Strategisch beleid informatieveiligheid

2023-2027

Universiteit Leiden

Vastgesteld: CvB 10.06.2023

INHOUDSOPGAVE

SAMENVATTING 3
1. INLEIDING 4
1.1 Het belang van informatieveiligheid 4
1.2 Doel van het beleid 4
1.3 Reikwijdte van het beleid 5
1.4 Opzet van het beleid - kapstokmodel 5
1.5 Geldigheid & verantwoordelijkheid van het beleid 6
1.6 Leeswijzer 6
2. INFORMATIEVEILIGHEID 7
2.1 Wat is informatiebeveiliging 7
2.2 Relatie met privacy en gegevensbescherming 7
2.3 Digitale dreigingen 7
2.4 Visie 8
2.5 Strategie en doelen op het gebied van digitale weerbaarheid 8
2.6 Risico gebaseerde benadering 9
2.7 Wet- en regelgeving 9
3. PRINCIPES EN BELEIDSREGELS 10
3.1 Strategische principes 10
3.2 Beleidsregels 11
4. ORGANISATIE VAN INFORMATIEVEILIGHEID 13
4.1 Three Lines Model 13
4.2 Overleg- en rapportagestructuren 15
5. RANDVOORWAARDEN 16
6. NALEVING EN EVALUATIE 17

Samenvatting

Het succes van de Universiteit Leiden hangt steeds meer af van informatie, nieuwe technologieën en computersystemen. Die informatie moet goed worden beveiligd, zeker als er persoonsgegevens worden opgeslagen. In voorliggend document is verwoord op welke manier de Universiteit Leiden voorziet in adequate informatiebeveiliging en daarmee voldoet aan de relevante wet- en regelgeving.

Met dit strategisch informatiebeveiligingsbeleid wil de Universiteit Leiden 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 Universiteit Leiden 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. De eindverantwoordelijkheid ligt bij het College van Bestuur.

Vijf beleidsprincipes zijn leidend, namelijk:

1. *Informatiebeveiliging is risicogestuurd*
   We baseren de maatregelen op de mogelijke veiligheidsrisico's van onze informatie, processen en IT-faciliteiten.

2. *Informatiebeveiliging is een verantwoordelijkheid van iedereen*
   Iedereen is en voelt zich verantwoordelijk voor een juist en veilig gebruik van middelen en bevoegdheden. Beleid en technische maatregelen zijn niet voldoende om risico's op het terrein van informatiebeveiliging uit te sluiten. De mens zelf creëert de grootste risico's. We werken daarom voortdurend aan het vergroten van het beveiligingsbewustzijn om kennis van risico's te verhogen en veilig en verantwoord gedrag aan te moedigen

3. *Informatiebeveiliging is een continu proces*
   Informatiebeveiliging zit in het DNA van al onze werkzaamheden. Informatiebeveiliging is een continu proces, waarbij we steeds kijken naar mogelijke verbeteringen. Dit gebeurt onder andere door jaarplannen, controles en bijsturing.

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.

Op basis van onderzoek wordt de naleving van het beleid gemonitord en geëvalueerd. Hierover wordt gerapporteerd aan het College van Bestuur. Op basis van deze bevindingen worden verbetermaatregelen getroffen om de effectiviteit en doelmatigheid van informatiebeveiliging continu te optimaliseren.

1. Inleiding

Kwaliteit en betrouwbaarheid van informatie zijn een voorwaarde voor de Universiteit Leiden met haar toonaangevende onderwijs en onderzoek in de samenleving (zie Strategisch plan Universiteit Leiden 2022-2027). Verdergaande digitalisering, informatisering en ketenintegratie binnen de domeinen Onderwijs, Onderzoek en de Bedrijfsvoering vereisen een betrouwbare informatievoorziening, waarbij de informatieveiligheid op orde is en die compliant is aan de geldende wetgeving.

We kunnen niet meer zonder het digitaal verzamelen, vastleggen en delen van informatie met zowel interne als externe partners, collega's en studenten. Daarnaast is de Universiteit Leiden zich bewust van de toenemende dreiging van cybercriminaliteit en statelijke actoren. Daarom vindt het College van Bestuur informatieveiligheid van essentieel belang in een tijd van digitalisering en ketenafhankelijkheid. Met dit strategisch beleid geeft het College van Bestuur richting om de informatieveiligheid adequaat te borgen.

1.1 Het belang van informatieveiligheid

Informatie is één van de belangrijkst bedrijfsmiddelen voor de Universiteit Leiden voor de domeinen Onderzoek, Onderwijs en de Bedrijfsvoering. Toegankelijke en betrouwbare informatie is essentieel voor een universiteit. Te allen tijde moeten studenten, onderzoekers, medewerkers (waaronder docenten) en (keten)partners op een betrouwbare informatievoorziening en op een zorgvuldig beheer van (hun persoons) gegevens kunnen rekenen.

Informatieveiligheid behoort standaard onderdeel te zijn van alle processen binnen de domeinen van Onderzoek, Onderwijs en de Bedrijfsvoering. Naast een overzicht van potentiële informatierisico's voor de genoemde domeinen, is het essentieel om inzicht te hebben van de consequenties (impact) als deze risico's manifest worden. Informatierisico's vormen namelijk een bedreiging voor de kwaliteit en continuïteit van processen en voor het behalen van onze strategische doelen.

Deze bedreigingen schaden de beschikbaarheid, integriteit en vertrouwelijkheid van de informatie. Voorbeelden van bedreigingen zijn digitale inbraak (een hack), diefstal van informatie of kennis, het ongewenst wijzigen van informatie of het gijzelen van informatie met behulp van ransomware. Met het mogelijke gevolg dat de waarde van een Universiteit Leiden diploma, behaalde cijfers of de legitimiteit van onderzoekconclusies worden ondermijnd. Het kan tevens leiden tot discontinuïteit van (bepaalde) processen, reputatieschade of financiële schade. Maar ook kan de privacy van studenten, medewerkers, onderzoekers en andere personen worden geschaad. Het adequaat beveiligen van informatie is daarom van cruciaal belang.

1.2 Doel van het beleid

Het College van Bestuur geeft met dit beleid richting aan de wijze waarop de organisatie weerbaar moet zijn tegen de risico's die de actuele trends en ontwikkelingen met zich meebrengen op het gebied van informatieveiligheid. Dit beleid stelt de organisatie in staat om de betrouwbaarheid van de informatie(voorziening) te borgen en weerbaar te zijn tegen deze dreigingen.

1.3 Reikwijdte van het beleid

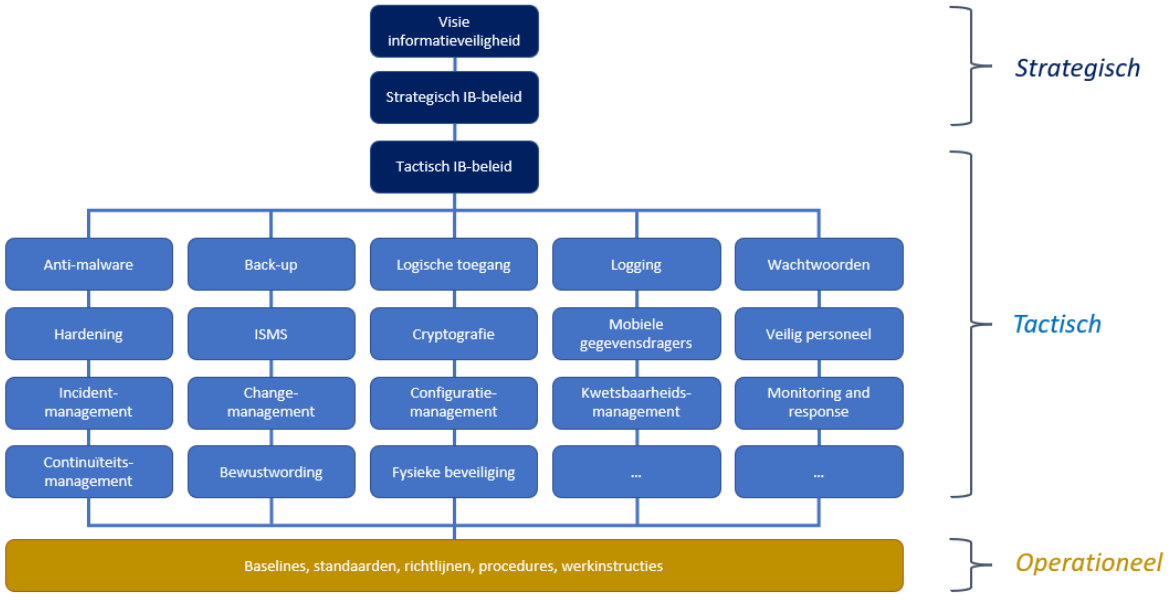
- Het beleid is van toepassing op alle onderdelen van de Universiteit Leiden. Als ook op de (gegevensverwerkings)processen waar wij verantwoordelijk voor zijn, gedeelde verantwoordelijkheid[1] in dragen, die zijn uitbesteed, ingekocht of op een andere manier zijn georganiseerd.

- Het beleid geldt voor alle processen van de Universiteit Leiden en borgt daarmee de informatievoorziening gedurende de gehele levenscyclus, ongeacht de toegepaste technologie en ongeacht het karakter van de informatie. Het beperkt zich niet alleen tot de ICT, maar richt zich ook op de fysieke beveiliging, personele processen en het informatiebeveiligingsbewustzijn van gebruikers.

- Het beleid is van toepassing op de gehele data-levenscyclus: van het genereren of verzamelen van gegevens, het dagelijkse gebruik ervan en de gegevensopslag (zowel digitaal als analoog) tot en met de (eventueel) archivering en vernietiging ervan.

1.4 Opzet van het beleid - kapstokmodel

Voor het beleid wordt het 'kapstokmodel' toegepast. Het College van Bestuur geeft middels voorliggend document richting door het stellen van uitgangspunten. Dit strategisch beleid vertaalt zich door naar tactisch beleid voor informatieveiligheid. Het strategisch beleid en het tactisch beleid vormen tezamen het informatiebeveiligingsbeleid van waaruit operationele documenten worden opgesteld onder verantwoordelijkheid van de verantwoordelijke proceseigenaar. Figuur 1 visualiseert het kapstokmodel. Er is bewust gekozen voor het kapstokmodel. Dit bevordert de onderhoudbaarheid van het beleid. En aanpassing van beleid(sonderdelen) is eenvoudiger te organiseren. Daarbij zijn deze producten in lijn met de verantwoordelijkheden in de organisatie.



Figuur 1 Kapstokmodel van het informatiebeveiligingsbeleid

[1] Samenwerkingsverbanden, convenanten, coalities e.d.

1.5 Geldigheid & verantwoordelijkheid van het beleid

Het college is eigenaar van dit beleidsdocument. Het beheer, opstellen en actueel houden van het beleidsdocument is de verantwoordelijkheid van de Chief Information Security Officer (CISO) namens de directie/het college.

Dit beleid treedt in werking op de datum dat het is vastgesteld door het college. Hiermee komt het 'Raamwerk Strategisch Informatiebeveiligingsbeleid (2020; versie 1.0) te vervallen.

Dit beleid is geldig tot en met 2027 (in lijn met het Strategisch plan Universiteit Leiden 2022-2027) en wordt minimaal één keer per jaar geëvalueerd onder leiding van de CISO. Tussentijdse bijstelling is mogelijk als daarvoor aanleiding is. Aanpassing van het beleid kan plaatsvinden op basis van voortschrijdend inzicht, zoals:

- wijziging van organisatiedoelen;
- feedback en ervaring ten aanzien van de werkbaarheid, doelmatigheid en effectiviteit op basis van de uitvoering van het beleid;
- de stand van de techniek (nieuwe beveiligingstechnieken);
- nieuwe dreigingen of aanvalstechnieken;
- veranderingen aan wet- en regelgeving of de organisatie.

1.6 Leeswijzer

- In hoofdstuk 2 is het domein informatieveiligheid uiteengezet. In dit hoofdstuk staan de doelen en visie.
- In hoofdstuk 3 zijn de principes en uitgangspunten geformuleerd, die beleidsbepalend zijn voor de realisatie van de doelen voor informatieveiligheid.
- De rollen, verantwoordelijkheden en taken zijn in hoofdstuk 4 beschreven. In dit hoofdstuk staan tevens de overleg- en rapportagestructuren.
- Hoofdstuk 5 bevat de randvoorwaarden die gelden om informatieveiligheid succesvol in te bedden in de organisatie en de gestelde doelen te verwezenlijken.
- Tot slot is in hoofdstuk 6 beschreven hoe op naleving van dit beleid wordt gecontroleerd.

2. Informatieveiligheid

In dit hoofdstuk is uiteengezet wat het belang van informatiebeveiliging is. Als ook wat de visie en doelen zijn van de Universiteit Leiden op dit gebied.

2.1 Wat is informatiebeveiliging

Onder informatiebeveiliging wordt verstaan het treffen en onderhouden van een samenhangend pakket aan beheersmaatregelen om de vereiste betrouwbaarheid van informatie te waarborgen in termen van:

- **Beschikbaarheid:** Informatie dient beschikbaar te zijn op het moment dat het nodig is, wat eisen stelt aan de beschikbaarheid van informatiesystemen en databases.

- **Integriteit:** De gebruiker moet erop kunnen vertrouwen dat informatie juist, volledig, tijdig en geoorloofd is. Handhaving hiervan is verankerd in procesafspraken, maar ook in maatregelen die ongeoorloofde of ongewenste (expres of per ongeluk) mutaties tegengaan.

- **Vertrouwelijkheid:** Informatie is afgeschermd op het juiste niveau.

2.2 Relatie met privacy en gegevensbescherming

In een digitale samenleving is de bescherming van persoonsgegevens essentieel. Privacy en de bescherming van persoonsgegevens vormen een grondrecht. Privacy is een voorwaarde om vrij te zijn in wie je bent, wat je doet en om jezelf verder te ontwikkelen. Elke persoon moet regie kunnen houden over zijn eigen gegevens. Wat betekent dat deze persoon recht heeft op weten welke gegevens er van ze worden verzameld, wat daarmee gebeurt en hoe deze bijvoorbeeld zijn beschermd.

Elke betrokkene (de persoon wiens persoonsgegevens wij verwerken) mag erop rekenen dat wij persoonsgegevens zorgvuldig, rechtmatig, transparant en veilig verwerken. Bij de verwerking houden we rekening met hun belangen. Hierbij is verhoogde aandacht voor de bescherming van gegevens van kwetsbare betrokkenen, zoals minderjarigen.

De borging van privacy is hierbij afhankelijk van adequate informatieveiligheid. Om de privacy te waarborgen geldt onder andere de verplichting om passende technische en organisatorische beheersmaatregelen te treffen. Hier gaat het om de effectiviteit van informatieveiligheid. Is de informatieveiligheid niet op orde, dan kan privacy niet gewaarborgd worden.

2.3 Digitale dreigingen

Data als ook de digitale veiligheid wordt steeds belangrijker. Dit heeft te maken met de informatiesamenleving waarin wij leven. We zijn meer online dan ooit. We werken digitaal, we winkelen digitaal, we volgen onderwijs digitaal en we ontmoeten elkaar steeds vaker digitaal. De snelle digitalisering die dit mogelijk maakt biedt ons veel kansen, maar het brengt ook risico's met zich mee. Het Nationaal Cyber Security Centrum en SURF constateren in hun onderzoeken dat digitale aanvallen jaarlijks toenemen en bovendien steeds complexer worden.

Jaarlijks stelt het Security Office van de Universiteit Leiden een dreigingsbeeld op waarin de belangrijkste informatiebeveiligingsrisico's staan. Op basis daarvan wordt het College van Bestuur geadviseerd over deze dreigingen en de te nemen beheersmaatregelen.

2.4 Visie

We willen bereiken dat studenten, docenten, onderzoekers, medewerkers en keten(partners) kunnen rekenen op de Universiteit Leiden. We zijn betrouwbaar en leveren kwalitatief goed onderwijs en onderzoek. We beheersen informatiebeveiligingsrisico's en treffen hiervoor passende beheersmaatregelen. We werken blijvend aan onze weerbaarheid.[2]

Met informatieveiligheid zorgen we er verder voor dat persoonsgegevens passend beschermd zijn. Het is hier waar privacy en informatiebeveiliging samenkomen en waar onze digitale weerbaarheid de belangrijkste rol speelt. Cyber incidenten waarbij persoonsgegevens op het spel staan zijn een van de grootste risico's voor de rechten en vrijheden van onze studenten, docenten, onderzoekers, medewerkers en andere personen.

2.5 Strategie en doelen op het gebied van digitale weerbaarheid

De digitale weerbaarheid komt tot stand door te zorgen dat de betrouwbaarheid is gewaarborgd van de informatie(systemen) en processen waarmee wij werken.

Met voorliggend strategisch beleid informatieveiligheid wil de Universiteit Leiden bijdragen aan de kwaliteit van de informatievoorziening en zorgen voor een juiste balans tussen functionaliteit, veiligheid en privacy, en uiteraard de daarmee samenhangende kosten. Dit beleid vindt aansluiting met de missie en strategische doelen van de instelling.

Met het continu werken aan onze weerbaarheid hebben wij het volgende als doel:

- We waarborgen de kwaliteit én continuïteit van de onderwijs-, onderzoeks- en bedrijfsvoeringsprocessen.
- We bieden een veilige en toekomstbestendige leer-, onderzoeks- en werkomgeving.
- We hebben zicht op informatiebeveiligingsrisico's en treffen een samenhangend pakket aan passende beheersmaatregelen om deze risico's adequaat te beheersen.

Dit doen wij door te zorgen dat:

- Het juiste beschikbaarheids-, integriteits- en vertrouwelijkheidsniveau van de informatie (systemen) wordt gewaarborgd.
- We voldoen aan een gemiddeld volwassenheidsniveau 3 van het SURFaudit Toetsingskader.

Hierdoor is het mogelijk om:

- De kwaliteit en continuïteit te waarborgen van onze processen binnen de domeinen van onderwijs, onderzoek en bedrijfsvoering.
- De digitale veiligheid voldoende zeker te stellen;
- Risico's te beheersen en weerbaar te zijn tegen digitale dreigingen;

[2] Weerbaarheid: het vermogen om (relevante) risico's tot een aanvaardbaar niveau te reduceren door middel van een verzameling van beheersmaatregelen om schade te voorkomen en wanneer informatiebeveiligingsincidenten zich hebben voorgedaan deze tijdig te ontdekken, de schade ervan te beperken en herstel eenvoudiger te maken. Wat een aanvaardbaar niveau van weerbaarheid is, is de uitkomst van een risico-afweging. Die kan helpen om de juiste technische, procedurele of organisatorische maatregelen te kiezen (Definitie gebaseerd deze definitie uit Cyber securitybeeld (2022, NCTV)).

- Te voldoen aan wet- en regelgeving, inclusief de informatiebeveiligingseisen uit de privacy wetgeving.

Dit betekent concreet:

- Dat voor informatieveiligheid een systeem van risicomanagement is geïmplementeerd en effectief werkt.
- De betrouwbaarheid van de informatievoorziening is geborgd conform geldende normenkaders en best practices.
- Een proces van zelfregulering aanwezig is dat uitgaat van de plan-do-check-act-cyclus, waardoor de effectiviteit van dit risicomanagementproces, de geïmplementeerde beheersmaatregelen en het beveiligingsniveau wordt geëvalueerd en hiervan wordt geleerd. Via de P&C-cyclus wordt hierover gerapporteerd.
- Er een governance aanwezig is, dat ervoor zorgt dat informatiebeveiliging geborgd is in beleid en processen en waarbij aansluitend de verantwoordelijkheden en rollen zijn belegd.
- Adequaat en pro-actief wordt geacteerd wanneer informatiebeveiligingsincidenten en/of datalekken zich voordoen.
- Er structureel wordt ingezet op het bewustzijn.

2.6 Risico gebaseerde benadering

100% Informatieveiligheid bestaat niet. Dat maakt de Universiteit gesloten, is niet realistisch en bovendien onbetaalbaar. Het voldoende weerbaar zijn tegen (digitale) dreigingen houdt de Universiteit Leiden open en verbonden met de (veranderende) behoeften en wensen van de maatschappij. Dit betekent dat op bestuurlijk niveau keuzes gemaakt worden welke risico's (on)acceptabel zijn. Voor de risico's die niet geaccepteerd worden, worden passende beheersmaatregelen getroffen die zich richten op het voorkomen van risico's of het adequaat herstellen van een incident dat zich heeft voorgedaan. Het proces van risicomanagement staat daarom centraal in dit beleid.

2.7 Wet- en regelgeving

Naast onze doelen op het gebied van digitale weerbaarheid willen we voldoen aan geldende wet- en regelgeving. De belangrijkste aan informatieveiligheid gerelateerde wet- en regelgeving betreft:

- Wet op het Hoger onderwijs en Wetenschappelijk onderzoek (WHW)
- Algemene verordening gegevensbescherming;
- Uitvoeringswet Algemene verordening gegevensbescherming;
- De Telecommunicatiewet
- Wet Computercriminaliteit
- NIS2-richtlijn
- Archiefwet (en bewaartermijnen)
- Auteurswet
- Geldende normenkaders, zoals de NEN-ISO 27001 en 27002 (best practice)

3. Principes en beleidsregels

3.1 Strategische principes

De Universiteit Leiden hanteert de onderstaande vijf principes:

1 Informatiebeveiliging is risicogestuurd

Beheersmaatregelen zijn gebaseerd op de mogelijke risico's van onze informatie, processen en IT-faciliteiten.

Het delen van kennis (openheid) is een belangrijke kernwaarde van het onderwijs- en onderzoekproces. 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').

2 Informatiebeveiliging is een verantwoordelijkheid van iedereen

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

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, onderzoekers 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.

3 Informatiebeveiliging is een continu proces

Informatiebeveiliging zit in het DNA van al onze werkzaamheden

De omgeving verandert continu; cyber dreigingen nemen toe; 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.

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 (‘Security by Design).

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.

5 Security by Default
Standaard hanteren wij een beperkte (logische) toegang en veilige instellingen.
Gebruikers hebben alleen toegang tot informatie en IT-faciliteiten die zij nodig hebben voor hun werkzaamheden.

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.

3.2 Beleidsregels

De doorvertaling van de vijf principes leiden tot de volgende beleidsregels (uitgangspunten):

1. Informatieveiligheid draagt bij aan de realisatie van onze **maatschappelijke opgaves en doelen** op het gebied van onderwijs, onderzoek en bedrijfsvoering. Hierbij houden wij rekening met geldende wet- en regelgeving.

2. Het inrichten van de informatievoorziening volgens dit beleid in opzet, bestaan en werking, geeft **afdoende garantie** voor onze digitale weerbaarheid.

3. Het primaire uitgangspunt is **risicomanagement**. Wij hanteren een risicomanagement-systematiek conform de NEN-ISO 27001 waardoor wij continu risico’s in beeld brengen, waar nodig passende beheersmaatregelen treffen en monitoren of de beheersmaatregelen over de tijd heen nog steeds effectief en efficiënt werken. De klassieke aanpak waarbij inperking van de mogelijkheden de boventoon voert, maakt plaats voor veilig en verantwoord faciliteren.

4. Het **beveiligingsniveau is in lagen uitbreidbaar**. In de basis streven wij naar een volwassenheidsniveau 3 op basis van het SURFaudit Toetsingskader. Waar nodig of vereist worden extra (specifieke) maatregelen getroffen boven op dit basisniveau. Een uitgevoerde risicoanalyse kan hiertoe aanleiding geven. Daarnaast kan wet- en regelgeving hier ons toe verplichten.

5. Informatie wordt **geclassificeerd** om te bepalen welke beheersmaatregelen nodig en passend zijn. Hierbij is de aard van de informatie in de processen leidend. Er wordt geclassificeerd op de drie betrouwbaarheidsaspecten van informatie: Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV). Op basis van een classificatie wordt bepaald hoe deze informatie

behandeld dient te worden.

6. Bij de start van **projecten**, het inrichten van **processen** en het **inkopen** of **uitbesteden** van diensten en systemen wordt een risicoanalyse vroegtijdig uitgevoerd. Er wordt een expliciet besluit genomen door de risico-eigenaar op de beheersing van de gevonden risico's en de opvolging van het advies.

7. Het beleid is leidend en bepalend voor een adequate bescherming van de betrouwbaarheid van onze informatie bij samenwerkingen met **leveranciers** en andere **(keten)partners** met wie wordt samengewerkt. Er zijn afspraken gemaakt op het gebied van informatieveiligheid en op de naleving wordt toegezien.

8. Structureel en planmatig wordt gewerkt aan het **bewustzijn**.

9. Het systeem van **zelfregulering** staat centraal, waarbij jaarlijks opzet, bestaan en werking van de beleidsregels worden geëvalueerd. Op basis hiervan wordt een verbeterplan opgesteld en wordt via de **P&C-cyclus verantwoording** afgelegd door het college van bestuur aan de raad van toezicht. Er wordt gewerkt conform de plan-do-check-act verbetercyclus.

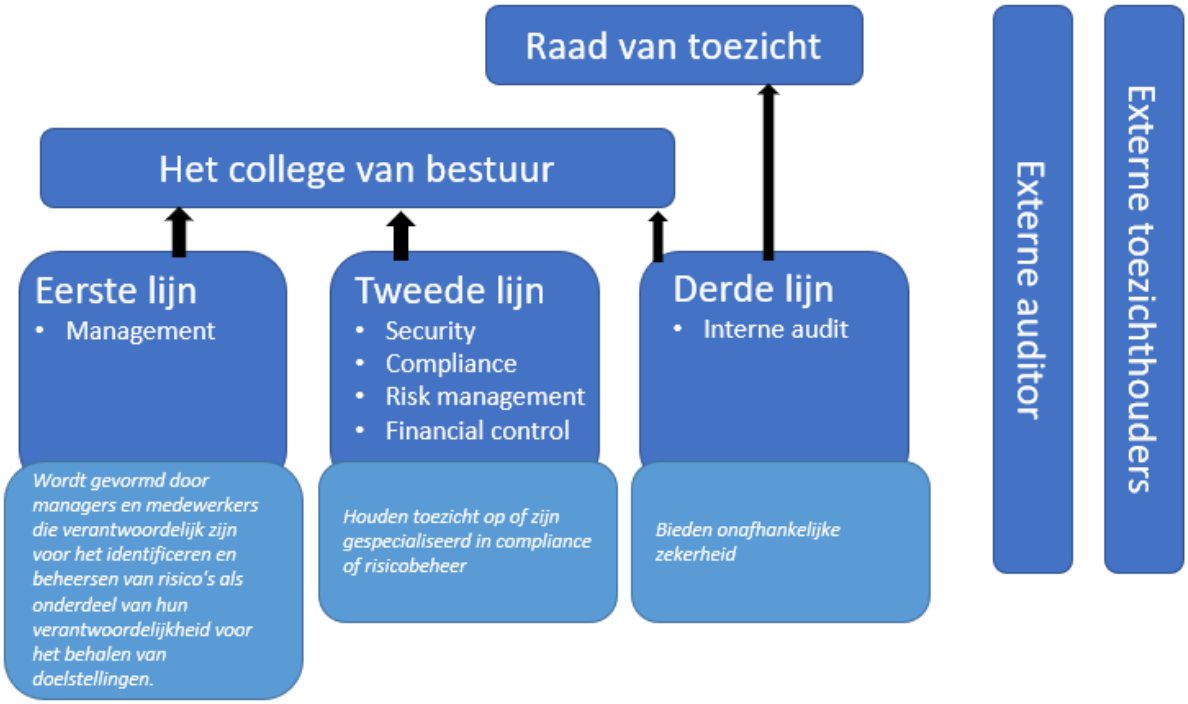
10. Het **Zero-trust principe** wordt gehanteerd. Dit is een bekend beveiligingsmodel om moderne digitale omgevingen te beschermen.

4. Organisatie van informatieveiligheid

Dit hoofdstuk beschrijft hoe de governance voor informatiebeveiliging is georganiseerd, wie waarvoor verantwoordelijk is en aan wie wordt gerapporteerd. Dit is op hoofdlijnen uiteengezet.[3]

4.1 Three Lines Model

De governance van informatiebeveiliging is ingericht volgens het zogenaamde Three Lines Model, zie figuur 3.[4] Dit model wordt algemeen toegepast als model om Governance, Risk en Compliance (GRC) te borgen in een operationele organisatie ten aanzien van risicobeheersing. Het beschrijft niet alleen de rollen binnen de organisatiestructuur, maar ook hun onderlinge samenwerking.



Figuur 3 Three Lines Model

Het College van Bestuur is eindverantwoordelijk voor de informatieveiligheid. Het college ziet toe op de risicobeheersing van informatiebeveiliging, stelt de risicobereidheid en het strategisch informatie-beveiligingsbeleid vast. Via een mandaatregeling zijn specifieke verantwoordelijkheden belegd bij de decanen van de faculteiten en de directeuren van de expertisecentra.

Het Three Lines Model heeft als uitgangspunt dat de eerste lijn (de business) verantwoordelijk is voor diens eigen processen, inclusief risicobeheersing.

Dit betekent dat de decanen van de faculteiten en de directeuren van de expertisecentra organisatorisch integraal eindverantwoordelijk zijn voor de informatiebeveiliging binnen hun organisatieonderdeel in overeenstemming met dit beleid. Hierbij worden zij in de operatie bijgestaan vanuit de tweede lijn door een Local Information Security Officer (LISO).

[3] In een separaat operationeel document is de informatiebeveiligingsorganisatie geoperationaliseerd met aan RACI-tabel.

[4] Internal audit: three lines model explained | ICAS

De LISO adviseert de eerste lijn, ondersteunt bij de implementatie van het beleid, zorgt voor het plannen en uitvoeren van risico-analyses, adviseert aansluitend over en ziet toe op het treffen van passende beheersmaatregelen, doet bewustwordingsinterventies en werkt samen met het Security Office.

De tweede lijn ondersteunt, adviseert, coördineert en bewaakt of de eerste lijn zijn verantwoordelijkheden ook daadwerkelijk neemt. Het opstellen van beleid, het organiseren van de PDCA-cyclus, het ondersteunen bij de uitvoering van integrale risico-analyses en self-assessments en het opstellen van jaarplannen en rapportages zijn taken van de tweede lijn. In de tweede lijn zit ook het Security Office. Het Security Office ondersteunt hierbij, borgt de kwaliteit van deze producten, draagt bij aan het op peil houden van kennis en kunde van LISO's.

Daarnaast ondersteunt het Security Office de onderdelen van de Universiteit Leiden vanuit de 2e lijn in het gepast beheersen van informatiebeveiligingsrisico's. Het Security Office doet dit door middel van bindende richtlijnen, adviezen en professionele, behulpzame en kwalitatieve dienstverlening. Met actuele kennis van de materie en van de lokale situaties zal het Security Office alles er aan doen om te ontzorgen, de lasten minimaal te houden, heldere richtlijnen op te stellen en duidelijk te communiceren zodat de 1e lijn zelf in staat gesteld wordt om gepaste informatiebeveiligingsrisicobeheersing toe te passen. Hierin werkt het Security Office nauw samen met de LISO's. Het Security Office zal centraal regie voeren op de hiervoor belangrijke onderwerpen en zal rapporteren over -en sturen op- de voortgang van deze risicobeheersing.

Vanuit het ISSC is Security Operations (/CERT) verantwoordelijk voor de vertaling van het informatiebeveiligingsbeleid op inrichtingsniveau ten aanzien van de IT-omgeving. Binnen de kaders van het gestelde informatiebeveiligingsbeleid is Security Operations (/CERT) daarom ook bevoegd om op dit niveau voorwaarden te definiëren om de beveiliging van de IT-omgeving te borgen. Hierbij kan gedacht bijvoorbeeld gedacht worden aan het voorschrijven van specifieke cryptografische technieken, specifieke hardening baselines en het bijhouden van bijvoorbeeld een black list ten aanzien van ongewenste informatiesystemen e.d. Hierbij past het ook dat Security Operations (/CERT) een controlerende en toetsende rol heeft. Security Operations (/CERT) is verantwoordelijk voor detectie en response, en bevoegd om passende herstelmaatregelen te treffen wanneer een informatiebeveiligingsrisico zich voordoet ten aanzien van de IT-omgeving.

Binnen de organisatie is het verder noodzakelijk dat er in de organisatie een functie bestaat die controleert of het samenspel tussen de eerste en tweede lijn soepel functioneert en of de organisatorische doelen behaald worden door middel van opzet, bestaan en werking van de nodige beheersmaatregelen in de eerste en tweede lijn. Het is de derde lijn die daarover een objectief, onafhankelijk oordeel velt met mogelijkheden tot verbetering. De binnen de AVG verplichte Functionaris Gegevensbescherming (FG) en de Interne Auditafdeling (AIC) behoren typisch tot de derde lijn. Maar ook de Chief Information Security Officer (CISO) zit in de derde lijn. Zij opereren volledig los van alle andere organisatie-onderdelen en rapporteren niet alleen aan het CvB, maar ook aan de RvT.

De CISO is hierbij een functie op strategisch niveau. De CISO adviseert aan het bestuur en heeft direct toegang tot het bestuur. De CISO heeft de taak om toe te zien of het informatiebeveiligingsproces doeltreffend is. De CISO formuleert de strategie en het strategisch beleid voor informatiebeveiliging en

rapporteert aan het college van bestuur over de risicobeheersing en heeft de bevoegdheid om onderzoek te (laten) doen naar de staat van informatiebeveiliging binnen de Universiteit Leiden om zo uitvoering te geven aan de controlerende functie van de CISO. Advies van de CISO moet ingewonnen worden bij alle aangelegenheden met mogelijk significante gevolgen voor de informatieveiligheid. De CISO werkt in dit geheel samen met het Security Office.

4.2 Overleg- en rapportagestructuren

De volgende overlegstructuur wordt aangehouden voor informatiebeveiliging:

Overleg	**Frequentie** (minimaal)
CISO en Raad van Toezicht	Jaarlijks
CISO en college van bestuur / portefeuillehouder	Maandelijks
CISO en FG	Maandelijks
CISO, Security-Office en afvaardiging ISSC (IB-kernteam)	Om de twee weken
CISO, Security-Office, LISO's en informatiemanagers (IB-team)	Maandelijks

De rapportage over informatieveiligheid volgt het stramien van de P&C cyclus.

Rapportage	**Toelichting**
Jaarverslag Informatieveiligheid	Jaarverslag van de CISO aan het College
Paragraaf Informatieveiligheid in de jaarrekening	Verantwoording (voorbereid door de CISO) van het college van bestuur aan de raad van toezicht
Kwartaalrapportages (over voortgang, risico's, beoordelingen e.d.)	Van het Security Office aan de CISO, de directie en het college van bestuur
Maandrapportages (over incidenten, dreigingen, risico's e.d.)	Van Security Operations aan de CISO, het Security Office en verantwoordelijke management.

5. Randvoorwaarden

De Informatiebeveiligingsdienst voor gemeenten heeft in haar dreigingsbeeld (2022) zes succesfactoren benoemd voor informatieveiligheid die eveneens op het Hoger Onderwijs van toepassing zijn. Bij de inbedding van dit beleid, worden deze onderstaande randvoorwaarden meegenomen.

- **Organisatie**
  De informatiebeveiligingsorganisatie staat. Er is een veilige cultuur.

- **Eigenaarschap management**
  Informatiebeveiliging staat op de agenda van bestuur en management. Daarnaast oefent het bestuur/management minimaal eens per jaar een cyberoefening (uitval van systemen in de eigen organisatie).

- **Financiën**
  Er zijn voldoende middelen structureel begroot.

- **Techniek**
  Techniek is niet onfeilbaar. De basis is op orde en een gelaagd beveiligingsniveau is toegepast.

- **Factor mens**
  Een belangrijke bouwsteen van informatiebeveiliging is het bewustzijn van medewerkers. Veel incidenten zijn terug te voeren op een gebrek aan digitaal bewustzijn en andersom: een verhoogd digitaal bewustzijn zorgt ervoor dat incidenten snel herkend en erkend worden. Een veilige omgang met data is onderdeel van het primaire proces en vraagt dus permanent aandacht en voorbeeldgedrag van bestuur/management en doorlopend trainen van alle medewerkers.

- **Samenwerkingsverbanden**
  Met samenwerkingsverbanden (IT-leveranciers, ketenpartners, derde partijen) worden afspraken gemaakt en hier wordt op toegezien.

6. Naleving en evaluatie

Beheersmaatregelen worden getroffen om risico's te verminderen. Om de controle over de risico's te waarborgen is het noodzakelijk regelmatig na te gaan of maatregelen nog werken en nog steeds de beoogde veiligheid bieden.

De Universiteit Leiden controleert hiervoor periodiek de maatregelen die voortkomen uit dit beleid door controles vanuit AIC, interne assessments en externe audits ten aanzien van (kosten)effectiviteit en informatieveiligheid. Hierover wordt ook gerapporteerd (zie paragraaf 4.2).

Daarnaast beoordeelt de CISO minimaal jaarlijks de effectiviteit van het informatiebeveiligings-managementproces op basis van verzamelde gegevens en informatie en adviseert hierover aan het College van Bestuur.

Input voor deze beoordeling is onder andere op basis van:

- Geregistreerde incidenten en (kwetsbaarheids)meldingen;
- Uitgevoerde controles en interne en externe audits;
- Uitgevoerde leveranciersbeoordelingen;
- Uitgevoerde risico-analyses;
- Rapportages ten aanzien van de voortgang van de implementatie van beheersmaatregelen en de effectieve werking van de geïmplementeerde maatregelen.

Op basis van de bevindingen en bijbehorende adviezen van de CISO naar aanleiding van de beoordeling van de effectiviteit van het informatiebeveiligingsmanagementproces, worden waar nodig corrigerende beheersmaatregelen doorgevoerd met als doel de kans en/of impact van een incident te minimaliseren, of de doeltreffendheid van het managementsysteem te verbeteren.

Sancties

Als blijkt dat de naleving ernstig tekortschiet door verantwoordelijke medewerkers of studenten, dan kan de Universiteit Leiden deze personen sanctioneren. 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).