2024/2025

Informatiebeveiligingsbeleid Tilburg University

TILBURG UNIVERSITY

Understanding Society

Inhoudsopgave

Versiebeheer

Versie	Datum	Opsteller	Toelichting
1.0	02-03-2021	LIS: Information Security	IB-beleid definitief.
1.02	28-06-2021	LIS: Information Security	Tekstuele aanpassingen. Versie 1.02 vastgesteld door het College van Bestuur op 07-09-2021.
1.1	25-03-2024	ES: CISO Office	Nieuwe versie IB-beleid, met wijzigingen in opmaak en tekstuele wijzigingen in: - paragraaf 2.2 (uitgangspunten IB-beleid) - hoofdstuk 3 (informatiebeveiligingsprincipes) - paragraaf 5.2 (rollen en verantwoordelijkheden) - paragraaf 5.3 (tabel governance structuur) - hoofdstuk 6 (bewustwording) - hoofdstuk 9 (melding en afhandeling van incidenten) - bijlage B (informatiebeveiligingsprincipes) - bijlage C (BIV-classificatie) - bijlage D (wet- en regelgeving) - bijlage E (rollen informatiebeveiliging) - bijlage F (inrichting CERT). - de RASCI matrix (oude bijlage E) is verwijderd.

Model informatiebeveiligingsbeleid

Dit Informatiebeveiligingsbeleid is gebaseerd op het Model Informatiebeveiligingsbeleid SCIPR. Onderdeel van het SCIPR Framework Informatiebeveiliging.

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

Voorwoord

Voor het uitvoeren van onze taken is het goed beveiligen van onze informatievoorziening van cruciaal belang. De werkprocessen van Tilburg University kunnen niet worden uitgevoerd zonder het verzamelen, vastleggen en delen van informatie met zowel interne als externe partners, collega's en studenten.

In dit informatiebeveiligingsbeleid (hierna te noemen: IB-beleid) is verwoord op welke manier Tilburg University voorziet in adequate informatiebeveiliging en daarmee voldoet aan de relevante wet- en regelgeving, maar ook aan de intern gehanteerde beveiligingsmaatstaven. Met het IB-beleid wil Tilburg University bijdragen aan een betere kwaliteit van de informatievoorziening en zorgen voor een juiste balans tussen functionaliteit, veiligheid en privacy.

Tilburg, maart 2024

College van Bestuur

Samenvatting

Informatiebeveiliging is het geheel aan maatregelen, processen en procedures die de beschikbaarheid, integriteit en vertrouwelijkheid van informatie en de informatievoorziening borgen. Tilburg University hanteert vijf beleidsprincipes voor informatiebeveiliging, te weten:

1. **Risico-gebaseerd**
   We baseren maatregelen op de mogelijke veiligheidsrisico's van onze informatie, processen en IT-faciliteiten (in de breedste zin van het woord).

2. **Iedereen**
   Alle medewerkers, studenten, gasten, bezoekers en externe relaties van Tilburg University voelen zich verantwoordelijk voor een juist en veilig gebruik van middelen en bevoegdheden.

3. **Altijd**
   Informatiebeveiliging zit in het DNA van al onze werkzaamheden.

4. **Security by Design**
   Informatiebeveiliging is vanaf de start een integraal onderdeel van ieder project of iedere verandering m.b.t. informatie, processen en IT-faciliteiten.

5. **Security by Default**
   In elke configuratie die wordt geïmplementeerd staan de aanwezige security-opties standaard aan. Het openstellen van informatie en de inrichting van configuraties zijn daarmee altijd een bewuste keuze na zorgvuldige afweging

De verantwoordelijkheid voor informatiebeveiliging is conform het Three Lines Model ingericht. De business is in de eerste lijn verantwoordelijk voor haar eigen processen, inclusief risicobeheersing. Het College van Bestuur is eindverantwoordelijk. De CISO heeft in de tweede lijn een adviserende en ondersteunende verantwoordelijkheid. Vanuit de derde lijn vindt de onafhankelijke controle op de eerste en tweede lijn plaats. Hierbij wordt het SURF normen- en toetsingskader IBHO, dat is gestoeld op ISO 27001/27002 en het NBA/NOREA Volwassenheidsmodel als uitgangspunt gebruikt.

De te nemen beveiligingsmaatregelen bestaan altijd uit een vastgestelde verplichte set van basismaatregelen (de Baseline Informatiebeveiliging Tilburg University). Door informatie(systemen) te classificeren, wordt duidelijk gemaakt welk beveiligingsniveau vereist is voor de onderdelen beschikbaarheid, integriteit en vertrouwelijkheid. Beleid en maatregelen alleen zijn niet voldoende om risico's op het gebied van informatiebeveiliging volledig uit te sluiten. De mens zelf creëert de grootste risico's. Bij Tilburg University werken we daarom voortdurend aan het vergroten van het beveiligingsbewustzijn binnen onze organisatie door middel van het awareness jaarplan.

Informatiebeveiliging is een continu proces, waarbij we steeds kijken naar mogelijke verbeteringen. Dit gebeurt onder andere door jaarplannen, controles en bijsturing, waarover 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. De CISO dient hiervoor een toereikend budget te hebben.

De informatiebeveiligingsincidenten worden afgehandeld volgens het vastgestelde Incident Managementproces, waar meldingen van datalekken ook een onderdeel van zijn. De Functionaris Gegevensbescherming (FG) handelt de gemelde datalekken af.

Leeswijzer

In het IB-beleid wordt in hoofdstuk 1 beschreven op wie, op welke onderdelen en op welke devices en informatiesystemen het beleid van toepassing is. Het doel van het IB-beleid is opgenomen in hoofdstuk 2. Tilburg University hanteert vijf beveiligingsprincipes, welke in hoofdstuk 3 staan beschreven. Hoe Tilburg University omgaat met relevante wet- en regelgeving wordt aangestipt in hoofdstuk 4 en de verantwoordelijkheden inclusief beschrijving van de rollen van de betrokken functionarissen zijn in hoofdstuk 5 uiteengezet. Ook is in hoofdstuk 5 een overzicht opgenomen van belangrijke documenten op het gebied van informatiebeveiliging. In hoofdstuk 6 wordt stilgestaan bij bewustwording en hoofdstuk 7 gaat verder in op de onafhankelijke controle. Tot slot beschrijft hoofdstuk 8 de financiering en gaat hoofdstuk 9 in op de afhandeling van meldingen en incidenten.

In de bijlagen is aandacht voor de managementcyclus voor periodieke bijstelling. De vijf beleidsprincipes voor informatiebeveiliging zijn in bijlage B volledig uitgewerkt. Daarnaast is een overzicht gegeven van de belangrijkste wet- en regelgeving rondom informatiebeveiliging en worden de rollen van betrokken functionarissen op een rijtje gezet.

1. Inleiding

1.1 Aanleiding

De digitale en fysieke werkelijkheid is constant in beweging. Denk hierbij aan de continue technologische ontwikkelingen, de ontwikkelingen binnen cybercrime, de aangescherpte eisen om te voldoen aan de wet- en regelgeving rondom privacy[1] (AVG) en de afspraken met onderzoek- en onderwijspartners. Deze bewegingen brengen steeds nieuwe en andere risico's met zich mee met betrekking tot informatiebeveiliging en vraagt om bijstelling voor een passend beveiligingsniveau. De risico's kunnen een bedreiging vormen voor de kwaliteit en continuïteit van processen en het behalen van de strategische doelen. Ook kunnen zij mogelijk de privacy van medewerkers, studenten en gasten schaden. De bedreigingen kunnen de beschikbaarheid, integriteit en vertrouwelijkheid van informatie beïnvloeden:

1. **Beschikbaarheid**: informatie is op gewenste momenten beschikbaar.
2. **Integriteit**: informatie is juist en volledig.
3. **Vertrouwelijkheid**: informatie is alleen toegankelijk voor degenen die hiervoor bevoegd zijn.

Het verkleinen en beheersen van de risico's vraagt om inspanningen op organisatorisch en technisch vlak. Tilburg University moet zich bewust worden én blijven van de risico's en het handelen daarop afstemmen.

Tilburg University is een instelling met een open karakter. Vanuit het onderwijs- en onderzoeksperspectief is de insteek "Open waar mogelijk, gesloten waar nodig". Adequate beveiliging van informatie is steeds een randvoorwaarde en het openstellen van informatie moet een bewuste keuze zijn. De vast te stellen maatregelen, procedures en richtlijnen kunnen getoetst worden aan de vijf hoofdprincipes die in hoofdstuk 3 zijn beschreven.

1.2 Doelgroep

Het IB-beleid van Tilburg University is van toepassing op de organisatie van Tilburg University: de vijf schools, de zeven ondersteunende divisies en de samenwerkingspartners die gebruik maken van de infrastructuur en IT-faciliteiten van Tilburg University en door derden geleverde (cloud) diensten. Kortom, op iedereen die - intern dan wel extern - op enige manier te maken heeft met (aspecten van) het bedrijfsproces van Tilburg University. Het College van Bestuur, de decanen en directeuren zijn primair verantwoordelijk voor de naleving en het uitdragen van het beleid en door voorbeeldgedrag te tonen.

1.3 Reikwijdte van het beleid

Tilburg University interpreteert informatieveiligheid breed. Er is een nauwe relatie en een gedeeltelijke overlap met aangrenzende beleidsterreinen, zoals privacy, kennisveiligheid, fysieke beveiliging, sociale veiligheid, bedrijfshulpverlening en business continuity. In het kader van integrale veiligheid[2] wordt op strategisch niveau aandacht besteed aan deze raakvlakken en wordt zowel planmatig als inhoudelijk afstemming gezocht.

Onder het IB-beleid vallen in beginsel alle devices en informatiesystemen (zowel beheerd als onbeheerd) waarmee geautoriseerde[3] toegang tot (diensten van) het Tilburg University netwerk kan worden verkregen en/of waarmee informatie van Tilburg University wordt verwerkt.

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

---

[1] Voor het specifieke Beleid Privacy en Bescherming Persoonsgegevens van Tilburg University zie intranet.
[2] Integrale veiligheid is bedoeld om veiligheidsproblemen binnen een organisatie in samenhang aan te pakken, met als doel de veiligheid op een zo hoog mogelijk niveau te brengen.
[3] Ongeautoriseerde toegang is per definitie een beveiligingsincident.

2. Definitie, doelstelling en uitgangspunten

2.1 Informatieveiligheid en informatiebeveiliging

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

2.2 Doelstelling en uitgangspunten

Het IB-beleid heeft als doel om richting te geven aan de wijze waarop Tilburg University weerbaar moet zijn tegen de risico's die de actuele ontwikkelingen op het gebied van informatieveiligheid met zich meebrengen. Dit beleid stelt de organisatie in staat de beschikbaarheid, integriteit en vertrouwelijkheid van onderwijs, onderzoek en bedrijfsvoering te waarborgen.

Hierbij worden de volgende uitgangspunten gehanteerd:

- **Three Lines organisatie**
  De interne organisatie van risicobeheersing, risicomanagement en informatiebeveiliging worden vormgegeven volgens het Three Lines Model[4]. Dit model wordt algemeen toegepast als model om Governance, Risk en Compliance te borgen in een operationele organisatie. Het beschrijft niet alleen de rollen binnen de organisatiestructuur, maar ook hun onderlinge samenwerking.

- **Kader**
  Het IB-beleid biedt een kader om (toekomstige) maatregelen in de informatiebeveiliging te toetsen aan de vastgestelde beveiligingsprincipes (paragraaf 3.2), best practices en normen. Daarnaast biedt het een kader om de taken, bevoegdheden en verantwoordelijkheden binnen de instelling te beleggen.

- **Procesbenadering**
  Informatiebeveiliging is een continu proces en volgt een PDCA-cyclus. Periodiek worden risicoanalyses en audits uitgevoerd. De resultaten hiervan worden opgenomen in vastgestelde jaarplannen met duidelijke keuzes in beveiligingsmaatregelen. De uitvoering van deze beveiligingsmaatregelen wordt periodiek gecontroleerd.

- **Normen**
  De basis voor de inrichting van het informatiebeveiligingsmanagement is de internationale standaard ISO 27001. Specifiek voor de SURF gemeenschap 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.

- **Maatregelen**
  Maatregelen worden genomen op basis van best practices in het hoger onderwijs en op basis van de op ISO 27002 gebaseerde Baseline Informatiebeveiliging Tilburg University (hierna te noemen: baseline). Met het hanteren van de baseline is geborgd dat de basis aan informatiebeveiligingsmaatregelen geïmplementeerd en aantoonbaar gemaakt kan worden. Door informatie(systemen) te classificeren, wordt duidelijk gemaakt welk beveiligingsniveau vereist is voor beschikbaarheid, integriteit en vertrouwelijkheid. Als deze classificatie hoger scoort dan de baseline, zijn additionele maatregelen nodig om risico's te mitigeren.

- **Volwassenheid**
  Tilburg University streeft naar minimaal een volwassenheidsniveau 3 in opzet, bestaan en werking volgens het Capability Maturity Model (CMM).

[4] three-lines-model-updated-dutch.pdf (theiia.org).

3. Beleidsprincipes informatiebeveiliging

Tilburg University hanteert vijf beleidsprincipes voor informatiebeveiliging:

1	**Risico-gebaseerd** Informatiebeveiligingsmaatregelen worden risico-gebaseerd genomen 
Kern	We baseren de maatregelen op 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 Tilburg University. 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 en onze zogenaamde risk appetite (risicobereidheid). 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 is verantwoordelijk** Informatiebeveiliging is de verantwoordelijkheid van iedereen 
Kern	De verantwoordelijkheid voor informatiebeveiliging en privacybescherming ligt bij iedereen (alle medewerkers, studenten, gasten, bezoekers en externe relaties van Tilburg University) en het management stuurt hierop.
Achtergrond	Iedereen is zich bewust van de waarde van informatie en handelt daarnaar. Deze waarde wordt bepaald door de mogelijke schade als gevolg van verlies van beschikbaarheid, integriteit of vertrouwelijkheid. Van zowel medewerkers, studenten als derden wordt verwacht dat ze bewust omgaan met informatie 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 binnen Tilburg University.
Implicaties	Denk hierbij aan het vastleggen van afspraken in arbeidsvoorwaarden (zoals het verplicht volgen van de training Digitaal Veilig Werken), 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 wisselen, 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 creëren en controles uitvoeren.
Implicaties	Denk hierbij aan het inrichten van een PDCA-cyclus en het houden van bewustwordingscampagnes op basis van het awareness jaarplan. Zie bijlage B voor een overzicht van alle implicaties.

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. 
Achtergrond	Security by Design betekent dat al tijdens de start van een project, het ontwerp van een nieuw informatiesysteem 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** In elke configuratie die wordt geïmplementeerd staan de aanwezige security-opties standaard aan. 
Achtergrond	Security by Default voorkomt ongewenste en ongecontroleerde toegang tot (persoons)gegevens. Het openstellen van informatie en de inrichting van instellingen zijn daarmee altijd een bewuste keuze na een zorgvuldige afweging.
Implicaties	Denk hierbij aan het definiëren van standaard-rollen en het standaard beperken van autorisaties. Zie bijlage B voor een overzicht van alle implicaties

De beleidsprincipes helpen bij de implementatie van het IB-beleid, in die zin dat de principes bepalen welke beveiligingsmaatregelen er nodig zijn voor de bescherming van de processen. In bijlage B zijn de beleidsprincipes verder uitgewerkt met de belangrijkste implicaties.

4. Wet- en regelgeving

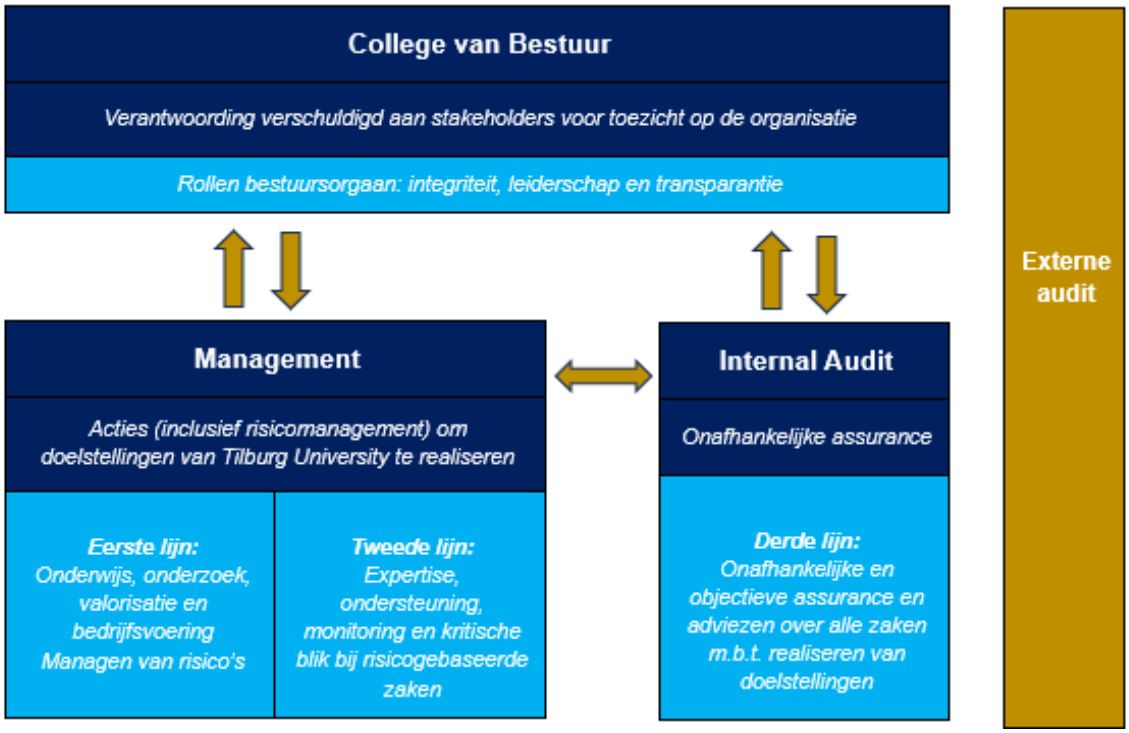
Het uitgangspunt is dat Tilburg University in haar processen en procedures voldoet aan alle van toepassing zijnde wet- en regelgeving en zich voorbereidt om aan aankomende wetgeving te voldoen. Hoe Tilburg University omgaat met relevante wet- en regelgeving staat meer in detail beschreven in bijlage D - Wet- en regelgeving.

5. Organisatie van de informatiebeveiligingsfuncties

Voor de borging van het IB-beleid is het niet alleen noodzakelijk dat de verschillende rollen en verantwoordelijkheden in de organisatie op het gebied van informatiebeveiliging zijn vastgelegd, maar ook de wijze waarop deze rollen en verantwoordelijkheden zich tot elkaar verhouden. In dit hoofdstuk zijn de rollen en verantwoordelijkheden en hun onderlinge samenhang nader uitgewerkt.

5.1 Three Lines Model

Informatieveiligheid is binnen Tilburg University ingericht volgens het zogenaamde IAA's Three Lines Model. Binnen dit model worden drie lijnen met hun eigen verantwoordelijkheden onderscheiden. Het beschrijft de rollen binnen de organisatiestructuur en onderlinge samenwerking.



Three Lines Model

5.2 Rollen en verantwoordelijkheden

College van Bestuur

Het College van Bestuur is eindverantwoordelijk voor de informatiebeveiliging en stelt het beleid vast. Zij stelt de benodigde middelen ter beschikking om het beleid uit te voeren, doelen te halen en risico's te mitigeren en stimuleert een cultuur van ethisch en verantwoord gedrag. Het College van Bestuur bepaalt de kaders voor risicobereidheid en legt verantwoording af aan stakeholders. De verantwoordelijkheid van het College van Bestuur wordt via de mandaat- en volmachtregeling[5] bij de decanen en directeuren belegd. Binnen het College van Bestuur is een van de leden benoemd als portefeuillehouder informatiebeveiliging.

[5] De mandaat- en volmachtregeling is gepubliceerd op intranet.

Eerste lijn

Het Three Lines Model heeft als uitgangspunt dat de eerste lijn (de business) verantwoordelijk is voor de eigen processen, inclusief risicobeheersing. De eerste lijn geeft leiding en sturing en is voortdurend in dialoog met het College van Bestuur over de realisatie van de doelstellingen en de risicobeheersing.

Directeuren en decanen zijn veelal proces[6]-, systeem[7]- of informatie-eigenaar[8] en daardoor verantwoordelijk voor de implementatie en naleving van het IB-beleid in haar eigen processen en systemen. Zij zorgen ervoor dat:

- beveiligingsmaatregelen worden geïmplementeerd;
- het bewustwordingsprogramma wordt uitgevoerd;
- medewerkers worden opgeleid;
- risicomanagement wordt uitgevoerd. Het CISO Office ondersteunt hierbij middels het uitvoeren van een BIV-classificatie[9]. De eigenaar levert hiervoor de juiste input aan;
- voldaan wordt aan de baseline en het toepassen van extra maatregelen om de juiste mate van beveiliging te bewerkstellingen. Het CISO Office controleert of aan de baseline wordt voldaan.

Om valide redenen kan ervoor gekozen worden om bewust af te wijken van de voorgeschreven beveiligingsmaatregelen en mitigerende maatregelen te nemen om het resterende risico te beperken. Dergelijke restrisico's worden vastgelegd in het risicoregister middels het invullen van een Risico Acceptatie Formulier. Met dit formulier wordt de risico-eigenaar op de hoogte gebracht, en worden afspraken gemaakt over eventuele tijdelijke beveiligingsmaatregelen en/of wanneer het risico gemitigeerd gaat worden. Met het tekenen van het Risico Acceptatie Formulier wordt de verantwoordelijkheid voor het risico vastgelegd en kunnen risico's beheerst en beheerd worden. In onderstaand risico-acceptatie matrix is weergegeven op welk niveau risico's geaccepteerd kunnen worden. De risico's worden ingeschat middels het bepalen van kans x impact.

Inschatting	Bevoegd tot accepteren
Kritiek	CvB
Hoog	CvB
Medium	Proces-/systeem-/informatie-eigenaar
Laag	Geen formele acceptatie vereist[10]

Risico-acceptatie matrix

De CISO heeft bij het opstellen van het risicoregister en het Risico Acceptatie Formulier een adviserende rol en gaat in overleg met het College van Bestuur om tot een definitief besluit te komen. De genomen restrisico's worden jaarlijks geëvalueerd. Daarnaast worden de portefeuillehouder informatiebeveiliging en de Auditcommissie (Stichtingsbestuur) periodiek geïnformeerd over de kritieke en hoge risico's.

Informatiemanager van divisies en faculteiten

De informatiemanagers bewaken, met het mandaat van de directeur, het IB-beleid binnen hun eigen divisie of faculteit. Hierbij worden ze ondersteund door leidinggevenden. Binnen Tilburg University zijn informatiemanagers van de divisies en informatiemanagers van de faculteiten aangesteld. De informatiemanager is betrokken bij informatievoorzieningsprojecten en -ontwikkelingen in onderwijs, onderzoek en bedrijfsvoering en stimuleert in deze projecten en ontwikkelingen de naleving van het IB-beleid. De informatiemanager werkt nauw samen met het CISO Office.

[6] Voor decentrale IT-infrastructuur is de eigenaar van het primaire of ondersteunende proces verantwoordelijk.
[7] Een systeemeigenaar is verantwoordelijk voor een informatiesysteem, waarmee een of meerdere processen worden ondersteund. Een systeemeigenaar is vaak ook de proceseigenaar van het desbetreffende proces en daarmee eindverantwoordelijk.
[8] Een informatie-eigenaar is verantwoordelijk voor de informatie in het proces en/of systeem.
[9] Classificatie op Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV).
[10] Lage risico's worden wel vastgelegd in het risicoregister en toegewezen aan de betreffende eigenaar.

Tweede lijn

De tweede lijn ondersteunt en adviseert de eerste lijn en bewaakt of het management zijn verantwoordelijkheden neemt. Ook bepaalde beleidsvoorbereidende taken, het organiseren van de PDCA-cyclus, integrale risicoanalyses, self-assessments en het opstellen van een jaarplan zijn taken van de tweede lijn. De tweede lijn rapporteert rechtstreeks aan het College van Bestuur.

CISO Office en IT Security Office

Informatiebeveiliging is belegd bij de afdelingen CISO Office en IT Security Office. Het CISO Office is gepositioneerd binnen de divisie Executive Services (ES) en valt daarmee onder de verantwoordelijkheid van de directeur ES. Het IT Security Office is onderdeel van het CIO Office. De verschillende rollen binnen beide afdelingen zijn hieronder uitgewerkt.

Chief Information Security Officer (CISO)

De CISO onderhoudt het IB-beleid en heeft een onafhankelijke rol richting het College van Bestuur. Deze rol voert hij uit middels het gevraagd en ongevraagd adviseren van het College van Bestuur. De CISO definieert de informatiebeveiligingsstrategie en -beleid, helpt bij een juiste vertaling daarvan naar instellingsonderdelen, ziet toe op de (uniforme) naleving ervan en rapporteert over lacunes, inconsistenties en onvolkomenheden (en daarmee risico's). Op basis hiervan schrijft hij beleid en risico en compliance gebaseerde prioriteiten voor. De naleving en borging bewaakt de CISO in het Information Security Management System (ISMS).

De CISO heeft verschillende bevoegdheden. Zo kan hij onderzoek doen, onderzoek laten uitvoeren (audits), informatie opvragen en ongevraagd en gevraagd advies uitbrengen. Indien de eigenaar niets doet met het advies (waarbij er sprake is van een duidelijke risico-indictie) en het risico accepteert, kan de CISO escaleren naar het College van Bestuur indien hij dit niet acceptabel vindt.

De CISO heeft een rechtstreekse rapportagelijn naar de portefeuillehouder informatiebeveiliging uit het College van Bestuur. De CISO staat aan het hoofd van het CISO Office.

Information Security Officer (ISO)

De ISO is de directe ondersteuning van de CISO en implementeert de informatiebeveiligingsstrategie in de organisatie. De ISO ondersteunt bij het uitvoeren van een BIV-classificatie en voert risicoanalyses en security checks uit. Ook adviseert zij over specifieke informatiebeveiligingsmaatregelen, bijvoorbeeld in projecten en bij acquisities van software of hardware. Hierbij werkt de ISO nauw samen met de architecten en informatiemanagers.

De functie van de ISO is belegd bij meerdere personen. De ISO maakt deelt uit van het CISO Office.

Awareness Officer Privacy & Security

De Awareness Officer vormt de directe ondersteuning van de CISO voor het definiëren en implementeren van bewustwordingsactiviteiten in de organisatie. De Awareness Officer initieert (periodieke) bewustwordingsprogramma's en zet deze op. Daarnaast faciliteert de Awareness Officer voorlichtingen en trainingen aan medewerkers en studenten op het gebied van informatieveiligheid en privacy.

De rol van Awareness Officer is belegd bij één persoon. De Awareness Officer maakt deelt uit van het CISO Office.

IT Security Officer (ITSO)

De ITSO definieert de IT-beveiligingsrichtlijnen voor de organisatie in overeenstemming met de informatiebeveiligingsstrategie en -architectuur, signaleert en bewaakt de beveiliging van IT-systemen en de ontwikkelingen op dit vlak en legt daarbij voortdurend de relatie tot de business- en organisatiedoelen. De ITSO adviseert over specifieke technische informatiebeveiligingsmaatregelen. Tevens beoordeelt hij de resultaten van penetratietests, vulnerability scans en assessments die door leverende partijen overlegd worden.

De ITSO maakt deel uit van het Computer Emergency Response Team (CERT-team), stuurt de dienstverlening rondom het Security Operations Center (SOC) aan, die is uitbesteed aan SURF. De rol van ITSO is belegd bij meerdere personen. De ITSO maakt deel uit van het CIO Office.

Computer Emergency Response Team (CERT)

Het CERT is het team van IT-professionals binnen de organisatie dat in staat is snel te handelen indien er sprake is van een IT Security incident met één of meerdere computers of het netwerk. Het doel is om schade te reduceren en snel herstel van dienstverlening te realiseren. Het CERT bestaat naast de ITSO's uit oproepbare specialisten binnen de organisatie.

Architectuur

De informatie architect borgt de implementatie van de baseline informatiebeveiliging en eventueel aanvullende maatregelen voortkomend uit de classificatie. Daarnaast bewaakt hij de consistentie van de maatregelen middels een projectstartarchitectuur.

Samenhang met privacy

Centrale Privacy Officer

De Centrale Privacy Officer (CPO) houdt zich binnen Tilburg University centraal bezig met de toepassing en naleving van de AVG en is adviseur op dit vlak.

Data Representative

De Data Representative is het eerste aanspreekpunt en de adviseur voor vragen over hoe om te gaan met privacy en persoonsgegevens, bijvoorbeeld bij een nieuwe of wijzing van een bestaande informatievoorziening. Iedere divisie en faculteit heeft lokaal een Data Representative aangesteld.

Samenhang met risicomanagement

Governance, Risk, Safety & Compliance Officer (GRSCO)

De GRSCO richt zich op het ontwikkelen, implementeren en onderhouden van beleid, processen en procedures om de algemene governance, risicobeheersing en compliance van de organisatie te waarborgen. De nadruk ligt op het creëren van een gestructureerde aanpak voor het beheersen van risico's en het voldoen aan de wet- en regelgeving. De GRSCO is onafhankelijk en rapporteert rechtstreeks aan het College van Bestuur. De coördinatie en monitoring van riskmanagement, is ondergebracht bij de onafhankelijk gepositioneerde afdeling Governance, Risk, Safety & Compliance binnen ES.

Samenhang met contractmanagement

Contractmanager
De contractmanager is altijd betrokken bij de aanschaf van centrale systemen en besteedt daarbij expliciet aandacht aan informatiebeveiliging. Dit doet zij door de informatiebeveiligingsmaatregelen uit de risico analyse onderdeel van het inkoopproces en van de inkoopvoorwaarden te maken en door het vastleggen van beveiligingseisen in contracten.

Derde lijn

De onafhankelijke derde lijn beoordeelt de betrouwbaarheid van informatie en systemen en adviseert over verbetering van het risicomanagement en de interne beheersing.

Internal Audit

Internal Audit levert vanuit haar onafhankelijke positie toegevoegde waarde door de opzet, bestaan en werking van de interne beheersing inzake informatiebeveiliging te toetsen. Zij voert controles uit of adviseert de eerste en tweede lijn over verbetermogelijkheden, waarbij ze ook kijkt of er geen overlap of blinde vlekken bestaan. Internal Audit rapporteert rechtstreeks aan de voorzitter van het College van Bestuur en aan de Auditcommissie (Stichtingbestuur). Internal Audit is onderdeel van de PDCA-cyclus (met name de onderdelen Check en Act).

Samenhang met privacy

Functionaris Gegevensbescherming
De FG houdt toezicht op de toepassing en naleving van de AVG en heeft een onafhankelijke positie. De FG rapporteert rechtstreeks aan de voorzitter van het College van Bestuur en wordt functioneel aangestuurd door het hoofd Governance, Risk, Safety & Compliance.

5.3 Strategisch, tactisch en operationeel

De bovengenoemde rollen en verantwoordelijkheden worden vertaald naar strategisch, tactisch en operationeel niveau:

- **Strategisch niveau**: op strategisch niveau wordt richtinggevend gesproken over governance, risk, safety en compliance, alsmede over doelen, scope en ambitie op het gebied van informatiebeveiliging, in samenhang met privacy.
- **Tactisch niveau**: 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.
- **Operationeel niveau**: het operationele niveau is verantwoordelijk voor de implementatie van de informatiebeveiligingsmaatregelen en de afhandeling van incidenten. Dat gebeurt in overleg met de functionele beheerders, relevante IT-functionarissen en waar nodig met de tactische laag.

In de volgende tabel is de governance structuur per niveau samengevat.

Niveau	Wat	Wie	Overleg
Richtinggevend (strategisch)	• Eindverantwoordelijk voor informatiebeveiliging binnen Tilburg University. • Bepalen, vaststellen en communiceren IB-strategie en beleid. • Organisatie t.b.v. IB inrichten. IB-planning en control vaststellen. • Business continuity	• College van Bestuur (de portefeuillehouder IB)	• Periodiek overleg CISO met portefeuillehouder IB

	management. • Communicatie naar management en organisatie.		
Sturend (tactisch)	• Monitoren toepassing en naleving van het IB-beleid. • Communicatie naar proceseigenaren. • Operationele verantwoordelijkheid informatiebeveiliging.	• Informatie-, proces- en systeemeigenaren • CISO • Information Security Officers • IT Security Officers • Centrale Privacy Officer	• Periodieke gesprekken met directeuren • Domeinoverleggen onderzoek, onderwijs en bedrijfsvoering
Uitvoerend (operationeel)	• Implementeren IB-maatregelen • Communicatie verzorgen naar eindgebruikers • Implementeren technische security- maatregelen • Security monitoring en advies • Registreren, analyseren en evalueren incidenten, inclusief datalekken	• Informatie-, proces- en systeemeigenaren • Leidinggevenden • Functioneel Beheerders • Informatiemanager • Information Security Officers • IT Security Officers • Awareness Officer • CERT • Centrale Privacy Officer • Functionaris Gegevensbescherming	• Het wekelijkse CISO Office overleg • Het vierwekelijkse Privacy & Security overleg • Elke 6 weken is het operationele Tilburg University CERT overleg. Ook een ISO neemt hieraan deel.

De governance structuur informatiebeveiliging samengevat in een tabel.

5.4 Documenten informatiebeveiliging

In het kader van informatiebeveiliging hanteert Tilburg University de volgende documenten:

Beleid/richtlijnen

1. **IB-beleid**: het IB-beleid ligt ten grondslag aan de aanpak van informatiebeveiliging binnen Tilburg University. Het beleid wordt opgesteld door de CISO en vastgesteld door het CvB.
2. **Baseline Informatiebeveiliging Tilburg University**: de baseline beschrijft de maatregelen die een minimumniveau van informatiebeveiliging waarborgen. Deze basismaatregelen dienen overal binnen Tilburg University geïmplementeerd te zijn.
3. **BIV-classificatierichtlijn:** aan de hand van een BIV-classificatie wordt bepaald of een systeem (of proces) meer beveiligingsmaatregelen nodig heeft dan die in de baseline zijn getroffen. De eigenaar is dan ook verplicht voor ieder systeem (of proces) van Tilburg University een BIV-classificatie uit te voeren. De classificatie vindt plaats aan de hand van de BIV-classificatierichtlijn en in afstemming met het CISO Office, die tevens ongevraagd kan adviseren. Afhankelijk van de waarde van de BIV-classificatie wordt bepaald welke beveiligingsmaatregelen er aanvullend geïmplementeerd moeten worden.
4. **Gedragscodes**: richtlijnen op het gebied van informatiebeveiliging voor medewerkers, studenten en derden (al dan niet voor specifieke doelgroepen).

Monitoring en verantwoording

5. **Information Security Management System** (proces en vastlegging).
6. **Risicoregister**
7. **Jaarplan/jaarverslag**: 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 CvB. 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. Waar nodig wordt apart aandacht besteed aan specifieke informatiesystemen. Het jaarplan wordt getoetst op de beschikbaarheid van resources (mensen en middelen), afgezet tegen de risico's die gemitigeerd moeten worden. Het jaarplan wordt vooraf afgestemd met het Privacy jaarplan wat door de FG wordt opgesteld. De verslagen worden geconsolideerd in de bestuurlijke Planning & Control-cyclus.

Informatiebeveiliging als vast onderdeel in documenten:

8. **Dienstenovereenkomsten (DVO's, SLA's), inhuur- en uitbestedingscontracten, non-disclosure agreements (NDA) en eventueel bijbehorende verwerkersovereenkomsten:** bij de inhuur van personeel en bij de inkoop van middelen (met name hardware en software) en diensten wordt expliciet aandacht besteed aan informatiebeveiliging. Dit wordt gedaan door o.a. het IB-beleid toe te passen op externen en door beveiliging standaard onderdeel van de inkoopvoorwaarden te maken. Afspraken worden in een contract met de leverancier vastgelegd en gecontroleerd. Het contract bevat standaard een informatiebeveiligingsparagraaf waarin de verantwoordelijkheden van de leverancier zijn opgenomen. De basis hiervoor is het SURF Juridisch Normenkader Cloudservices Hoger Onderwijs en STITCH (middels het opvragen van een actueel pentest rapport wordt gecontroleerd of aan STITCH voldaan is).
9. **Business Continuity Plan**: de divisies en faculteiten zijn zelf verantwoordelijk voor het calamiteitenplan en de bedrijfcontinuïteitsmaatregelen die ervoor zorgen dat de continuïteit van onderwijs, onderzoek en bedrijfsvoering gegarandeerd.

6. Bewustwording en training

Beleid en maatregelen zijn niet voldoende om risico's op het gebied van informatiebeveiliging uit te sluiten. De mens zelf is verantwoordelijk voor de grootste risico's. Binnen Tilburg University werken we daarom voortdurend aan het vergroten van het beveiligingsbewustzijn van de organisatie om de kennis van risico's te verhogen en om veilig en verantwoord gedrag aan te moedigen. Onderdeel van het beleid is het security en privacy awareness jaarplan, met regelmatig terugkerende bewustwordingscampagnes voor medewerkers en studenten. Hierbij is onderscheid gemaakt in verschillende doelgroepen en behoeften, zodat ook doelgroep specifieke bewustwordingscampagnes kunnen worden uitgevoerd. Verhoging van het beveiligingsbewustzijn is een verantwoordelijkheid van het management, ondersteund vanuit het CISO Office. Aandacht voor bewustwording is tevens een onderdeel van het introductieprogramma voor nieuwe medewerkers en studenten.

7. Controle, oefenen, naleving en sancties

De Internal Audit-afdeling is verantwoordelijk voor de (planning van) operational audits. Deze worden uitgevoerd door de Operational Auditor. Voor IT-audits wordt meestal gebruik gemaakt van externe auditors in verband met expertise. De CISO is verantwoordelijk voor de controle op de uitvoering van het informatiebeveiligingsjaarplan.

De interne controles vinden jaarlijks plaats en worden naast de periodieke audits aangevuld met diverse incidentele activiteiten, zoals het uitvoeren van deelwaarnemingen, het uit (laten) voeren van penetratietesten, vulnerability tests, assessments en het controleren van de feitelijke werking van de vastgestelde beveiligingsmaatregelen. Daarnaast worden vaardigheden en operationele procedures regelmatig getest in brainstormsessies of oefeningen. Een voorbeeld hiervan is de OZON-oefening die tweejaarlijks door SURF wordt gecoördineerd.

Het SURF normen- en toetsingskader IBHO, dat is gestoeld op ISO 27001/27002 en het NBA/NOREA Volwassenheidsmodel Informatiebeveiliging wordt gebruikt als uitgangspunt voor interne en externe controles.

Tilburg University neemt deel aan de externe SURF-audit, waarbij opzet, bestaan en werking van het informatiebeveiligingsbeleid worden getoetst. De externe SURF-audit vindt elk jaar plaats. Daarnaast neemt Tilburg University deel aan de SURF-selfassessment cyclus en de bijbehorende tweejaarlijkse benchmark (waarbij alleen opzet en bestaan worden getoetst). Minimaal eens per 4 jaar wordt een SURF Peerreview aangevraagd. De CISO levert input voor de audits.

Naar aanleiding van de bevindingen die uit tweede- en derdelijns activiteiten naar voren komen dient de proces-, systeem- of informatie-eigenaar een verbeterplan op te stellen. Dit verbeterplan dient minimaal te bevatten: actie, eindverantwoordelijke en deadline.

Naast het uitvoeren van interne en externe audits, vindt controle op de naleving plaats door monitoring vanuit de tweede lijn. Zo wordt binnen het SOC actief gemonitord op beveiligingsincidenten, kwetsbaarheden en dreigingen. Daarnaast houden leidinggevenden toezicht op de dagelijkse praktijk van informatiebeveiliging en spreken zij medewerkers en studenten aan in geval van tekortkomingen. Voor het toezicht op de naleving van de AVG is de FG verantwoordelijk.

Als uit de controles blijkt dat de naleving ernstig tekortschiet en er sprake is van verwijtbaar handelen, dan kan Tilburg University de betrokken verantwoordelijke medewerker of student een sanctie opleggen. De sanctie wordt opgelegd binnen de kaders van de wettelijke mogelijkheden (zoals Wet op het hoger onderwijs en wetenschappelijk onderzoek (WHW), cao, arbeidsovereenkomsten en de Code of Conduct). Primair is dit een verantwoordelijkheid van het CvB, maar dit kan in sommige gevallen worden gemandateerd aan de verantwoordelijke leidinggevenden (decaan/directeur).

8. Financiering

8.1 Centraal

De CISO dient een toereikend eigen budget te hebben om uitvoering te geven aan de strategische en tactische processen en de jaarplandoelen. Dit budget dient ook toereikend te zijn om tijdelijke medewerkers uit andere organisatiedelen toe te wijzen om informatiebeveiligingsprojecten gerealiseerd te krijgen.

8.2 Decentraal

Zoals aangegeven in hoofdstuk 5 van dit IB-beleid is de CISO niet eindverantwoordelijk voor informatiebeveiliging en is derhalve ook geen risico-eigenaar. Er ligt dan ook budget voor informatiebeveiligingsactiviteiten en -projecten in de lijn bij de divisies en faculteiten (respectievelijk de proces- en systeemeigenaren). Deze vorm van prioriteren en budgetteren dient verankerd te zijn in de planning– en control cyclus en in het project portfoliomanagement.

9. Melding en afhandeling van incidenten

Een incident is een gebeurtenis die de bedrijfsvoering negatief kan beïnvloeden. Incidentbeheer en -registratie gaat over het detecteren, vastleggen, analyseren en afhandelen van incidenten en verbeteringen naar aanleiding van lessons learned. 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. Incidentregistratie en periodieke rapportage over opgetreden incidenten horen thuis in een volwassen informatiebeveiligingsomgeving.

Incidenten kan men melden via het beveiligingsprobleem formulier[11] op intranet. Tilburg University heeft de contactgegevens van dit meldpunt duidelijk gecommuniceerd naar haar medewerkers, studenten en derden.
Iedere medewerker, student en derde is verantwoordelijk voor het signaleren en melden van incidenten en inbreuken op de informatiebeveiliging, inclusief datalekken. De incidenten worden afgehandeld volgens het vastgestelde Incident Managementproces, waar meldingen van datalekken ook een onderdeel van zijn. De FG handelt de gemelde datalekken af.

Tilburg University heeft een vastgesteld beleid voor Responsible Disclosure. Daarmee geeft Tilburg University melders van mogelijke kwetsbaarheden in de informatiesystemen een garantie dat Tilburg University, onder voorwaarden, geen juridische stappen tegen hen onderneemt.
Binnen Tilburg University is ook een Coördinerend SURF Contactpersoon (CSC)[12] voor SURF benoemd. De medewerker die deze rol (erbij) heeft, is een security vertegenwoordiger namens Tilburg University. Dit is met name van belang als er in verband met een incident vanuit SURF CERT of vanuit de politie contact wordt gezocht met Tilburg University. Dit contact verloopt dan altijd via de benoemde CSC

10. Vaststelling & wijziging

Het initiële IB-beleid is vastgesteld door het College van Bestuur op 7 september 2021. Het IB-beleid volgt de kaders van het instellingsbeleid en wordt minimaal 1x per 2 jaar geëvalueerd en zo nodig bijgesteld. Ook na een substantiële verandering van het instellingsbeleid of belangrijke ontwikkelingen op cyberveiligheidsgebied, wordt het beleid herzien door zorg van de CISO en opnieuw vastgesteld.

Evaluatie van het beleid heeft plaatsgevonden in maart 2024. Er zijn tekstuele wijzigingen en wijzigingen in de opmaak doorgevoerd.

Voor vragen of opmerkingen met betrekking tot dit beleid kun je terecht bij het CISO Office (ciso-office@tilburguniversity.edu).

[11] Zie https://www.tilburguniversity.edu/nl/form/report-security-problem.
[12] Zie Coördinerend SURF Contactpersoon, special interest groups | SURF.nl voor een overzicht van de CSC's.

Bijlage A – Schematisch overzicht inrichting ISMS

Informatiebeveiliging is een continu proces. Eerst moet worden vastgesteld wat nodig is en vervolgens moeten 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 controles aan een herijking toe zijn en zal daarom periodiek geëvalueerd moeten worden. Het gehele proces van informatiebeveiliging volgt daarmee 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.

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

Voorbereiding

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

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

Vervolgens moet het ISMS worden opgesteld.

De PDCA-cyclus omvat de volgende fasen:

Plan In de planfase worden de volgende zaken gedefinieerd: • Beleid • Scope • Bedrijfsmiddelen (assets) • Risico's en kansen • Middelen • Competenties • Bewustzijn • Communicatie • Gedocumenteerde informatie	**Do** Bij de uitvoering van het ISMS gaat het om: • De operationele planvorming en beheersing • Risicobeoordeling(en) • Risicobehandeling
Check De checkfase omvat de evaluatie van de werking van het ISMS: • Bewaking, meting, analyse en evaluatie • Rapportage • Interne audit • Management review	**Act** Op basis van de uitkomsten van de checkfase worden verbeteringen doorgevoerd. Vervolgens start een nieuwe PDCA-cyclus.

Bijlage B – Informatiebeveiligingsprincipes

1	**Risico-gebaseerd** Informatiebeveiligingsmaatregelen worden risico-gebaseerd genomen 
Achtergrond	Het delen van kennis (openheid) is een belangrijke kernwaarde van het onderwijs- en onderzoekproces van Tilburg University. 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 en onze zogenaamde risk appetite (risicobereidheid). Proportionaliteit daarin is gewenst, ook om de beschikbare financiële middelen efficiënt te gebruiken ('fit for purpose').
Implicaties	• Tilburg University voert voor alle processen en/of informatiesystemen een BIV-classificatie uit. • De risico's worden ingeschat en vastgesteld op basis van een risico-classificatie (zie bijlage C). • De risicoclassificatie wordt uitgevoerd op basis van de Classificatie Richtlijn. Waar nodig worden aanvullende maatregelen op de baseline maatregelen getroffen om het vastgestelde risico op beschikbaarheid, integriteit en vertrouwelijkheid te brengen naar het geaccepteerde niveau. • Informatie binnen Tilburg University heeft één eigenaar. • Eigenaren van informatie, informatiesystemen 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 Tilburg University, uiteindelijk te bepalen door het College van Bestuur. Voor afwijkingen wordt het risico-acceptatieproces gevolgd, met acceptatie door de proces-, systeem- of informatie-eigenaar. • Risico acceptaties worden, inclusief motivatie, gelogd in een centraal risicoregister. • De proces-, systeem- of informatie-eigenaar tekent voor acceptatie van de risico's. • Maatregelen worden zo ingericht dat hun effect controleerbaar is. • De hoogste risico's worden als eerste gemitigeerd. • Op basis van de risicoanalyse kan voor gebruiksgemak worden gekozen boven informatiebeveiliging. • Maatregelen moeten (qua kosten) in balans zijn met de vermindering van risico's (proportionaliteitsprincipe). • Informatie heeft één bron, waardoor eigenaarschap en "single source of truth" goed te duiden zijn. Hierdoor ontstaat ook een extra ketenverantwoordelijkheid voor de consequenties van wijzigingen bij de bron. • Tilburg University blijft verantwoordelijk voor adequate bescherming van informatie, ook bij gebruik van externe diensten voor informatieverwerking.

	• Waar van toepassing bevatten contracten de veiligheidseisen en de eis voor levering van externe toetsing (assurance) die laat zien dat maatregelen effectief zijn. • Software en diensten moeten aan diverse veiligheidseisen en normen voldoen. Tilburg University hanteert hiervoor STITCH en het SURF Juridisch Normenkader Cloudservices Hoger Onderwijs.

2	**Iedereen** Informatiebeveiliging is een verantwoordelijkheid van iedereen 
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 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 binnen Tilburg University.
Implicaties	• Directie en management stuurt op informatieveiligheid en privacybescherming en zorgt voor de juiste 'tone-at-the-top'. • Voor alle gebruikers van digitale informatievoorzieningen van Tilburg University is een Gedragscode beschikbaar die is gepubliceerd via de website van Tilburg University. • Het veilig omgaan met informatie en informatiedragers is een onderdeel van de aanstelling/arbeidsovereenkomst van alle medewerkers. • Tilburg University voert jaarlijks een security bewustwordingsprogramma uit. • Er is een verplichte deelname aan de training Digitaal Veilig Werken voor alle medewerkers. • Informatiebeveiliging krijgt aandacht bij indiensttreding van medewerkers en bij jaargesprekken. • Informatiebeveiliging krijgt aandacht in reguliere overleggen van 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 CERT (eventueel met tussenkomst van IT-support). • Er is een 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 
Achtergrond	De omgeving verandert continu; cyberdreigingen nemen toe en af; processen veranderen, medewerkers en studenten wisselen, 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 creëren en controles uitvoeren.
Implicaties	• Er is een Information Security Management Systeem (ISMS, Bijlage A) ingericht waarmee door middel van een PDCA-cyclus alle aspecten van het IB-beleid adequaat worden opgevolgd. • Periodiek worden audits en assessments uitgevoerd die het mogelijk maken het beleid en de genomen maatregelen te controleren op effectiviteit (controleerbaarheid). • Bij instroom van nieuwe medewerkers en studenten is er aandacht voor de bewustwording van de risico's en de beveiligingsprocedures van Tilburg University rond toegang en gebruik van IT-middelen. • Periodiek worden accounts met hoge privileges gevalideerd. • Tilburg University organiseert regelmatig privacy en (cyber)security bewustwordingsactiviteiten voor de diverse doelgroepen: studenten, medewerkers, leidinggevenden en samenwerkingspartners van Tilburg University. • 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 Tilburg University te bepalen en periodiek bij te stellen. Nieuwe dreigingen leiden waar nodig tot aanpassing van maatregelen.

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 
Achtergrond	Security by Design betekent dat al tijdens de start van een project, het ontwerp van een nieuw informatiesysteem 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	• Tilburg University heeft Security by Design opgenomen als architectuurprincipe. • Voor elk nieuw project/software/dienst-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 het uitgangspunt is om niet meer rechten te verlenen dan strikt noodzakelijk voor een 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 altijd herleidbaar is tot een verantwoordelijke gebruiker. • Er is een richtlijn "security in projecten" vastgesteld, gebaseerd op de maatregelen die voortkomen uit de risicoclassificatie en maatregelen die mogelijk voortvloeien uit de gegevens bescherming - effectbeoordeling (DPIA) in het kader van de AVG. • Bij het procesontwerp worden de maatregelen meegenomen die de continuïteit van het proces afdoende kunnen waarborgen.

5	**Security by Default** In elke configuratie die wordt geïmplementeerd staan de aanwezige security-opties standaard aan. 
Achtergrond	Security by Default voorkomt ongewenste en ongecontroleerde toegang tot (persoons)gegevens. Het openstellen van informatie en de inrichting van instellingen zijn daarmee altijd een bewuste keuze na een zorgvuldige afweging.
Implicaties	• Tilburg University heeft een Identity Access Management-proces ingericht, inhoudende dat HR in samenspraak met de betreffende leidinggevende de rechten van de gebruiker bepaalt op basis van de functie en de daarbij behorende rechten (vastgelegd in een autorisatie-schema) • De beveiligingsbaseline van de standaardconfiguratie wordt vastgelegd (bijv. het standaard beschermen van alle externe communicatie met TLS-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. • 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 – De BIV-classificatie

Classificatie volgens BIV (Beschikbaarheid – Integriteit – Vertrouwelijkheid) kan zowel toegepast worden op data zelf als op het informatiesysteem waarin data wordt verwerkt en/of opgeslagen, maar ook op processen. Op dit moment is de keuze gemaakt voor de TiU om classificaties te doen op informatiesystemen.

Wanneer we de noodzaak tot beschikbaarheid, integriteit en vertrouwelijkheid van de informatiesystemen willen beoordelen, moeten wel rekening houden wat voor type data er in dit informatiesysteem verwerkt wordt.

Het CISO-office (tweede lijn) adviseert en Internal Audit (derde lijn) ziet erop toe dat het proces verloopt zoals afgesproken. De classificatie richt zich op:

1. De classificatie van het informatiesysteem waarin data wordt vastgelegd;
2. De inventarisatie van de risico's;
3. De te nemen beveiligingseisen uit de baseline;
4. De samenhang tussen 1, 2 en 3.

Aspect		Laag	Midden	Hoog
Beschikbaarheid		B=1	B=2	B=3
Integriteit		I=1	I=2	I=3
Vertrouwelijkheid	V=0*	V=1	V=2	V=3

* Voor vertrouwelijkheid bestaat een vierde classificatie, V=0. Deze classificatie wordt gegeven aan informatie waarbij geen sprake is van vertrouwelijkheid en die als 'openbaar' gezien moet worden.

Aan de hand van de BIV-classificatie wordt aangetoond in hoeverre een informatiesysteem laag, midden of hoog scoort op de onderdelen beschikbaarheid, integriteit en vertrouwelijkheid. Als de BIV-classificatie in zijn totaliteit op laag of midden scoort, moet voldaan worden aan de basis beveiligingseisen, conform de baseline. Als men nog risico's ziet na de basiseisen dan zijn aanvullende maatregelen nodig om de risico's te kunnen mitigeren. Ook die beveiligingseisen die Tilburg University noodzakelijk acht bij een classificatie hoog, zijn beschreven in de baseline.

Bijlage D – Wet- en regelgeving

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

1. **Wet op het Hoger onderwijs en Wetenschappelijk onderzoek (WHW)**
   Tilburg University heeft een kwaliteitszorgsysteem conform de Instelling Toets Kwaliteitszorg (ITK). Hierin is (onder meer) het zorgvuldig omgaan met persoonsgegevens in de studentenadministratie en met de studieresultaten gewaarborgd. Daarnaast worden integriteitscodes voor wetenschappelijk onderzoek nageleefd en toegepast.

2. **Algemene Verordening Gegevensbescherming (AVG)**
   Tilburg University heeft een separaat gegevensbeschermingsbeleid vastgesteld waarin naleving van de AVG wordt geborgd. Naleving van het informatiebeveiliging- en gegevensbeschermingsbeleid, inclusief de daarin vermelde technische en organisatorische maatregelen, zorgen samen voor het voldoen aan de AVG.

3. **Wettelijke Bewaartermijnen/Archiefwet**
   Tilburg University 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. Tilburg University hanteert daarbij het Basisselectiedocument Wetenschappelijk Onderwijs (1985)[13] van de sector universiteiten/hogescholen. Dit selectiedocument gaat over alle informatie zoals die bijvoorbeeld is vastgelegd in (gedigitaliseerde) documenten, informatiesystemen, websites en e-mail. Dit is onderdeel van de jaarlijkse externe accountantsrapportages.

4. **Auteurswet**
   Tilburg University respecteert auteursrechten en handelt daarnaar.

5. **Telecommunicatiewet**
   Omdat de doelgroep van Tilburg University voldoende is afgebakend worden de netwerkvoorzieningen van Tilburg University 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 Tilburg University een adequaat basisniveau van beveiliging heeft tegen deze dreigingen. Indien er aanvallen op Tilburg University plaatsvinden die de beveiliging significant doorbreken en die vallen onder de Wet Computercriminaliteit, zal het bestuur van Tilburg University altijd aangifte doen.

[13] Referentie VH-document /referentie VSNU-document.

7. Network and Information Security Directive (NIS2)

Deze nieuwe Europese cybersecurity wetgeving gaat eind 2024 in Nederland gelden. De richtlijn is vastgesteld door de Europese Unie. Met als doel de cyberbeveiliging en de weerbaarheid van essentiële diensten in EU-lidstaten te verbeteren. Deze wet heeft de volgende verplichtingen:

- Zorgplicht: de organisatie voert risicobeoordelingen uit en past op basis daarvan passende maatregelen toe om de diensten te beveiligen.
- Meldplicht: incidenten worden binnen 24 uur bij de toezichthouder gemeld. Een cyberincident moet ook bij het Computer Security Incident Response Team (CSIRT) worden gemeld.
- Toezicht: er is een onafhankelijke (externe) toezichthouder die naar de naleving van de verplichtingen uit de richtlijn kijkt.

8. Overige codes en landelijke afspraken

Het informatiebeveiligingsbeleid is gebaseerd op het SURF Normenkader en Tilburg University is deelnemer in de Universiteiten van Nederland. Tilburg University is in dit kader gehouden aan de volgende codes en landelijke afspraken:

- Code goed bestuur universiteiten.
- Nederlandse gedragscode wetenschappelijke integriteit.
- SURF Norm- en toetsingskader Informatiebeveiliging Hoger Onderwijs.
- Basisselectie document WO/UMC.
- SURF-aansluitvoorwaarden.
- ISTLP (Information Sharing Traffic Light Protocol)

Bijlage E – Rollen informatiebeveiliging

Rollen uit informatiebeveiligingsbeleid
Awareness Officer
Centrale Privacy Officer
CERT-voorzitter (is onderdeel van de ITSO-rol)
Chief Information Officer
Chief Information Security Officer
College van Bestuur
Contractmanager
Data Representative
Functionaris Gegevensbescherming
Functioneel beheerders
Governance Risk, Safety & Compliance Officer
Hoofd Internal Audit
Informatiearchitect
Informatie-eigenaar
Informatiemanager
Information Security Officer
IT Security Officer
Management (decanen, directeuren)
Medewerkers
Portefeuillehouder informatiebeveiliging
Proceseigenaar
Risk Manager
Servicedesk/IT support/Student Desk
Stichtingsbestuur
Systeemeigenaar

Bijlage F – Inrichting van CERT

Het doel van het Computer Security Emergency Response Team (CERT) is het voorkomen van informatiebeveiligingsincidenten en ze te bestrijden als ze zich toch voordoen. Hierbij is het waarborgen van de continuïteit van Tilburg University en haar reputatie beschermen het resultaat. Het CERT houdt zich ook bezig met beveiligingsincidenten buiten Tilburg University als daar eigen medewerkers in enige rol bij betrokken zijn. In zulke gevallen wordt, als dat mogelijk is, gebruikgemaakt van de diensten van SURF-CERT die wereldwijd in verbinding staat met andere CERT's.

De voorzitter CERT stelt een Chapter/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 Tilburg University als geheel werkzaam is en haar opdracht direct van het CvB/CISO krijgt. Ook worden directe escalaties via de voorzitter CERT naar het bestuursniveau (via de CISO) vastgelegd. Tevens worden de directe contacten vastgelegd met de afdelingen c.q. personen die binnen Tilburg University zorgdragen voor juridische kwesties en contacten met de pers.

De ITSO (hoofd van CERT) adviseert in het geval er tijdelijk computersystemen of netwerksegmenten van Tilburg University moeten worden geïsoleerd. Hiertoe heeft het ITSO mandaat gekregen vanuit de directeur LIS/CIO.

Incidenten kunnen bij Tilburg University worden gemeld bij het CERT-meldpunt.
Tilburg University heeft de contactgegevens van dit meldpunt duidelijk gecommuniceerd naar haar medewerkers, studenten en derden.

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

Om incidenten op de juiste manier te kunnen afhandelen, worden ze in het relevante operationeel overleg besproken. In het geval dat het bedrijfsproces, de financiën of de goede naam van Tilburg University in gevaar zijn, wordt het incident ook met de CISO besproken. Bij het bespreken met de CISO wordt rekening gehouden met een eventueel op dat moment geldende vertrouwelijkheid voor het incident. Als er verontrustende trends worden geconstateerd speelt Tilburg University CERT hier proactief op in door het nemen van extra maatregelen of het creëren van (extra) bewustwording binnen de organisatie.