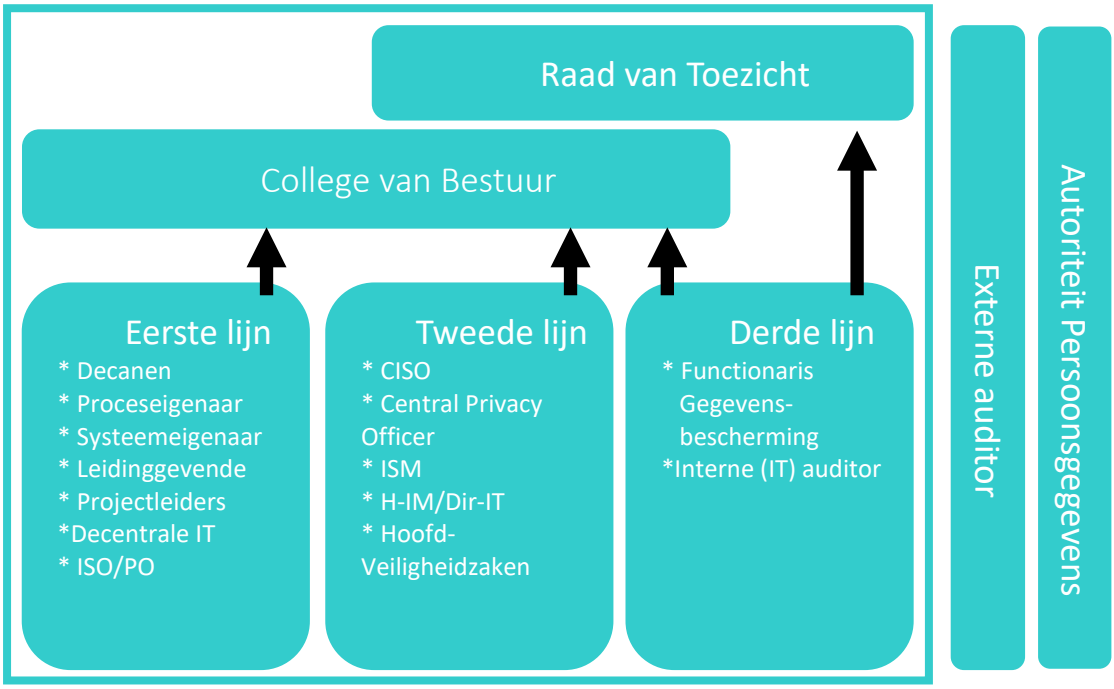
[10] https://www.icas.com/ca-today-news/internal-audit-three-lines-of-defence-model-explained

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 Interne Auditafdeling (AIC) behoren typisch tot de derde lijn. Beiden opereren volledig los van alle andere organisatieonderdelen en rapporteren niet alleen aan het CvB, maar ook aan de RvT.



Schema: Three Lines of Defence, vertaald naar rollen Universiteit Leiden

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

5.2.3 Eindverantwoordelijkheid

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

5.2.4 Taken, bevoegdheden, verantwoordelijkheden

De diverse taken, bevoegdheden en verantwoordelijkheden zijn onderverdeeld in Strategisch, Tactisch en Operationeel niveau. Deze drie niveaus kenmerken zich door hun overlegstructuur. De onderstaande tabel weergeeft de drie niveaus (volgende pagina).

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 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 zij samen met de CISO (vanwege de uniformiteit), de systeem- en proceseigenaren en de privacy organisatie.	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.

Niveau	Wat?	Wie?	Overleg	Documenten
Richtinggevend	Bepalen IB strategie. Organisatie t.b.v. IB inrichten. IB planning en control vaststellen. Business continuity management. Communicatie naar management en organisatie.	College van Bestuur, i.h.b. de portefeuillehouder IB, op basis van advies CISO en Hoofd IM. Portefeuillehouder IB bij faculteit/eenheid. Wetenschappelijk directeur. Onderwijs directeur.	College van Bestuur stelt vast. De CISO en ISO sluiten periodiek en naar behoefte aan bij bestuurlijke overleggen (faculteitsbesturen en OBV).	IB beleid. IB plan. Jaarbeeld IB. *Business continuity plan*.
Sturend	Planning & Control IB: - voorbereiden normen en wijze van toetsen - evalueren beleid en maatregelen - begeleiding externe audits Communicatie naar proceseigenaren.	Proces eigenaren. Leidinggevenden. CISO. ISO (faculteiten en eenheden). Hoofden Functioneel beheer. Wetenschappelijke data management support (datastuarts).	Voorbereiding van en advisering over beleid vindt plaats in het periodiek overleg met de ISO's faculteiten, eenheden en FB. Platform Veiligheid (samenwerking diverse disciplines op het gebied van veiligheid).	Risicoanalyses en audits in processen en projecten. SURF audit. Handreikingen IB maatregelen Gedragscode voor medewerkers en studenten. IB *baselines* (basismaatregelen). Jaarplan en –verslag faculteiten en eenheden. Procedures. Documentatie (bijv. over veilig werken, over processen etc.). Data management plan-model (wetenschappelijke

				data). Rapportage ISO aan facultair bestuur en aan CISO; volgt P&C cyclus (3 x per jaar).
Uitvoerend	Implementeren IB maatregelen. Registreren en evalueren incidenten. Communicatie eindgebruikers.	ISSC i.s.m. proces eigenaren. ISO (faculteiten en eenheden). CERT. Helpdesk ISSC. Ondersteuners voor wetenschappelijk onderzoek. Security deskundigen bij ISSC. ICT ondersteuners. Functioneel beheerders. Medewerkers. Studenten.	Operationeel IB overleg bij faculteiten, eenheden, teams. CERT overleg. Security overleg ISSC (technisch). Team of afdeling overleg (bij alle organisatie onderdelen).	SLA's en contracten met externe partijen. Werkinstructies en procedures IB. Technische documentatie en handreikingen. Incidentregistratie incl. rapportage en evaluatie. Gedragscodes (voor medewerkers en studenten). Data Management Plan (wetenschappelijk onderzoek).

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 Universiteit Leiden gestructureerd overleg gevoerd over het onderwerp informatiebeveiliging op diverse niveaus.

Strategisch	Tactisch	Operationeel
Op strategisch niveau wordt richtinggevend gesproken over governance en compliance, alsmede over doelen, scope en ambitie op het gebied van informatiebeveiliging, in samenhang met privacy. Dit gebeurt in het bestuur, geadviseerd door Hoofd IM, Directeur ICT, de CISO, Hoofd Veiligheidszaken en de FG. Dit is afgestemd op de IT-strategie en de risicobereidheid van Universiteit Leiden.	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, CPO en ISO's. Waar nodig in overleg met overige betrokken functionarissen zoals de 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.

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 Universiteit Leiden te maken kan krijgen, zoals financieel, personeel en commercieel.

Dat betekent bij Universiteit Leiden dat informatiebeveiliging op de agenda staat van het CvB vanuit de benadering van integrale veiligheid. Op tactisch niveau zal het ook gaan over keuze van IT-functionaliteit en-services op de agenda van het IM-overleg. Op operationeel niveau staat informatiebeveiliging op de agenda van overleggen tussen onder anderen IT-ondersteuners, functioneel beheerders en IT-beheerders, maar ook op overleggen met key-users en projectteams.

Documenten

Voor informatiebeveiliging wordt bij Universiteit Leiden dezelfde (PDCA-)managementcyclus gevolgd, die ook voor andere onderwerpen geldt: visie/idee, beleid, analyse, plan implementatie, uitvoering, controles en evaluatie. Die cyclus wordt op de verschillende niveaus ondersteund door een aantal formeel vastgestelde documenten. In bijlage G is een uitgebreider overzicht opgenomen van de documenten die Universiteit Leiden 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 Universiteit Leidenwerken 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.

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 ISO's. Bewustwording is een onderdeel van het verplichte introductieprogramma voor nieuwe medewerkers en studenten. Dit wordt versterkt met de realisatie van een (integrale) beveiligingsgeoriënteerde cultuur en werkomgeving.

5.4. Controle, oefenen, naleving en sancties

Bij Universiteit Leiden is de Interne Auditafdeling verantwoordelijk voor de (planning van) interne IT-audits en de CISO voor de controle op de uitvoering van de informatiebeveiligingsjaarplannen. De ISO's ondersteunen daarbij. De uitvoering wordt belegd door de Interne Auditafdeling (AIC) samen met Informatiemanagement en het CERT.

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 zoals OZON & NOZON[11].

Audits

De informatiesystemen (of-processen) van Universiteit Leiden 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.

Normen

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.

[11] Deze worden door SURF gecoördineerd.

Naleving en opvolging

Universiteit Leiden neemt deel aan de SURF-audit selfassessment cyclus en de bijbehorende tweejaarlijkse benchmark. Minimaal eens per 2 jaar wordt ook een SURF Peerreview aangevraagd.

De bevindingen van de interne en externe controles en mogelijke externe eisen met betrekking tot beveiliging, zijn input voor de nieuwe jaarplannen van Universiteit Leiden. 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.

Sancties

Als uit de controles blijkt dat de naleving ernstig tekortschiet, dan kan Universiteit Leiden de betrokken verantwoordelijke medewerkers of studenten een sanctie opleggen conform bepalingen zoals opgenomen in de Regeling ICT- en Internetgebruik Universiteit Leiden 2020[12]. 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 leidinggevende decaan.

5.5. Financiering

Financiële middelen voor informatiebeveiliging worden structureel opgenomen in de diverse (project)begrotingen. De financiering van informatiebeveiliging wordt bij Universiteit Leiden 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. Wanneer er een acute dreiging ontstaat waarbij buiten de reguliere cyclus om financiële middelen nodig zijn, zal ook hier centraal invulling aan gegeven worden[13].

Decentraal

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

6. Melding en afhandeling van incidenten

Een incident is een gebeurtenis 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.

Wij leren van incidenten. Incidentregistratie en periodieke rapportage over opgetreden incidenten horen dan ook thuis in een volwassen informatiebeveiligingsomgeving.

[12] https://www.medewerkers.universiteitleiden.nl/binaries/content/assets/ul2staff/reglementen/ict/regeling-ict-en-internetgebruik-2019.pdf

[13] Ten tijde van dit schrijven is als voorbeeld te noemen Actieplan Cyber 2020

Iedere medewerker, student en derde is verantwoordelijk voor het signaleren en melden van incidenten en inbreuken op de informatiebeveiliging, inclusief datalekken. Incidenten moeten gemeld worden via de Helpdesk ISSC of direct bij het CERT[14]. Het CERT handelt de meldingen af en registreert deze voor evaluatie.

Er is een door het College van Bestuur vastgesteld beleid voor Responsible Disclosure[15]. Daarmee geeft Universiteit Leiden mogelijke melders van kwetsbaarheden in de informatiesystemen een garantie dat Universiteit Leiden, onder voorwaarden, geen juridische stappen tegen hen onderneemt.

7. Vaststelling & wijziging

Het College van Bestuur stelt, het IB-beleid vast dat de Corporate Information Security Officer (CISO) voorstelt. Het IB-beleid volgt de kaders van het instellingsplan en sluit aan bij de ICT Strategie en het Instellingsbeleid Integrale Veiligheid. Het wordt 1x per 2 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.

Versie en datum

Dit raamwerk, versie <versienummer>, is vastgesteld door het bestuur van Universiteit Leiden op <datum> en kan worden aangehaald als “Raamwerk Strategisch Informatiebeveiligingsbeleid van Universiteit Leiden”.

[14] Computer Emergency Response Team

[15] https://www.medewerkers.universiteitleiden.nl/ict/privacy-en-gegevensbescherming/veilig-digitaal-werken/incidenten-melden/bestuursbureau-expertisecentra/bestuursbureau?cf=bestuursbureau-expertisecentra&cd=bestuursbureau

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 de Universiteit Leiden, en meer in detail in de safety/privacy jaarplannen.

Door herhaling van de PDCA-cyclus werkt de organisatie doorlopend aan het verbeteren van het ISMS en is daardoor meer 'in control'. Een schematische weergave van de PDCA-cyclus is op de volgende pagina weergegeven.

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 eronder en wat doet niet mee;
- Leiderschap en commitment, zonder welke informatiebeveiliging in een organisatie niet serieus genomen kan worden.

Vervolgens moet het ISMS opgesteld worden.

De PDCA-cyclus omvat de volgende 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

Act

Op basis van de uitkomsten van de checkfase worden verbeteringen doorgevoerd

Check

De checkfase omvat de evaluatie van de werking van het ISMS:

- bewaking, meting, analyse en evaluatie
- interne audit
- management review

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 Universiteit Leiden. 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[16] uitgevoerd. • De risico's worden ingeschat en vastgesteld op basis van een risicoclassificatie (zie hiervoor Bijlage C). • Universiteit Leiden stelt een Classificatie Richtlijn vast. • Een gegevensbeschermingseffect beoordeling (DPIA – Data Protection Impact Assessment) in het kader van de AVG maakt waar nodig onderdeel uit van de risicoanalyse. • Waar nodig worden maatregelen getroffen om het vastgestelde risico op Beschikbaarheid, Integriteit en Vertrouwelijkheid te brengen naar het geaccepteerde niveau. • Informatie heeft één eigenaar. • Eigenaren van informatie, informatiesystemen, applicaties en processen zijn verantwoordelijk voor de implementatie en operationele handhaving van maatregelen onder het principe van "Pas toe of leg uit". • Afwijkingen kunnen worden geaccepteerd binnen de risicobereidheid (risk-appetite) van Universiteit Leiden, 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. • 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.	

[16] 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].

	• Universiteit Leiden 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 Universiteit Leiden is een zogenaamde Acceptabel Use Policy (AUP) beschikbaar die is gepubliceerd via de website van Universiteit Leiden. Deze AUP is van toepassing op zowel studenten, medewerkers als derden (zie hiervoor regelementen). • Het veilig omgaan met informatie en informatiedragers is een onderdeel van de aanstelling van alle medewerkers. • Informatiebeveiliging krijgt aandacht bij indiensttreding van medewerkers en bij 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, zie hiervoor 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 Universiteit Leidenrond toegang en gebruik van IT-middelen. • Periodiek worden accounts met hoge privileges gevalideerd. • Universiteit Leiden organiseert regelmatig cybersecurity-awareness activiteiten voor de diverse doelgroepen: studenten, medewerkers, leidinggevenden en partners van Universiteit Leiden. • 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 Universiteit Leiden te bepalen en periodiek bij te stellen. Nieuwe dreigingen leiden waar nodig tot aanpassing van maatregelen.

4

Security by Design

Integrale aanpak informatiebeveiliging

Kern	Informatiebeveiliging is vanaf de start een integraal onderdeel van ieder project of iedere verandering m.b.t. 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.

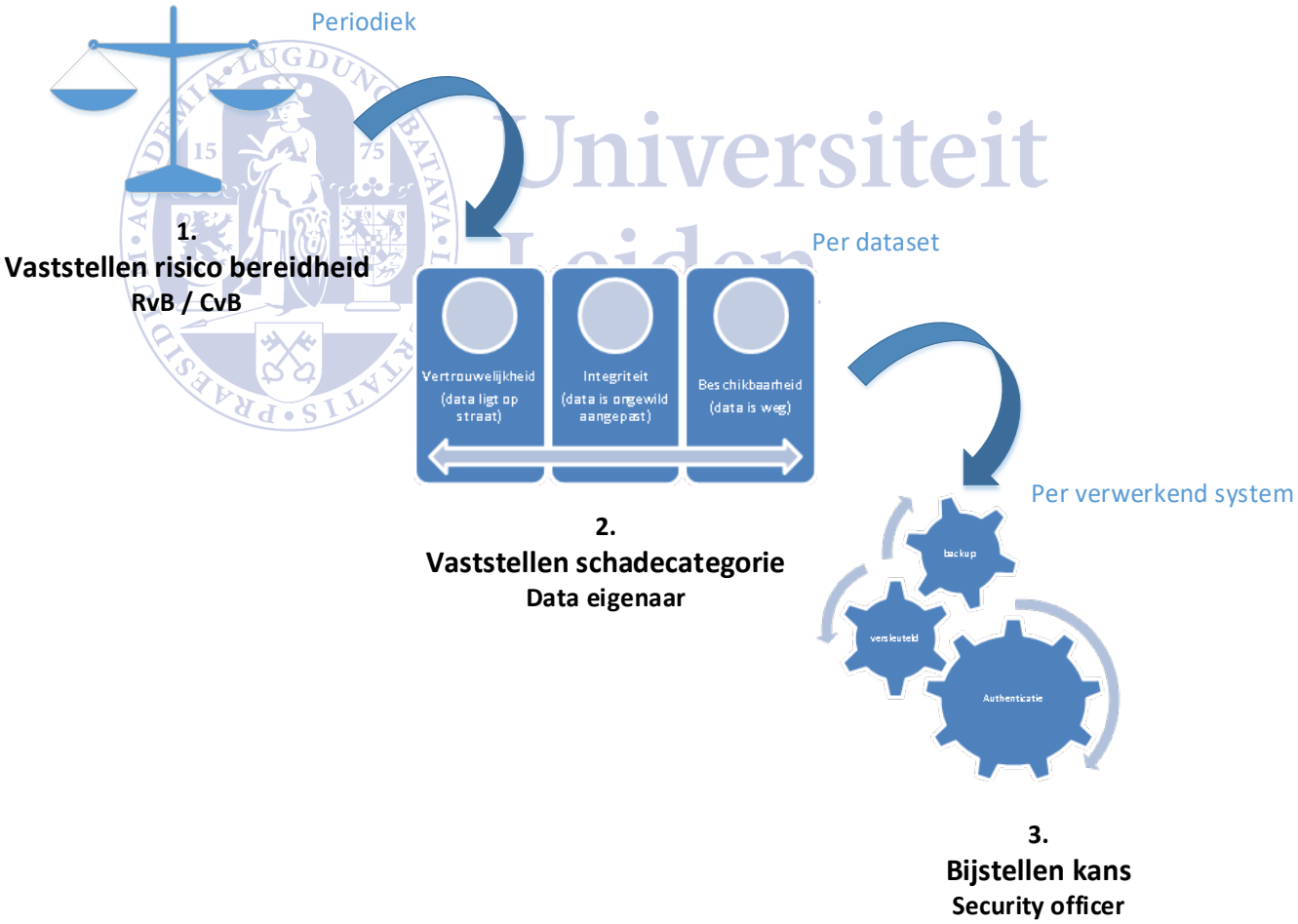
Bijlage C – Classificatie

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 efficiënt of gebruiksvriendelijk om niet-vertrouwelijke informatie op dezelfde manier te beschermen als vertrouwelijke informatie.

Universiteit Leiden volgt een risico gestuurde aanpak. Het 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. Het proces van classificatie ziet er als volgt uit:

Procesweergave



1. Risico bereidheid

Met een risicoanalyse kan de mogelijke schade worden geëvalueerd die een dreiging kan toebrengen aan specifieke informatie (bijv. misbruik door oneigenlijke toegang, ongeautoriseerde toegang) en wat de kans is dat die schade optreedt. Het gebruik van standaard risicoanalysehulpmiddelen is vaak een tijdrovend en abstract traject.
Niet alle risico' s hoeven gemitigeerd te worden. Universiteit Leiden 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 Universiteit Leiden 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 Universiteit Leiden 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 maatschappelijk	Langdurige verstoring van een groot deel van het onderwijs op een of meer instituten.	Publicatiebeperkingen, reputatieschade aan onderzoeker of instelling, patenten of contractuele afspraken	Directe schade tussen €250.000 en €1.500.000

	gevoelige werkzaamheden (zoals dierproeven).			
Ontwrichtend	Aanhoudende negatieve berichtgeving in de landelijke/international e 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)

2. Bepalen schade / waarde

De eigenaar van de data heeft de eindverantwoordelijkheid voor de uitvoering van het inschatten van de waarde/schade en het selecteren van een gepast systeem om de data te verwerken. Schade kan worden veroorzaakt door de data kwijt te raken, maar ook door dat de data onbetrouwbaar is geworden of boetes vanwege onzorgvuldige omgang. De waarde van de data is het financiële gewin voor een derde als ongeautoriseerde toegang tot de data kan krijgen.

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

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

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

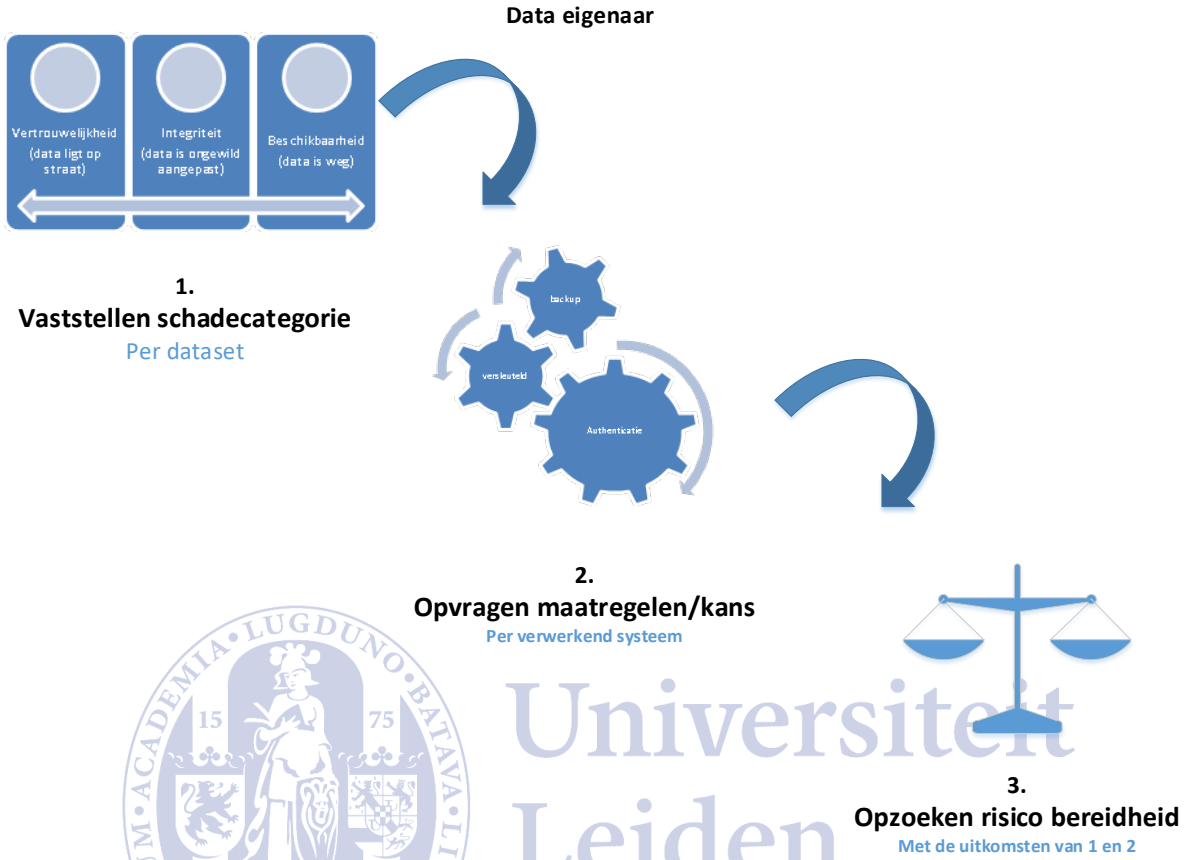
Onderstaande tabel geeft een handvat voor het inschatten van de schade:

Tabel 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.

Leiden

Proces gezien vanuit de data-eigenaar



Universiteit Leiden

Toelichting:

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.

3. Bepalen maatregelen/kansen

De CISO 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[17], 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[18]. Bijlage C van het SURF juridisch normenkader (cloud)diensten bevat de “Handreiking Beveiligingsmaatregelen”. Deze handreiking bevat voornamelijk maatregelen uit ISO 27002 die zowel gaan over de governance van bij de leverancier van de dienst, als technische eisen die gesteld worden aan het

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

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

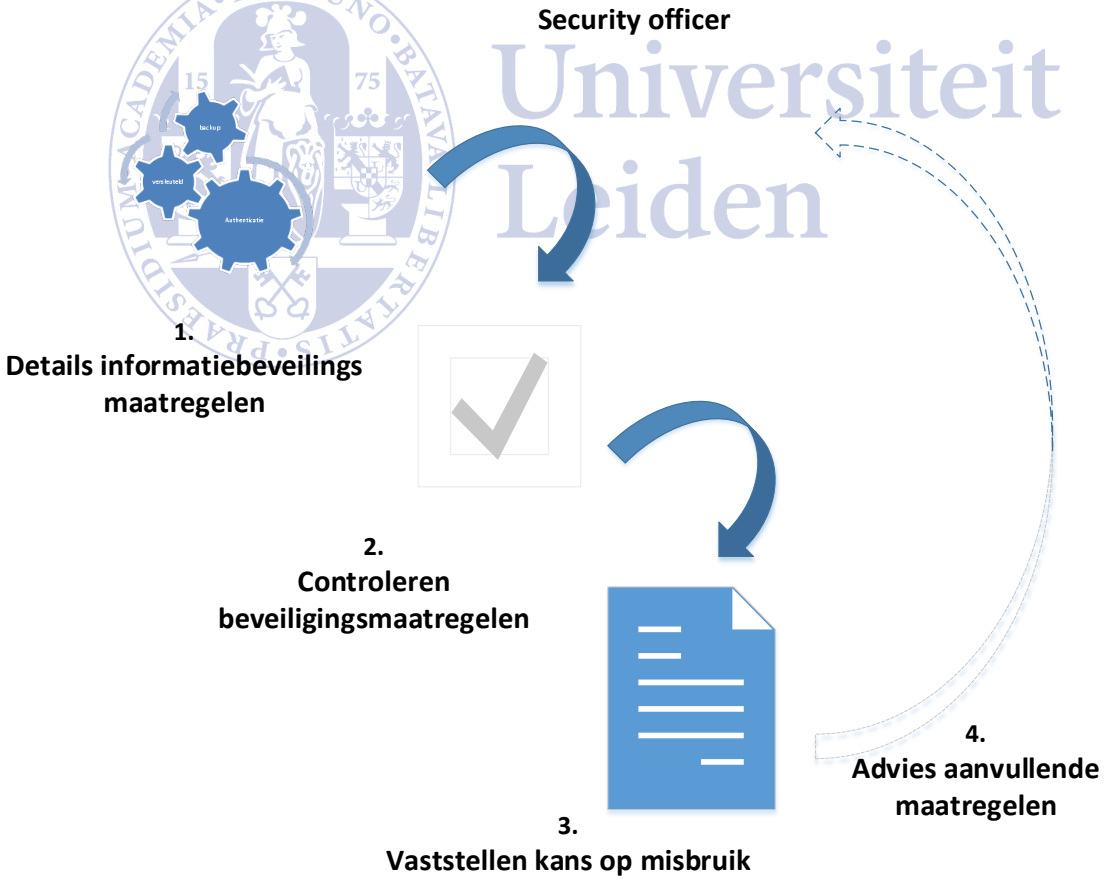
systeem dat de dienst levert. Implementatie van de maatregelen voor 'laag' en 'midden' of compenserende maatregelen die hetzelfde doel halen geeft een systeem een goede weerbaarheid.

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 systeemeigenaar



Toelichting:

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.

Universiteit Leiden

Bijlage D - Wet- en regelgeving

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

1. Wet op het Hoger onderwijs en Wetenschappelijk onderzoek (WHW)
   Universiteit Leiden 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 in het positionpaper Privacy vastgesteld waarin naleving van de AVG wordt geborgd. Naleving van het informatiebeveiligings- en gegevensbeschermingsbeleid inclusief de daarin vermelde technische en organisatorische maatregelen zorgen samen voor het voldoen aan de AVG.

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

4. Auteurswet
   Universiteit Leiden respecteert auteursrechten en handelt daarnaar.

5. Telecommunicatiewet / Wet Netneutraliteit
   Omdat de doelgroep van Universiteit Leidenvoldoende afgebakend is worden de netwerkvoorzieningen van Universiteit Leiden 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.

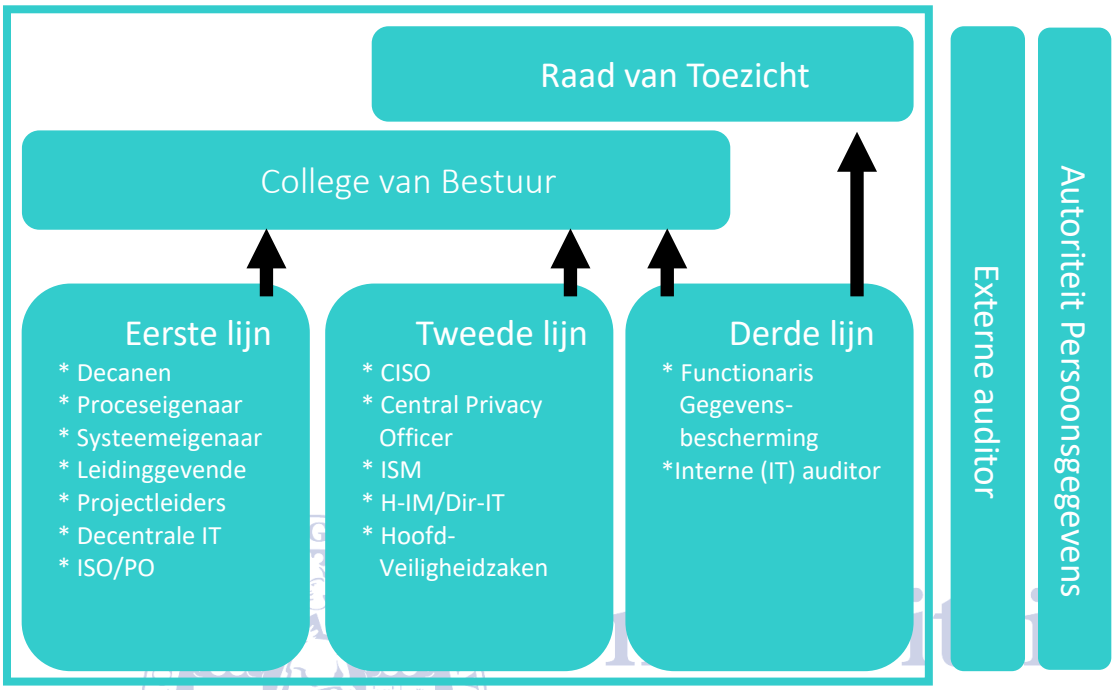
6. Wet Computercriminaliteit III
   De Wet Computercriminaliteit richt zich op de strafrechtelijke probleemgebieden in relatie tot het computergebruik. De wet bestaat uit artikelen die op diverse plekken zijn toegevoegd aan het Wetboek van Strafrecht. De extra artikelen houden zich bezig met:
   - Vernieling 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 Universiteit Leiden een adequaat basisniveau van beveiliging heeft tegen deze dreigingen. Indien er aanvallen op Universiteit Leiden plaatsvinden die de beveiliging significant doorbreken en die vallen onder de Wet Computercriminaliteit, zal het bestuur van Universiteit Leiden aangifte doen.

7. Overige codes en landelijke afspraken
   Het informatiebeveiligingsbeleid bij Universiteit Leiden is gebaseerd op het SURF Normenkader en de instelling is deelnemer in de VSNU. Universiteit Leiden is in dit kader gehouden aan de volgende codes en landelijke afspraken:
   - Code goed bestuur universiteiten.
   - Nederlandse gedragscode wetenschappelijke integriteit.
   - Juridisch Normenkader Hoger Onderwijs.
   - Aankomende gedragscode privacy is in onderzoek (vsnu)

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.



Toelichting:

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

De inhoudelijke verantwoordelijkheid voor zover het de digitale informatiebeveiliging betreft is door de portefeuillehouder 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 proceseigenaren.

Functionaris Gegevensbescherming (FG)
De FG houdt binnen Universiteit Leidentoezicht op de toepassing en naleving van de AVG, zoals beschreven in het privacy-beleid van Universiteit Leiden. De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie in de instelling.

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

Chief Information Security Officer (CISO)

De CISO is een functie op strategisch (en tactisch) niveau. De CISO adviseert aan het bestuur en heeft direct toegang tot het bestuur en is zelf geen lijnverantwoordelijke. Zijn/Haar taak is te waken over IB-beleid. Tevens het jaarplan en jaarverslag op te stellen, lastige vragen te stellen, auditing-agenda voor te bereiden en overkoepelend beleid en aanbevelingen te formuleren.

De CISO formuleert het beveiligingsbeleid, helpt bij een juiste vertaling daarvan naar instellingsonderdelen, ziet toe op de (uniforme) naleving ervan en rapporteert gestructureerd over voortgang van plan.

De CISO heeft de bevoegdheid om onderzoek te doen of laten doen (audits) en informatie op te vragen en in principe ook te krijgen, tenzij privacy in het geding is – in alle bijzondere gevallen beslist het bestuur. De CISO kan zowel gevraagd als ongevraagd van advies dienen.

De CISO adviseert in complexe beveiligingsvraagstukken, initieert en stimuleert risicoanalyses en security audits en organiseert bedrijfsbrede security awareness. De CISO rapporteert (via de lijn: het hoofd informatiemanagement en de directeur Bedrijfsvoering van het Bestuursbureau) aan het College van Bestuur. In uitzonderlijke situaties en indien nodig heeft CISO direct toegang tot portefeuillehouder IB in het CvB.

Information Security Manager (ISM)

De ISM vervult een rol bij de vertaling van de strategie naar tactische (operationele) en technische plannen en maatregelen. Dit doet de ISM samen met de CISO en met de systeem- en proceseigenaren. Tevens adviseert de ISM over specifieke informatiebeveiligingsmaatregelen, bijvoorbeeld in projecten, bij acquisities van software of hardware, etc. Ook vervult de ISM binnen Universiteit Leiden de rol van CERT-Coördinator. De ISM heeft Directeur IT als hiërarchisch leidinggevende. Naast de ISM zijn er decentraal meer functionarissen met de rol Information Security Officer. Deze functionarissen vertalen de centraal vastgestelde maatregelen en operationele plannen door naar de decentrale organisatie.

Information Security Officer

De ISO binnen faculteit/eenheid vervult een rol bij de vertaling van de strategie naar tactische en operationele plannen en vormt daarmee de verbindende schakel tussen het strategische niveau waarop de CISO opereert, en de dagelijkse inrichting en uitvoering van informatiebeveiliging. Dit doet hij/zij samen met de CISO en met de proceseigenaren. Tevens adviseert de ISO over specifieke informatiebeveiliging maatregelen in projecten.

Alle organisatieonderdelen kennen een functionaris met de rol ISO. De ISO is binnen de faculteit of eenheid het aanspreekpunt voor informatiebeveiliging vraagstukken en daarbij is hij verantwoordelijk voor de implementatie van het informatiebeveiligingsbeleid en de minimale maatregelen. Hiertoe behoort het (laten) uitvoeren van risico-analyses voor informatiesystemen, het opstellen van plannen en de coördinatie van de uitvoering ervan, opstellen van de informatiebeveiligingsrapportages en zorg dragen voor de vergroting van het beveiligingsbewustzijn. Verder signaleert de ISO de incidenten die zijn voortgedaan en adviseert hoe ze op te lossen.

Voor de activiteiten op het gebied van wetenschappelijk onderzoek wordt ondersteuning georganiseerd per faculteit en/of instituut, waarbij deze ondersteuner ook de rol van Information Security Officer heeft (ondersteunt bij informatiebeveiliging vraagstukken in het wetenschappelijk onderzoek). ISO's binnen faculteit (vanuit diverse instituten en diverse aandachtsgebieden) werken samen en coördineren hun werkzaamheden.

Information Security Officer is een rol, waarbij de functionaris rapporteert aan de portefeuillehouder informatiebeveiliging binnen eigen organisatie(onderdeel). Deze rol kan worden toegekend aan informatiemanager, research data stuart, of een andere lid van de staf van het organisatorische onderdeel. Het is van belang om de invulling aan te sluiten op de benodigde capaciteit. Er kan decentraal, per organisatorische eenheid of faculteit, meer dan één functionaris zijn met de rol Information Security Officer.

Voor concern-systemen, die in centraal beheer zijn, vervullen de Hoofden Functioneel Beheer de rol van ISO, ieder voor hun eigen werkgebied. Daarbij is één van de taken de uitvoering van risicoanalyses op de concern systemen. De CISO wordt ingelicht als de minimale maatregelen van de operationele concern systemen niet worden nageleefd.

Universiteit Leiden

Central Privacy Officer (PO)

De Central Privacy Officer houdt zich binnen Universiteit Leiden centraal bezig met de toepassing en naleving van de AVG. In sommige gevallen in samenwerking met de CISO of een 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 Gegevensbeschermingseffect beoordeling (DPIA) of bij het afsluiten van verwerkersovereenkomsten in het kader van de AVG.]

Proceseigenaar

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

Hoofd Veiligheidszaken

Hoofd Veiligheidszaken is verantwoordelijk voor een breed scala van beveiliging onderwerpen, waaronder fysieke beveiliging, terrorisme dreigingen, afwijkend gedrag e.d.
In het kader van Integrale veiligheid werken de CISO en de Hoofd Veiligheidszaken samen.
Waar wenselijk en mogelijk wordt brede afstemming vertaald naar het tactische en operationele niveau, maar alleen daar waar het toegevoegde waarde biedt. Hiervoor is de Platform Veiligheid opgericht, waarvan het hoofd beveiliging de voorzitter is.

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.

Universiteit Leiden

Bijlage F - Documenten informatiebeveiliging

Voor informatiebeveiliging wordt bij Universiteit Leiden 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 Universiteit Leidende volgende documenten:

1. *Het Raamwerk IB-beleid*
   Het Raamwerk IB-beleid ligt ten grondslag aan de aanpak van (digitale) informatiebeveiliging binnen Universiteit Leiden. 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*
   Deze baseline beschrijft de maatregelen die minimaal nodig zijn om het voor Universiteit Leiden 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 ISM en ISO'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 CERT (zie hoofdstuk 6. Melding en afhandeling van incidenten (CERT).
   - Operational model van het CERT.
   - Privacy Beleid.
   - Richtlijn Authenticatie (inclusief wachtwoordbeleid.
   - Richtlijn Autorisatie.
   - Toepassing van cryptografische hulpmiddelen.
   - Richtlijn responsible disclosure.
   - IT Lifecycle management[19].
   - Integriteits-/gedragscode voor ICT-functionarissen.

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

Daarnaast is informatiebeveiliging een vast onderdeel van de volgende documenten:

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 informatie-beveiligingsparagraaf waarin de verantwoordelijkheden van de leverancier zijn opgenomen. De basis hiervoor is het SURF Juridisch Normenkader Cloudservices Hoger Onderwijs[20] die een informatiebeveiliging bijlage bevat.

Universiteit Leiden

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

Bijlage H - Inrichting van Computer Emergency Response Team- ISSC

Het doel van het Computer Emergency Response Team (CERT) is het voorkomen van informatiebeveiligingsincidenten en ze te bestrijden als ze zich toch voordoen. Het doel is de continuïteit van Universiteit Leiden te ondersteunen en haar reputatie te beschermen. Het CERT houdt zich ook bezig met beveiligingsincidenten buiten Universiteit Leiden als daar eigen medewerkers in enige rol bij betrokken zijn. Het CERT werkt hiervoor samen met een extern gecontracteerd Security Operations Centre (SOC). In zulke gevallen wordt als dat mogelijk is, gebruikgemaakt van de diensten van SURFcert, die wereldwijd in verbinding staat met andere CERT's en CSIRT's.

De leden van het CERT zijn in die rol benoemd door de Directeur-IT en opereren in opdracht van het bestuur. De leden van het CERT zijn allen werkzaam bij het ISSC.

Het CERT 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 CERT voor Universiteit Leiden als geheel werkzaam is en haar opdracht direct van het bestuur van Universiteit Leiden krijgt. Ook worden directe escalaties naar het bestuursniveau (via de CISO) vastgelegd. Ook worden directe contacten vastgelegd met de afdelingen c.q. personen die binnen Universiteit Leiden zorgdragen voor juridische kwesties, privacyvraagstukken (CPO of FG) en contacten met de pers.

Het CERT 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 Universiteit Leiden worden gemeld bij het CERT via de Helpdesk ISSC[21]. Universiteit Leiden heeft de contactgegevens van dit meldpunt duidelijk gecommuniceerd naar haar medewerkers, studenten en derden.

Elke medewerker, student en derde is zelfverantwoordelijk 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 Universiteit Leiden mogelijke melders van veiligheidsgaten in de informatiesystemen een garantie dat Universiteit Leiden, 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 Universiteit Leiden in gevaar zijn, wordt het incident ook met het bestuur besproken. Als er verontrustende trends worden geconstateerd, dan speelt Universiteit Leiden hierop in door het nemen van extra maatregelen of het creëren van bewustwording binnen de organisatie. Ook het SOC werkt daar actief aan in samenwerking coördinatie met het CERT.

[21] helpdesk@issc.leidenuniv.nl, tel. +31 71 527 8888