Informatiebeveiligingsbeleid

Aangepast door	Ludwig Geers / Koen Arts
Laatste Wijziging	05-01-2018
Document Ref	Informatiebeveiligingsbeleid 2.02.docx
Versie	2.02

Document Control

Wijzigingshistorie

Datum	Auteur	Versie	Status	Doorgevoerde wijzigingen
2013-03-26	T. Nijssen/ H. Kempff	0.24	Concept	Opmerkingen MT verwerkt
2013-12-11	T. Nijssen/ H. Kempff	0.25	Concept	Kleine aanpassingen
2014-03-05	T. Nijssen/ H. Kempff	DEF		Positief advies SIA naar CvB
08-05-2014		1.0		Vastgesteld door CvB
27-11-2015	H. Kempff	1.01		Aanpassingen door nieuwe ontwikkelingen
6-7-2017	L. Geers	1.02	Concept	Aanpassingen in het kader van de AVG, het autorisatiemechanisme en samenhang en invulling van functies
24-8-2017	L. Geers	1.03	Concept	Aanpassingen naar aanleiding van reacties van N. de Groot en J. Hoogervorst
12-9-2017	L. Geers	1.04	Concept	Reacties van het LIS-MT verwerkt
3-10	L. Geers	2.0	Definitief	Reacties van de Governance, Risk & compliance Officer verwerkt
5-1-2018	L. Geers	2.01	Concept	Aanpassingen naar aanleiding van de wijzigingen die in de Engelse samenvatting van ‘IBB 2.0 def’ zijn doorgevoerd. De Nederlandse samenvatting is toegevoegd en de relevante afwijkingen van de vorige versie zijn in dit document aangepast.
23-3-2018	L. Geers	2.02		Schema over Governance toegevoegd.

Distributie

Versie	Datum	Verzonden aan
0.24	2013-03-05	MT LIS
0.25	2013-12-11	H. Kempff, T. Nijssen
0.25	2014-02-17	SIA
DEF	2014-03-05	CvB
1.0		Alle schools en offices
1.01	1-7-2016	H. Kempff
1.02	6-7-2017	K. Arts
1.02	13-7-2017	Informatiemanagers TiU en J. Hoogervorst
1.03	24-8-2017	Koen Arts / LIS-MT
1.04	8-9-2017	Verwerkte besprekingscommentaar MT-LIS (5-9-2017)
2.0	10-10-2017	Koen Arts/LIS MT/SIA

Autorisatie

Versie	Datum	Geautoriseerd door
1.0		
2.0	5-9-2017	CvB
3.0		

Inhoud

1 Samenvatting

Introductie

In 2014 heeft het College van Bestuur (CvB) op advies van de Stuurgroep Informatievoorziening en Automatisering (SIA) de eerste versie van het Informatiebeveiligingsbeleid vastgesteld.

Het CvB heeft besloten het beleidsplan tweejaarlijks te actualiseren en aan te passen aan de veranderende omstandigheden. Het voorliggende plan is een bijstelling van de vorige versie.

Het CvB heeft intussen ook een notitie over de te volgen privacy strategie opgesteld. Het informatiebeveiligingsbeleid en deze privacy strategie zijn nauw met elkaar verbonden.

De belangrijkste wijzigingen in het informatiebeveiligingsbeleid komen dan ook voort uit het toenemend belang van de privacy en de bescherming van persoonsgegevens.

Het aanscherpen van het autorisatiemechanisme van concernsystemen, de invulling van specifieke beveiligingsfuncties in relatie tot de technologische ontwikkelingen en de veranderende terminologie als gevolg van de BEST-operatie zijn ook meegenomen in deze bijgestelde versie.

Dit document is een managementsamenvatting met hoofdlijnen en kan niet los gezien worden van het bijbehorende document ‘Informatiebeveiligingsbeleid TiU 2.0’.

Waarom informatiebeveiliging?

De universitaire processen (onderwijs, onderzoek, bedrijfsvoering) zijn in toenemende mate afhankelijk van ICT en informatiebeveiliging. Informatiebeveiliging omvat het treffen en onderhouden van een samenhangend pakket aan maatregelen om de beschikbaarheid, integriteit en vertrouwelijkheid (de zgn. BIV-classificatie) van de informatievoorziening te garanderen. Onderdeel van de informatiebeveiliging is ook de controleerbaarheid van de maatregelen die genomen zijn om deze drie aspecten te borgen.

Voor wie geldt dit informatiebeveiligingsbeleid?

Het informatiebeveiligingsbeleid binnen de universiteit heeft betrekking op alle medewerkers, studenten, bezoekers, externe relaties (inhuur / outsourcing), en op alle informatie die zij verwerken. Het informatiebeveiligingsbeleid is tevens van toepassing op alle apparaten van waaraf geautoriseerde toegang tot het instellingsnetwerk mogelijk is.

Gehanteerde beleidsuitgangspunten en principes

De universiteit hanteert als uitgangspunt de ISO 27002:2013-norm voor de informatiebeveiliging. Informatiebeveiliging is als proces ingericht en gebaseerd op de kwaliteitscirkel van Deming: Plan, Do, Check, Act.

In deze bijgewerkte versie van het informatiebeveiligingsbeleid worden: de volgende uitgangspunten gehanteerd:

- De universiteit is een open en toegankelijke instelling. Medewerkers en studenten moeten zich qua houding ‘fatsoenlijk’ gedragen.
- De beveiliging dient te voldoen aan de geldende wet- en regelgeving, in het bijzonder aan de Wet bescherming persoonsgegevens en de Algemene Verordening Gegevensbescherming.
- Informatiebeveiliging is een lijnverantwoordelijkheid.
- Informatiebeveiliging raakt alle medewerkers, studenten en bezoekers. Daarbij dienen de verwachtingen ten aanzien van individuen helder te zijn zodat ze actief kunnen bijdragen aan de informatieveiligheid.
- Informatiebeveiliging is een continu en iteratief verbeterproces.
- De onderwijsinstelling is als rechtspersoon eigenaar van de informatie die medewerkers onder haar verantwoordelijkheid opslaan, ontsluiten en beheren, tenzij dit voor bijvoorbeeld onderzoek anders is overeengekomen.
- Projectleiders van infrastructurele wijzigingen of van de aanschaf en invoering van nieuwe systemen moeten vanaf de start rekening houden met informatiebeveiliging.

Bescherming van informatie

De belangrijkste concernsystemen en de daarin verwerkte gegevens waarop dit informatiebeveiligingsbeleid van toepassing is, zijn geclassificeerd. De classificering is een continu proces en leidt tot een bijpassend set van maatregelen. De eigenaar van het betreffende informatiesysteem bepaalt de klasse en het beschermingsniveau.

- Voor beschikbaarheid van informatie worden de volgende klassen/beveiligingsniveaus onderkend:
    - Niet nodig, noodzakelijk, belangrijk en essentieel
- Voor de integriteit van informatie worden de volgende klassen/beveiligingsniveaus onderkend:
    - Niet beschermd, beschermd, hoog en absoluut.
- Voor de vertrouwelijkheid van informatie worden de volgende klassen/beveiligingsniveaus onderkend:
    - Openbaar, bedrijfsvertrouwelijk, vertrouwelijk en geheim

Welke wettelijke voorschriften worden gehanteerd?

De volgende wetten zijn van toepassing binnen Tilburg University en daarmee vormen zij onderdeel van het informatiebeveiligingsbeleid.

Wet bescherming persoonsgegevens

De Wet bescherming persoonsgegevens (Wbp) is de Nederlandse uitwerking van de Europese richtlijn bescherming persoonsgegevens (95/46/EG). De Wbp is sinds 1 september 2001 van kracht.

Algemene verordening gegevensbescherming

Per 25 mei 2018 is de Algemene verordening gegevensbescherming (AVG) van toepassing. Dat betekent dat er vanaf die datum dezelfde privacywetgeving geldt in de hele Europese Unie. De Wet bescherming persoonsgegevens geldt dan niet meer.

Archiefwet

De universiteit houdt zich aan de voorschriften uit de Archiefwet en het Archiefbesluit over de wijze waarop een organisatie moet omgaan met informatie vastgelegd in (gedigitaliseerde) documenten, informatiesystemen, websites, e.d.

Auteurswet

De universiteit verspreidt geen originele werken zonder dat daarvoor toestemming is verkregen van de eigenaar van de auteursrechten. Dit impliceert ook dat de instelling het gebruik van software zonder het bezitten van de juiste licenties tegengaat.

Wet Computercriminaliteit

Naleving van dit informatiebeveiligingsbeleid en handhaving van de wet computercriminaliteit moet leiden tot een voldoende niveau van beveiliging.

De telecommunicatiewet

De Telecommunicatiewet regelt in artikel 11.7 dat het versturen van reclame via e-mail alleen onder bepaalde omstandigheden is toegestaan.

Binnen Tilburg University zijn de volgende richtlijnen en landelijke afspraken van toepassing:

- VSNU gedragscode Wetenschappelijke integriteit
- VSNU gedragscode persoonsgegevens in Wetenschappelijk onderzoek
- Klachtprocedure Wetenschappelijke integriteit
- Klokkenluidersregeling
- Klachtenregeling ongewenst gedrag
- Gedragscode e-mail, internet en telefoonfaciliteiten

- Studielink-afspraken en audit procedures
- Aansluitvoorwaarden SURFconext / SURFnet.

Daarnaast voldoet de universiteit zoveel als mogelijk aan specifieke gemeenschappelijke landelijke afspraken in het hoger onderwijs veld.

Effectuering van het informatiebeveiligingsbeleid

Randvoorwaardelijk voor een goede uitvoering van het informatiebeveiligingsbeleid is een ingerichte organisatie met bijbehorende afspraken en verantwoordelijkheden. Deze governance komt neer op het goed, efficiënt en verantwoord leiden van een organisatie. Een goed governance-beleid op instellingsniveau zorgt ervoor dat er aandacht is voor de rechten van alle belanghebbenden.

Governance en organisatie van de informatiebeveiligingsfunctie

Onderdeel van governance is dat de universiteit aan alle soorten risico's en hun onderlinge verwevenheid passende aandacht schenkt. Het is om die reden dat de organisatie op strategisch niveau zowel aandacht schenkt aan informatiebeveiliging, als aan fysieke beveiliging, privacy en bedrijfscontinuïteit. Immers, samenwerking tussen deze disciplines is een noodzakelijke voorwaarde voor governance. De privacy is als gevolg van de Algemene Verordening Gegevensbescherming (AVG) verder uitgewerkt in privacy beleid en privacy statements.

Onderdeel van de governance is ook de IT-governance. Van belang daarbij is om onderscheid te maken naar het strategisch, het tactisch en het operationele niveau. Het streven is om het overleg op strategisch, tactisch of operationeel niveau zo mogelijk te houden bij bestaande overlegorganen, zoals het CvB, de SIA.

De volgende functies/rollen rondom informatiebeveiliging worden onderkend.

College van Bestuur

Het College van Bestuur is eindverantwoordelijk voor de informatiebeveiliging binnen de universiteit en stelt het beleid en de basismaatregelen op het gebied van informatiebeveiliging vast.

Portefeuillehouder informatiebeveiliging

De portefeuillehouder informatiebeveiliging is het Collegelid dat informatiebeveiliging in portefeuille heeft. Hij is eindverantwoordelijk voor informatiebeveiliging binnen de instelling.

Chief Information Officer (CIO)

De directeur van LIS is verantwoordelijk voor zowel de technische beveiliging als de informatie beveiliging en vervult hiermee de rol van Chief Information Officer (CIO). De hieronder genoemde beveiligingsfunctionarissen (ITSO en CISO) maken deel uit van verschillende afdelingen met ieder eigen, gescheiden, verantwoordelijkheden en adviseren de directeur van LIS. Bij tegenstrijdige belangen neemt de directeur van LIS een besluit.

Chief Information Security Officer

De Chief Information Security Officer is een rol op strategisch (en tactisch) niveau. Hij adviseert samen met de directeur LIS (CIO) en/of de afdeling Informatiemanagement het College van Bestuur. De Information Security Officer bewaakt de uniformiteit van de informatiebeveiliging binnen de instelling.

ICT Security Officer / coördinator CERT

De kern van de functie van de ICT Security Officer betreft de deskundigheid om op het snijvlak van ICT-techniek en informatiebeveiliging te opereren. Zowel als ontwerper, adviseur of auditor van beveiligingsfunctionaliteiten, als bij het dagelijkse beheer van complexe omgevingen die een hoog niveau van informatiebeveiliging vergen. Gelet op het raakvlak met het Computer Emergency Respons Team (CERT) is voor een combinatiefunctie gekozen.

Proceseigenaar

De proceseigenaar is verantwoordelijk voor een primair of ondersteunend proces, zoals inkoop, HRM en onderwijsadministratie. De proceseigenaar maakt afspraken over het technisch, applicatie en functioneel beheer en is verantwoordelijk voor het beleggen van deze beheersfuncties en wordt hierin door LIS ondersteund.

De functioneel beheerder

Die rol van het functioneel beheer is in dit verband het inrichten en verrichten van het functioneel beheer in afstemming met de informatiebeveiligingseisen.

Informatiearchitect

De informatiearchitect adviseert desgevraagd over specifieke informatiebeveiligingsmaatregelen in projecten (overkoepelende systemen) en bewaakt de consistentie van de maatregelen.

Leidinggevende

Naleving van het informatiebeveiligingsbeleid is onderdeel van de integrale bedrijfsvoering. Iedere leidinggevende heeft de taak om:

- er voor te zorgen dat zijn medewerkers op de hoogte zijn van het informatiebeveiligingsbeleid;
- toe te zien op de naleving van het informatiebeveiligingsbeleid door zijn medewerkers;
- periodiek het onderwerp informatiebeveiliging onder de aandacht te brengen in werkoverleggen;
- als aanspreekpunt beschikbaar te zijn voor alle personeel gerelateerde informatiebeveiligingszaken.

Functionaris gegevensbescherming (FG)/Data Protection Officer (DPO)

De functionaris voor de gegevensbescherming (FG) houdt binnen de universiteit toezicht op de toepassing en naleving van de Wet bescherming persoonsgegevens. De wettelijke taken en

bevoegdheden van de FG vereisen dat deze functionaris een onafhankelijke positie in de organisatie heeft.

CERT-coördinator

De IT-manager (MT-lid van LIS) benoemt de CERT-coördinator van de universiteit. Die opereert in diens opdracht en op instellingsniveau. Hij is bevoegd tot het isoleren of blokkeren van computersystemen, netwerksegmenten of gebruikersaccounts.

Governance, Risk & compliance Officer

Bij de divisie Executive Support is de Governance, Risk & compliance Officer benoemd.

Internal Auditor

Bij de Division Executive Support is de afdeling Internal Audit (IA) ingericht. De afdeling houdt Tilburg University als objectieve, onafhankelijke en kritische partner een spiegel voor die de organisatie helpt haar strategie en beleid binnen de juiste beheersingskaders ten uitvoer te brengen.

Over de bevindingen van deze audits wordt periodiek verantwoording afgelegd aan de Voorzitter van het College van Bestuur en de Audit Commissie van het Stichtingsbestuur.

Documenten informatiebeveiliging

In het kader van informatiebeveiliging hanteert de instelling de volgende documenten.

Het informatiebeveiligingsbeleid

Het informatiebeveiligingsbeleid ligt ten grondslag aan de aanpak van informatiebeveiliging binnen de instelling.

Basisniveau maatregelen

Dit basisniveau beschrijft de maatregelen die nodig zijn om instelling breed een minimaal niveau van informatiebeveiliging te kunnen waarborgen. Dit vloeit voort uit het beleid of uit besluiten die door het tactisch overleg genomen zijn.

Elke twee jaar komt dit niveau opnieuw aan de orde en kan de systeemeigenaar de klasse en maatregelen opnieuw bepalen. Het CvB neemt daarover een besluit na advies van de SIA.

Jaarplan/verslag

In een tweejaarlijkse cyclus leveren de CISO elke twee jaar een jaarverslag en een plan op. Het plan is mede gebaseerd op de resultaten van de periodieke controles / audits. Incidenten, resultaten van risicoanalyses (incl. genomen maatregelen) en andere initiatieven die de afgelopen twee jaar hebben plaatsgevonden vormen de basis van de rapportages en bijstellingen.

Bedrijfscontinuïteit Plan

Bedrijfscontinuïteit Management (BCM) is de benaming van het proces dat potentiële

bedreigingen voor een organisatie identificeert en bepaalt wat de impact op de “operatie” van de organisatie is als deze bedreigingen daadwerkelijk manifest worden. Dit plan is nog niet opgeleverd.

***Dienstenniveau overeenkomsten (DVO’s*)**
Een dienstverleningsovereenkomst is een overeenkomst tussen een leverancier en een afnemer. In deze overeenkomsten zit standaard een informatiebeveiligingsparagraaf, waarin de verantwoordelijkheden van de leverancier zijn opgenomen. Deze paragrafen zijn niet voor alle concernsystemen aanwezig.

Verwerkersovereenkomsten
Een verwerkersovereenkomst of data processing agreement (DPA) is een begrip uit de privacyregelgeving. Twee termen uit die privacyregelgeving staan centraal, dat zijn de begrippen 'verantwoordelijke' en 'bewerker'.
De verantwoordelijke is degene die het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. De verwerker (processor) is degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen. De verwerkersovereenkomst is de overeenkomst tussen verantwoordelijke en bewerker, waarin vastligt hoe de bewerker met de persoonsgegevens moet omgaan.

Inhuur- en uitbestedingscontracten
Bij de inhuur van diensten en personeel van derde partijen is informatiebeveiliging ook een aandachtspunt, bijvoorbeeld door te stellen dat het informatiebeveiligingsbeleid ook van kracht is voor derden. Hetzelfde uitgangspunt geldt voor uitbestedingen.

Policies
Dit zijn gedragscodes en richtlijnen voor medewerkers, studenten en derden, al dan niet voor specifieke doelgroepen, op het gebied van informatiebeveiliging. Zoals:

- spelregels (*acceptable use policy*) voor het gebruik van ICT-voorzieningen;
- wachtwoordregels;
- toepassing van crypto grafische hulpmiddelen;
- classificatierichtlijnen;
- gebruiks- en beheer voorwaarden;
- integriteits- en gedragscode voor ICT-functionarissen;
- gedragscode voor veilig e-mail- en internetgebruik.

Controle, naleving en sanctionering

Bij de universiteit van Tilburg initieert de Directeur LIS in samenwerking met de interne auditor de controle op de uitvoering van de informatiebeveiligingsjaarplannen.

Onafhankelijk accountants voeren periodiek de externe controles uit. Dit is gekoppeld aan het jaarlijkse accountantsonderzoek en dat zoveel mogelijk aansluit bij de normale Planning & Control cyclus.

De universiteit neemt iedere twee jaar deel aan een informatiebeveiligingsaudit de zogenaamde SURF audit. De uitkomsten hiervan zijn input voor de nieuwe jaarplannen. De naleving bestaat uit algemeen toezicht op de dagelijkse praktijk van het security management proces. Van belang hierbij is dat lijnmanagers hun verantwoordelijkheid nemen en hun medewerkers aanspreken in geval van tekortkomingen. Voor de bevordering van de naleving van de Wet Bescherming Persoonsgegevens vervult de functionaris gegevensbescherming een belangrijke rol. Hij rapporteert jaarlijks zijn bevindingen aan het CvB.

Het handelen van individuele medewerkers blijft de belangrijkste risicofactor. Daarom worden jaarlijks diverse bewustwordingscampagnes georganiseerd.

Bewustwording en training

Beleid en maatregelen zijn niet voldoende om risico’s op het terrein van informatiebeveiliging uit te sluiten. In de praktijk blijkt de mens meestal de belangrijkste risicofactor. Daarom organiseert de universiteit stelselmatig bewustwordingscampagnes voor medewerkers, studenten en gasten. Zulke campagnes kunnen aansluiten bij landelijke campagnes in het hoger onderwijs, zo mogelijk in afstemming met beveiligingscampagnes voor ARBO, milieu en veiligheid.

Melding en afhandeling van datalekken en incidenten

Onderdeel van de uitvoering van afspraken binnen de governance zijn incidentbeheer en –registratie. Beide hebben betrekking op de wijze waarop de medewerkers, studenten en onderzoekers geconstateerde dan wel vermoede inbreuken op de informatiebeveiliging -zoals datalekken-, moeten melden en de wijze waarop de organisatie deze afhandelt.

Het is van belang om te leren van incidenten. Incidentregistratie en periodieke rapportage over opgetreden incidenten horen thuis in een volwassen informatiebeveiligingsomgeving. Bij de instelling rapporteert de ICT Security Officer de securityincidenten ieder kwartaal aan de IT-directeur. De Functionaris Gegevensbescherming rapporteert tussentijds aan de desbetreffende directeuren en jaarlijks aan het CvB. Hiervoor is een protocol meldplicht datalekken en bijbehorende procedure opgesteld.

Elke eenheid en medewerker is zelf verantwoordelijk voor het signaleren en melden van incidenten en inbreuken op informatiebeveiliging. De lijnmanager en/of medewerker dient de incidenten en inbreuken direct te melden.

De incidenten worden afgehandeld en dienen als input voor de incidentrapportages, waarover in het operationeel overleg wordt gesproken. Bij constatering van bepaalde trends kan hierop meteen worden ingespeeld, bijvoorbeeld door het nemen van extra maatregelen of een bewustwordingscampagne.

Bij de behandeling van beveiligingsincidenten speelt het TiU-CERT team een essentiële rol. Het doel van het TiU-CERT is instelling brede preventie en curatieve zorg voor informatiebeveiligingsincidenten. Het CERT houdt zich ook bezig met beveiligingsincidenten buiten de universiteit als daar eigen medewerkers of studenten in enige rol bij betrokken zijn. In zulke gevallen maakt het CERT gebruik van de diensten van het SURF-CERT, dat wereldwijd in verbinding staat met andere CERT’s.

De dienstverlening van TiU-CERT bij de universiteit is gedocumenteerd en door het College van Bestuur bekrachtigd.

2 Inleiding

In 2014 heeft het College van Bestuur (CvB) op advies van de Stuurgroep Informatievoorziening en Automatisering (SIA) de eerste versie van het Informatiebeveiligingsbeleid vastgesteld.

Het CvB heeft besloten het beleidsplan tweejaarlijks te actualiseren en aan te passen aan de veranderende omstandigheden. Het voorliggende plan is een bijstelling van de vorige versie.

Het CvB heeft intussen ook een notitie over de te volgen privacy strategie opgesteld. Het informatiebeveiligingsbeleid en deze privacy strategie zijn nauw met elkaar verbonden.

De belangrijkste wijzigingen in het informatiebeveiligingsbeleid komen dan ook voort uit het toenemend belang van de privacy en de bescherming van persoonsgegevens.

Het aanscherpen van het autorisatiemechanisme van concernsystemen, de invulling van specifieke beveiligingsfuncties in relatie tot de technologische ontwikkelingen en de veranderende terminologie als gevolg van de BEST-operatie zijn ook meegenomen in deze bijgestelde versie.

2.1 Informatiebeveiliging

In het onderzoek- en onderwijsveld is men steeds meer afhankelijk van informatie en van computersystemen, waardoor nieuwe kwetsbaarheden en risico's optreden. Het is daarom van belang hiertegen adequate maatregelen te nemen. Immers, onvoldoende informatiebeveiliging kan leiden tot onacceptabele risico's bij de uitvoering van onderwijs en onderzoek en bij de bedrijfsvoering van de universiteit. Incidenten en inbreuken in deze processen kunnen leiden tot financiële schade en tot imagoverlies.

Informatiebeveiliging komt neer op het treffen en onderhouden van een samenhangend pakket aan maatregelen om de beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening te garanderen. De informatievoorziening omvat niet alleen de gegevens maar ook de functionaliteit om deze beschikbaar te stellen en te onderhouden.

De beschikbaarheid gaat over de mate waarin gegevens of functionaliteit op de juiste momenten beschikbaar zijn voor gebruikers.

De integriteit gaat over de mate waarin gegevens of functionaliteit juist ingevuld zijn.

De vertrouwelijkheid gaat over de mate waarin de toegang tot gegevens of functionaliteit beperkt is tot degenen die daartoe bevoegd zijn. *Zie ook Bijlage 1a, 1b en 1c.*

Onderdeel van de informatiebeveiliging is ook de controleerbaarheid van de maatregelen die genomen zijn om deze drie aspecten te borgen.

De universiteit van Tilburg heeft de ambitie om informatiebeveiliging permanent naar een hoger niveau te brengen. Dat doet de universiteit door de aspecten besturing (‘governance’), wet- en regelgeving, de organisatie van de beveiligingsfunctie en het informatiebeveiligingsbeleid – ook in hun onderlinge relatie - duidelijk te beschrijven, vast te stellen en aan te passen aan de veranderende omstandigheden.

2.2 Reikwijdte van het beleid

De universiteit van Tilburg heeft de insteek gekozen om informatiebeveiliging breed op te pakken. Daardoor ontstaat een belangrijke relatie en gedeeltelijke overlap met de aanpalende beleidsterreinen *privacy, beveiliging* (fysieke beveiliging) en *bedrijfscontinuïteit*. Op strategisch niveau krijgen deze raakvlakken zowel planmatig als inhoudelijk afstemming (*zie ook hoofdstuk 4*).

Het informatiebeveiligingsbeleid binnen de universiteit heeft betrekking op alle medewerkers, studenten, bezoekers en externe relaties (inhuur / outsourcing), alsmede op alle organisatieonderdelen en op alle informatie die zij verwerken. Tevens vallen onder het informatiebeveiligingsbeleid alle apparaten van waaraf geautoriseerde toegang tot het instellingsnetwerk mogelijk is.

Bij het informatiebeveiligingsbeleid ligt de nadruk op die toepassingen die vallen onder de verantwoordelijkheid van de instelling. Dit heeft vooral betrekking op gecontroleerde informatie, die de instelling zelf genereert en beheert. Toch valt niet-gecontroleerde informatie, bijv. uitspraken van studenten in discussies (op sociale media) en op (persoonlijke) websites, enigszins binnen de scope omdat de universiteit daarvoor ook aanspreekbaar is, of daardoor imagoschade kan oplopen.

3 Beleidsprincipes informatiebeveiliging

3.1 Beleidsuitgangspunten en principes

De universiteit hanteert ISO 27002:2013 als de standaard voor de informatiebeveiliging. Deze standaard sluit aan bij het Normenkader Informatiebeveiliging Hoger Onderwijs, dat aangeeft wat de universiteit minimaal geregeld moet hebben qua veiligheid en continuïteit om de bedrijfsgegevens en privacy van studenten en medewerkers te beschermen. Dit normenkader maakt het ook mogelijk vergelijkingen te maken tussen de Tilburgse situatie en die van andere onderwijsinstellingen in het Hoger Onderwijs.

Informatiebeveiliging is als proces ingericht en gebaseerd op de kwaliteitscirkel van Deming: Plan, Do, Check, Act.

De algemene beleidsuitgangspunten bij de universiteit zijn de volgende.

- De universiteit is een open en toegankelijke instelling. Medewerkers en studenten moeten zich qua houding ‘fatsoenlijk’ gedragen. Het is niet acceptabel dat door al dan niet opzettelijk gedrag onveilige situaties ontstaan die leiden tot schade en/of imagoverlies. Het is om deze reden dat er gedragscodes zijn geformuleerd en geïmplementeerd.
- De beveiliging dient te voldoen aan de geldende wet- en regelgeving, in het bijzonder aan de Wet bescherming persoonsgegevens en de Algemene Verordening Gegevensbescherming.

De universiteit van Tilburg concretiseert deze uitgangspunten in de volgende beleidsprincipes.

- Informatiebeveiliging is een lijnverantwoordelijkheid. Dat betekent dat de lijnmanagers (afdelingshoofden) de primaire verantwoordelijkheid dragen voor een goede informatie-beveiliging op hun afdeling of eenheid. Dit omvat ook de keuze van maatregelen en de uitvoering en handhaving ervan. Daarbij dient de instelling aan hen de (financiële en personele) middelen beschikbaar te stellen om die verantwoordelijkheid waar te kunnen maken.
- Informatiebeveiliging raakt alle medewerkers, studenten en bezoekers. Daarbij dienen de verwachtingen ten aanzien van individuen helder te zijn zodat ze actief kunnen bijdragen aan de informatieveiligheid. Dat gebeurt bijvoorbeeld in de aanstellingsbrief, tijdens functioneringsgesprekken, met een instelling brede gedragscode, met periodieke bewustwordingscampagnes, et cetera. Het opleggen van sancties na overtredingen maakt het geheel geloofwaardig.
- Informatiebeveiliging is een continu en iteratief verbeterproces. Technologische en organisatorische ontwikkelingen binnen en buiten de instelling maken het noodzakelijk om

periodiek te bezien of men nog wel op de juiste wijze bezig is de beveiliging te waarborgen. Op gezette tijden vinden audits plaats. Deze audits maken het mogelijk het beleid en de genomen maatregelen te controleren op haalbaarheid en effectiviteit.

- De onderwijsinstelling is als rechtspersoon eigenaar van de informatie die medewerkers onder haar verantwoordelijkheid opslaan, ontsluiten en beheren, tenzij dit voor bijvoorbeeld onderzoek anders is overeengekomen. Daarnaast beheert de instelling informatie, waarvan het eigendom toebehoort aan derden. Medewerkers en studenten dienen goed geïnformeerd te zijn over de regelgeving voor het (her)gebruik van deze informatie.
- Projectleiders van infrastructurele wijzigingen of van de aanschaf en invoering van nieuwe systemen moeten vanaf de start rekening houden met informatiebeveiliging. Dit ligt vast in het projectenprotocol.

3.2 Classificatie

Bij de universiteit zijn de belangrijkste concernsystemen en de daarin verwerkte gegevens waarop dit informatiebeveiligingsbeleid van toepassing is geclassificeerd.

Een risicoanalyse leidt tot de klasse c.q. het beveiligingsniveau van de informatie/informatiesystemen en bijpassende maatregelen.

Door de periodieke toetsing moet het niveau van de beveiligingsmaatregelen blijven aansluiten bij de klasse.

Voor beschikbaarheid van informatie gelden de volgende klassen/beveiligingsniveaus.

Klasse	Basisprincipes
Niet nodig	De gegevens kunnen zonder gevolgen langere tijd niet beschikbaar zijn. Schending van beschikbaarheid heeft geen gevolgschade.
Noodzakelijk	De informatie of service mag incidenteel uitvallen, het bedrijfsproces staat incidentele uitval toe. De continuïteit zal op redelijke termijn moeten worden hervat. Schending van deze classificatie kan enige (in)directe schade toebrengen.
Belangrijk	De informatie of service mag bijna nooit uitvallen, het bedrijfsproces staat nauwelijks uitval toe. De continuïteit zal snel moeten worden hervat. Schending van deze classificatie kan serieuze (in)directe schade toebrengen.
Essentieel	De informatie of service mag alleen in zeer uitzonderlijke situaties uitvallen, bijvoorbeeld als gevolg van een calamiteit, het bedrijf kritische bedrijfsproces staat eigenlijk geen uitval toe. De continuïteit zal zeer snel moeten worden hervat. Schending van integriteit kan (zeer) grote schade toebrengen.

Voor de integriteit van informatie gelden de volgende klassen/beveiligingsniveaus.

Klasse	Basisprincipes

Niet zeker	Deze informatie mag worden veranderd. Geen extra bescherming van integriteit noodzakelijk. Schending van integriteit heeft geen gevolgschade.
Beschermd	Het bedrijfsproces dat gebruik maakt van deze informatie staat enkele (integriteits-)fouten toe. Een basisniveau van beveiliging is noodzakelijk. Schending van deze classificatie kan enige (in-)directe schade toebrengen.
Hoog	Het bedrijfsproces dat gebruik maakt van deze informatie staat zeer weinig (integriteits-)fouten toe. Bescherming van integriteit is absoluut noodzakelijk. Schending van deze classificatie kan serieuze (in)directe schade toebrengen.
Absoluut	Het bedrijfsproces dat gebruik maakt van deze informatie staat geen (integriteits-)fouten toe. Schending van integriteit kan (zeer) grote schade toebrengen.

Voor de vertrouwelijkheid van informatie gelden de volgende klassen/beveiligingsniveaus.

Klasse	Basisprincipes
Openbaar	Alle informatie die algemeen toegankelijk is voor een ieder. Er is geen schending van deze classificatie mogelijk.
Bedrijfsvertrouwelijk	Informatie die toegankelijk mag of moet zijn voor alle medewerkers van de eigen organisatie(s). Vertrouwelijkheid is gering. Schending van deze classificatie kan enige (in)directe schade toebrengen.
Vertrouwelijk	Informatie die alleen toegankelijk mag zijn voor een beperkte groep gebruikers. De informatie wordt ter beschikking gesteld op basis van vertrouwen. Schending van deze classificatie kan serieuze (in)directe schade toebrengen.
Geheim	Dit betreft gevoelige informatie die alleen toegankelijk mag zijn voor de direct geadresseerde. Schending van deze classificatie kan zeer grote schade toebrengen.

Onderstaande tabel geeft weer welk beveiligingsniveau in principe bij welke klasse van informatie behoort.

Beschikbaarheid	
Niet nodig	Geen
Noodzakelijk	Bescherming basis
Belangrijk	Bescherming middel
Essentieel	Bescherming hoog
Integriteit	
Niet zeker	Geen
Beschermd	Bescherming basis
Hoog	Bescherming middel
Absoluut	Bescherming hoog
Vertrouwelijkheid	
Openbaar	Geen
Bedrijfsvertrouwelijk	Bescherming middel
Vertrouwelijk	Bescherming middel
Geheim	Bescherming hoog

De eigenaar van het betreffende informatiesysteem bepaalt de klasse en het beschermingsniveau.

‘Bescherming hoog’ is het hoogste beschermingsniveau bij de universiteit. Voor de beschrijving en uitwerking van genoemde beschermingsniveaus zie bijlage B. Classificatierichtlijnen.

4 Wet- en regelgeving

4.1 Wettelijke voorschriften

De volgende wetten zijn relevant voor het informatiebeveiligingsbeleid.

4.1.1 Wet bescherming persoonsgegevens

De Wet bescherming persoonsgegevens (Wbp) is de Nederlandse uitwerking van de Europese richtlijn bescherming persoonsgegevens (95/46/EG). De Wbp is sinds 1 september 2001 van kracht.

De universiteit heeft de wettelijke vereisten (juistheid en nauwkeurigheid van gegevens en passende technische en organisatorische maatregelen tegen verlies en onrechtmatige verwerking) geïmplementeerd via het informatiebeveiligingsbeleid. Naleving van de beveiligingsmaatregelen leidt tot voldoen aan de wet.

4.1.2 Algemene verordening gegevensbescherming

Per 25 mei 2018 is de Algemene verordening gegevensbescherming (AVG) van toepassing. Dat betekent dat er vanaf die datum dezelfde privacywetgeving geldt in de hele Europese Unie. De Wet bescherming persoonsgegevens geldt dan niet meer.

Als de algemene verordening gegevensbescherming van toepassing is, hebben organisaties die persoonsgegevens verwerken meer verplichtingen. De AVG legt meer nadruk op de verantwoordelijkheid van organisaties zelf om te kunnen aantonen dat zij zich aan de wet houden (accountability).

Het CvB heeft als gevolg van deze wet de te volgen strategie over de privacy opgesteld en vastgelegd in de notitie: Strategy data protection Tilburg University *From unconsious risk taking to controlled risk management.* Het informatiebeveiligingsbeleid en deze privacy strategie zijn nauw met elkaar verbonden.

4.1.3 Archiefwet

De bijzondere universiteiten, zoals de universiteit van Tilburg zijn een privaatrechtelijke instelling en vallen formeel niet onder de werking van de Archiefwet. De universiteit houdt zich wel aan de voorschriften uit de Archiefwet en het Archiefbesluit over de wijze waarop een organisatie moet

omgaan met informatie vastgelegd in (gedigitaliseerde) documenten, informatiesystemen, websites, e.d. Dit is onderdeel van de jaarlijkse externe accountantsrapportages.

4.1.4 Auteurswet

De **Auteurswet** (afgekort: Aw) is de wet die in Nederland het auteursrecht regelt. De wet werd aangenomen op 23 september 1912; ze kwam in de plaats van de oudere Auteurswet 1881 en is sindsdien meermalen gewijzigd. De wet regelt ook de zogenoemde persoonlijkheidsrechten.

De universiteit verspreidt geen originele werken zonder dat daarvoor toestemming is verkregen van de eigenaar van de auteursrechten. Dit impliceert ook dat de instelling het gebruik van software zonder het bezitten van de juiste licenties tegengaat.

4.1.5 Wet Computercriminaliteit

Per 1 september 2006 is de uit 1993 stammende wetgeving over computercriminaliteit of ook wel cybercrime ingrijpend veranderd. Vooral de definitie van computervredebreuk (soms ook wel "hacken" genoemd) is uitgebreid: elk opzettelijk en wederrechtelijk binnendringen in computersystemen is strafbaar, ook als daarbij geen beveiliging wordt gekraakt.

Het vernielen en onbruikbaar maken van computers, netwerken en gegevens was al langer strafbaar, maar het specifiek uitvoeren van denial-of-service aanvallen is nu apart strafbaar gesteld. De wetgeving over malware, zoals virussen, is aangescherpt. De regels over het afluisteren en aftappen van communicatie en het kraken of hacken van beveiligde diensten (zoals betaaltelevisie) zijn ook aangescherpt.

Naleving van dit informatiebeveiligingsbeleid en handhaving van de wet computercriminaliteit moet leiden tot een voldoende niveau van beveiliging.

4.1.6 De telecommunicatiewet

De Telecommunicatiewet regelt in artikel 11.7 dat het versturen van reclame via e-mail alleen onder bepaalde omstandigheden is toegestaan.

- Het versturen van ongevraagde communicatie voor commerciële, ideële of charitatieve doeleinden is in beginsel alleen toegestaan wanneer de betrokkene hiervoor voorafgaand toestemming heeft verleend (opt-in).
- Wanneer de ontvanger handelt in de uitoefening van zijn beroep of bedrijf is geen voorafgaande toestemming vereist voor ongevraagde communicatie. In dergelijke gevallen dient wel gebruik te worden gemaakt van contactgegevens die door de ontvanger voor dat doel zijn bestemd en bekend zijn gemaakt. Daarnaast is het mogelijk dat deze gebruiker buiten de Europese Economische Ruimte is gevestigd; dan dient te

worden voldaan aan de in dat land geldende voorschriften voor het verzenden van ongevraagde communicatie.

- Opt-in is niet vereist wanneer de communicatie gericht is op het aanbieden van producten en diensten die vergelijkbaar zijn met reeds eerder door de ontvanger afgenomen producten of diensten. Aanvullende voorwaarden zijn:
    - De ontvanger dient bij het verstrekken van zijn contactgegevens duidelijk en uitdrukkelijk de mogelijk zijn geboden om kosteloos verzet aan te tekenen tegen het gebruik van deze contactgegevens voor bovengenoemde doeleinden.
    - Bij elke verzonden communicatie moet opnieuw de mogelijkheid worden geboden om verzet aan te tekenen tegen het verder gebruik van deze contactgegevens (opt-out).

4.2 Overige richtlijnen en landelijke afspraken

Zoals eerder gesteld is het informatiebeveiligingsbeleid bij de universiteit gebaseerd op ISO 27002:13.

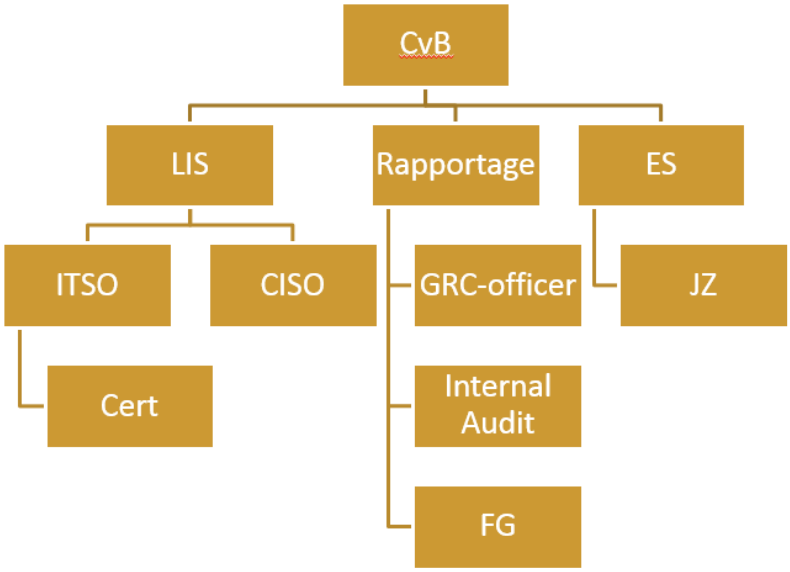
De universiteit voldoet aan de volgende richtlijnen en landelijke afspraken:

- Regeling Wetenschappelijke integriteit
- Klachtprocedure Wetenschappelijke integriteit
- Klokkenluidersregeling
- Klachtenregeling ongewenst gedrag
- Gedragscode e-mail, internet en telefoonfaciliteiten
- Studielink-afspraken en audit procedures
- Aansluitvoorwaarden SURFconext / SURFnet.

Daarnaast voldoet de universiteit zoveel als mogelijk aan specifieke gemeenschappelijke landelijke afspraken in het hoger onderwijs veld.

5 Governance informatiebeveiligingsbeleid

Governance komt neer op het goed, efficiënt en verantwoord leiden van een organisatie. Het omvat vooral ook de relatie met de belangrijkste belanghebbenden van de instelling, zoals het college van bestuur, werknemers, studenten, andere afnemers en de samenleving als geheel. Een goed governance-beleid op instellingsniveau zorg ervoor dat er aandacht is voor de rechten van alle belanghebbenden. De onderstaande partijen spelen hun specifieke rol in de governance.



nce.

5.1 Afstemming met aanpalende beleidsterreinen

Onderdeel van governance is dat de universiteit aan alle soorten risico's en hun onderlinge verwevenheid passende aandacht schenkt. Het is om die reden dat de organisatie op strategisch niveau zowel aandacht schenkt aan informatiebeveiliging, als aan fysieke beveiliging, privacy en bedrijfscontinuïteit. Immers, samenwerking tussen deze disciplines is een noodzakelijke voorwaarde voor governance. Dit is vormgegeven door de (budgettaire) planningscyclus voor deze aspecten parallel te laten verlopen. Dat biedt handvatten om onderlinge interferentie op te merken en te behandelen. Waar wenselijk en mogelijk vertaalt de organisatie dit naar het tactische en operationele niveau, maar alleen daar waar het toegevoegde waarde biedt.

De privacy is als gevolg van de Algemene Verordening Gegevensbescherming (AVG) verder uitgewerkt in privacy beleid en privacy statements.

5.2 Inpassing in de IT-governance van de instelling

Deze paragraaf geeft weer hoe IT-governance in de instelling is georganiseerd en wie waarvoor verantwoordelijk is. Van belang daarbij is om onderscheid te maken naar het strategisch, het tactisch en het operationele niveau.

Het streven is om het overleg op strategisch, tactisch of operationeel niveau zo mogelijk te houden bij bestaande overlegorganen.

Niveau	Wat?	Wie?	Overleg	Documenten
Richtinggevend	• Bepalen IB-strategie • Organisatie t.b.v. IB inrichten • IB-planning en control vaststellen • Bedrijfscontinuïteit management organiseren	CvB, o.b.v. advies van de Stuurgroep Informatie en Automatisering (SIA), waarin de directeur LIS als CIO en de CISO vertegenwoordigd is.	• CvB stelt vast • SIA adviseert	• IB-beleidsplan • IB-baseline (basis maatregelen) • Bedrijfscontinuïteitplan
Sturend	Planning & Control IB: • voorbereiden normen en wijze van toetsen • evalueren beleid en maatregelen • begeleiding externe audits	• Systeem eigenaren • Governance, Risk & Compliance Officer • Chief Information Security Officer	• bilateraal overleg	• Risicoanalyses en audits • Jaarplan en verslag
Uitvoerend	• implementeren IB-maatregelen • registreren en evalueren incidenten • communicatie eindgebruikers	• Chief Information Security Officer • Informatie managers • CERT • Functioneel beheerders	• Periodiek Privacy en Security overleg	• Besluitenlijsten, protocollen, procedures, PIA's, Bewerkersovereenkomsten • Incidentregistratie incl. evaluatie

De financiering van informatiebeveiliging is bij de universiteit als volgt geregeld.

Algemene zaken, zoals het opstellen van een informatiebeveiligingsplan voor de gehele instelling of een externe audit komen uit het centrale ICT-budget. De beveiliging van informatiesystemen

komen ten laste van het informatiesysteem zelf. Beveiligingskosten van werkplekken maken integraal onderdeel uit van de werkplekkosten.

Het zelfde geldt voor bewustzijn en training: brede bewustwordingscampagnes (centraal gefinancierd) en lokale voorlichting en training voor specifieke toepassingen of doelgroepen (decentraal gefinancierd).

5.3 Documenten informatiebeveiliging

In het kader van informatiebeveiliging heeft de instelling de volgende documenten:

1. **Het informatiebeveiligingsbeleid**
   Het informatiebeveiligingsbeleid ligt ten grondslag aan de aanpak van informatiebeveiliging binnen de instelling. In het informatiebeveiligingsbeleid worden de randvoorwaarden en uitgangspunten vastgelegd en de wijze waarop het beleid wordt vertaald in concrete maatregelen. Om er voor te zorgen dat het beleid gedragen wordt binnen de organisatie en de organisatie er naar handelt wordt het uitgedragen door (of namens) het College van Bestuur.

2. **Basisniveau maatregelen**
   Dit basisniveau beschrijft de maatregelen die nodig zijn om instelling breed een minimaal niveau van informatiebeveiliging te kunnen waarborgen. Dit vloeit voort uit het beleid of uit besluiten die door het tactisch overleg genomen zijn.

   Elke twee jaar komt dit niveau opnieuw aan de orde en kan de systeemeigenaar de klasse en maatregelen opnieuw bepalen. Het CvB neemt daarover een besluit na advies van de SIA.

3. **Jaarplan/verslag**
   In een tweejaarlijkse cyclus leveren de CISO elke twee jaar een jaarverslag en een plan op. Het plan is mede gebaseerd op de resultaten van de periodieke controles / audits. Incidenten, resultaten van risicoanalyses (incl. genomen maatregelen) en andere initiatieven die de afgelopen twee jaar hebben plaatsgevonden vormen de basis van de rapportages en bijstellingen. Dergelijke verslagen kunnen eventueel geconsolideerd worden in de bestuurlijke Planning & Control-cyclus. Waar nodig wordt apart aandacht besteed aan decentrale systemen.

4. **Bedrijfscontinuïteit Plan**
   Bedrijfscontinuïteit Management (BCM) is de benaming van het proces dat potentiële bedreigingen voor een organisatie identificeert en bepaalt wat de impact op de “operatie” van de organisatie is als deze bedreigingen daadwerkelijk manifest worden. Het product van BCM bestaat uit een samenhangend stelsel van maatregelen, die zowel preventief, detectief, repressief als correctief werkzaam zijn.

Library & IT Services stelt in samenwerking met Facility Services het bedrijfscontinuïteitsplan op. Dit plan is nog niet opgeleverd

5. **Dienstenniveau overeenkomsten (DVO's)**
   Een dienstverleningsovereenkomst is een overeenkomst tussen een leverancier en een afnemer. Bijvoorbeeld de IT-afdeling sluit met externe leveranciers een DVO af ten behoeve van de ondersteuning van concernsystemen. Dat zijn contracten met afspraken en randvoorwaarden over geleverde diensten. In deze contracten zit standaard een informatiebeveiligingsparagraaf, waarin de verantwoordelijkheden van de leverancier zijn opgenomen. Deze paragrafen zijn niet voor alle concernsystemen aanwezig.

6. **Verwerkersovereenkomsten**

   Een verwerkersovereenkomst of *data processing agreement* (DPA) is een begrip uit de privacyregelgeving. Twee termen uit die privacyregelgeving staan centraal, dat zijn de begrippen 'verantwoordelijke' en 'bewerker'.

   De *verantwoordelijke* is degene die het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. Denk hierbij aan de universiteit die persoonsgegevens van de werknemers bijhoudt met het oog op bijvoorbeeld de salarisadministratie (naam, adres, bankrekeningnummer enz.). De universiteit is verantwoordelijk voor de gegevens.

   De *verwerker* (processor) is degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen. In bovengenoemd voorbeeld zou dit de dienstverlener zijn waar de salarisgegevens zijn opgeslagen.

   De **verwerkersovereenkomst** is de overeenkomst tussen verantwoordelijke en bewerker, waarin vastligt hoe de bewerker met de persoonsgegevens moet omgaan. In bovengenoemd voorbeeld moeten de universiteit en de dienstverlener dus een schriftelijke overeenkomst met elkaar aangaan.

7. **Inhuur- en uitbestedingscontracten**
   Bij de inhuur van diensten en personeel van derde partijen is informatiebeveiliging ook een aandachtspunt, bijvoorbeeld door te stellen dat het informatiebeveiligingsbeleid ook van kracht is voor derden. Hetzelfde uitgangspunt geldt voor uitbestedingen.

   Policies
   Dit zijn gedragscodes en richtlijnen voor medewerkers, studenten en derden, al dan niet voor specifieke doelgroepen, op het gebied van informatiebeveiliging. Zoals:

- spelregels (*acceptable use policy*) voor het gebruik van ICT-voorzieningen;
- wachtwoordregels;
- toepassing van crypto grafische hulpmiddelen;
- classificatierichtlijnen;
- gebruiks- en beheer voorwaarden;
- integriteits- en gedragscode voor ICT-functionarissen;
- gedragscode voor veilig e-mail- en internetgebruik.

5.4 Controle, naleving en sancties

Bij de universiteit van Tilburg initieert de Chief Information Security Officer in samenwerking met de interne auditor de controle op de uitvoering van de informatiebeveiligingsjaarplannen.

Onafhankelijk accountants voeren periodiek de externe controles uit. Dit is gekoppeld aan het jaarlijkse accountantsonderzoek en dat zoveel mogelijk aansluit bij de normale Planning & Control cyclus.

De universiteit houdt ook elke twee jaar een audit op de informatiebeveiliging, de zogenaamde SURF audit.

De bevindingen van de interne en externe audits zijn input voor de nieuwe jaarplannen van de universiteit.

De naleving bestaat uit algemeen toezicht op de dagelijkse praktijk van het security management proces. Van belang hierbij is dat lijnmanagers hun verantwoordelijkheid nemen en hun medewerkers aanspreken in geval van tekortkomingen. Voor de bevordering van de naleving van de Wet Bescherming Persoonsgegevens vervult de functionaris gegevensbescherming een belangrijke rol. Hij rapporteert jaarlijks zijn bevindingen aan het CvB.

Mocht de naleving ernstig tekort schieten, dan kan de universiteit de betrokken verantwoordelijke medewerkers een sanctie opleggen, binnen de kaders van de CAO en de wettelijke mogelijkheden.

5.5 Bewustwording en training

Beleid en maatregelen zijn niet voldoende om risico’s op het terrein van informatiebeveiliging uit te sluiten. In de praktijk blijkt de mens meestal de belangrijkste risicofactor. Daarom organiseert de universiteit stelselmatig bewustwordingscampagnes voor medewerkers, studenten en gasten. Zulke campagnes kunnen aansluiten bij landelijke campagnes in het hoger onderwijs, zo mogelijk in afstemming met beveiligingscampagnes voor ARBO, milieu en veiligheid.

5.6 Organisatie van de informatiebeveiligingsfunctie

Om informatiebeveiliging gestructureerd en gecoördineerd op te pakken wordt bij de universiteit een aantal rollen onderkend die aan functionarissen in de bestaande organisatie zijn toegewezen.

5.6.1 College van Bestuur

Het College van Bestuur is eindverantwoordelijk voor de informatiebeveiliging binnen de universiteit en stelt het beleid en de basismaatregelen op het gebied van informatiebeveiliging vast. De inhoudelijke verantwoordelijkheid voor informatiebeveiliging is gemandateerd aan de Chief Information Security Officer. Deze heeft de opdracht om voor de informatiebeveiliging voor de gehele instelling zorg te dragen.

5.6.2 Portefeuillehouder informatiebeveiliging

De portefeuillehouder informatiebeveiliging is het Collegelid dat informatiebeveiliging in portefeuille heeft. Hij is eindverantwoordelijk voor informatiebeveiliging binnen de instelling.

5.6.3 Chief Information Officer (CIO)

De directeur van LIS is verantwoordelijk voor zowel de technische beveiliging als de informatie beveiliging en vervult hiermee de rol van Chief Information Officer (CIO). De hieronder genoemde beveiligingsfunctionarissen (ITSO en CISO) maken deel uit van verschillende afdelingen met ieder eigen, gescheiden, verantwoordelijkheden en adviseren de directeur van LIS. Bij tegenstrijdige belangen neemt de directeur van LIS een besluit.

5.6.4 Chief Information Security Officer

De Chief Information Security Officer is een rol op strategisch (en tactisch) niveau. Hij adviseert samen met de directeur LIS (CIO) en/of de afdeling Informatiemanagement het College van Bestuur. De Information Security Officer bewaakt de uniformiteit binnen de instelling.

5.6.5 ICT Security Officer / coördinator CERT

De kern van de functie van de ICT Security Officer betreft de deskundigheid om op het snijvlak van ICT-techniek en informatiebeveiliging te opereren. Zowel als ontwerper, adviseur of auditor van beveiligingsfunctionaliteiten, als bij het dagelijkse beheer van complexe omgevingen die een hoog niveau van informatiebeveiliging vergen. Gelet op het raakvlak met het Computer Emergency Respons Team (CERT) is voor een combinatiefunctie gekozen.

5.6.6 Proceseigenaar

De proceseigenaar is verantwoordelijk voor een primair of ondersteunend proces, zoals inkoop, HRM en onderwijsadministratie. De proceseigenaar maakt afspraken over het technisch,

applicatie en functioneel beheer en is verantwoordelijk voor het beleggen van deze beheersfuncties en wordt hierin door LIS ondersteund.

5.6.7 De functioneel beheerder

Die rol van het functioneel beheer is in dit verband het inrichten en verrichten van het functioneel beheer in afstemming met de informatiebeveiligingseisen.

De toegevoegde waarde van functioneel beheer hierin is dat zij kunnen faciliteren in wat goede oplossingsmogelijkheden zijn, in het kader van wijzigingenbeheer en behoeftemanagement, en dat de informatievoorziening wordt gebruikt volgens de informatiebeveiligingsvoorschriften.

5.6.8 Informatiearchitect

De informatiearchitect adviseert desgevraagd over specifieke informatiebeveiligingsmaatregelen in projecten (overkoepelende systemen) en bewaakt de consistentie van de maatregelen.

5.6.9 Leidinggevende

Naleving van het informatiebeveiligingsbeleid is onderdeel van de integrale bedrijfsvoering. Iedere leidinggevende heeft de taak om:

- er voor te zorgen dat zijn medewerkers op de hoogte zijn van het informatiebeveiligingsbeleid;
- toe te zien op de naleving van het informatiebeveiligingsbeleid door zijn medewerkers;
- periodiek het onderwerp informatiebeveiliging onder de aandacht te brengen in werkoverleggen;
- als aanspreekpunt beschikbaar te zijn voor alle personeel gerelateerde informatiebeveiligingszaken.

5.6.10 Functionaris gegevensbescherming (FG) / Data Protection Officer (DPO)

De functionaris voor de gegevensbescherming (FG) houdt binnen de universiteit toezicht op de toepassing en naleving van de Wet bescherming persoonsgegevens. De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie in de organisatie.

5.6.11 CERT-coördinator

De IT-manager (MT-lid van LIS) benoemt de CERT-coördinator van de universiteit. Die opereert in diens opdracht en op instellingsniveau. Hij is bevoegd tot het isoleren of blokkeren van computersystemen, netwerksegmenten of gebruikersaccounts.

.

5.6.12 Governance, Risk & compliance Officer

Bij de Division Executive Support is de Governance, Risk & compliance Officer benoemd met de volgende rol/taken:

- Initiërende en coördinerende rol bij het aangeven van kaders voor:
    - Inrichting van de administratieve organisatie / interne beheersing structuur en het inbouwen van de noodzakelijke functiescheidingen binnen TiU
    - Opzetten en (laten) uitvoeren van een TiU brede risicomanagementbeleid (strategisch, tactisch en operationeel) voor alle domeinen.
- Verantwoordelijk voor het opzetten en onderhouden van een (control) framework (inclusief compliance) voor TiU door middel van het opstellen van richtlijnen, standaarden, procedures, methoden en technieken van GRC management.
- Faciliteert door middel van workshops de uitvoering van een risico analyse om zowel organisatorisch als compliance risico's in beeld te krijgen.
- Inventariseert en analyseert periodiek alle risico's die de realisatie van de doelstellingen van TiU kunnen beïnvloeden op strategisch, tactisch en operationeel niveau.
- Bewaakt de integriteit van de organisatie en de medewerkers en zorgt voor verankering hiervan binnen de strategie en het beleid van TiU en het gedrag van medewerkers.
- Zorgt tevens voor het monitoren van de geïdentificeerde risico's (o.a. transacties en gedragingen van medewerkers voor het compliance stuk en rapporteert over bevindingen.

5.6.13 Internal Auditor

Bij de Division Executive Support is de afdeling Internal Audit (IA) ingericht. De afdeling houdt Tilburg University als objectieve, onafhankelijke en kritische partner een spiegel voor die de organisatie helpt haar strategie en beleid binnen de juiste beheersingskaders ten uitvoer te brengen.

Doelstelling van Internal Audit is dat door haar onafhankelijke toetsende functie het bestuur en het management over de meest risicovolle processen en beleidsmaatregelen aanvullende zekerheid krijgt of de organisatie wel op de meest doelmatige en effectieve wijze is ingericht en functioneert.

Internal Audit levert toegevoegde waarde door de opzet, het bestaan en de werking van de interne beheersing te onderzoeken door middel van operational audits. Over de bevindingen van deze audits wordt periodiek verantwoording afgelegd aan de Voorzitter van het College van Bestuur en de Audit Commissie van het Stichtingsbestuur.

5.7 Overleg

Om de samenhang in de organisatie van de informatiebeveiligingsfunctie goed tot uitdrukking te laten komen en de initiatieven en activiteiten op het gebied van informatiebeveiliging binnen de verschillende onderdelen op elkaar af te stemmen vindt bij de instelling gestructureerd overleg plaats over het onderwerp informatiebeveiliging op vele niveaus.

Op strategisch niveau wordt richtinggevend gesproken over besturing (‘governance’) en naleving (‘compliance’), alsmede over doelen, bereik en ambitie op het gebied van informatievoorziening en -beveiliging. Dit gebeurt in het strategisch ICT-overleg van de Stuurgroep Informatie en Automatisering en in de verschillende Business Information Plannings- processen van de desbetreffende School of Office.

Op tactisch niveau wordt de strategie vertaald naar plannen, te hanteren normen, evaluatiemethoden, e.d. Deze plannen en instrumenten zijn sturend voor de uitvoering. Dit tactisch overleg is per School of Office georganiseerd.

Op operationeel niveau worden de zaken besproken die de dagelijkse bedrijfsvoering (uitvoering) aangaan. Deze overlegvorm is zeer decentraal georganiseerd, indien nodig in elk organisatieonderdeel.

6 Melding en afhandeling van datalekken en incidenten

Onderdeel van de uitvoering van afspraken binnen de governance zijn incidentbeheer en –registratie. Beide hebben betrekking op de wijze waarop de medewerkers, studenten en onderzoekers geconstateerde dan wel vermoede inbreuken op de informatiebeveiliging -zoals datalekken-moeten melden en de wijze waarop de organisatie deze afhandelt.

Het is van belang om te leren van incidenten. Incidentregistratie en periodieke rapportage over opgetreden incidenten horen thuis in een volwassen informatiebeveiligingsomgeving. Bij de instelling rapporteert de ICT Security Officer de securityincidenten ieder kwartaal aan de IT-directeur. De Functionaris Gegevensbescherming rapporteert tussentijds aan de desbetreffende directeuren en jaarlijks aan het CvB. Hiervoor is een protocol meldplicht datalekken en bijbehorende procedure opgesteld.

Elke eenheid en medewerker is zelf verantwoordelijk voor het signaleren en melden van incidenten en inbreuken op informatiebeveiliging. De lijnmanager en/of medewerker dient de incidenten en inbreuken direct te melden.

De incidenten worden afgehandeld en dienen als input voor de incidentrapportages, waarover in het operationeel overleg wordt gesproken. Bij constatering van bepaalde trends kan hierop meteen worden ingespeeld, bijvoorbeeld door het nemen van extra maatregelen of een bewustwordingscampagne.

6.1 Computer Emergency Response Team (CERT)

Het doel van het TiU-CERT is instelling brede preventie en curatieve zorg voor informatiebeveiligingsincidenten. Het CERT houdt zich ook bezig met beveiligingsincidenten buiten de universiteit als daar eigen medewerkers of studenten in enige rol bij betrokken zijn. In zulke gevallen maakt het CERT gebruik van de diensten van het SURF-CERT, dat wereldwijd in verbinding staat met andere CERT’s.

De leden van het TiU-CERT zijn benoemd door de IT-directeur en opereren in diens opdracht.

TiU-CERT is gerechtigd het isoleren van computersystemen of netwerksegmenten te gelasten. TiU-CERT is ook bevoegd *penetration* tests uit te voeren om na te gaan of systemen en netwerken adequaat beveiligd zijn.

TiU-CERT heeft de volgende opdracht:

- het signaleren en registreren van alle beveiligingsincidenten, het coördineren van de bestrijding en het toezien op de oplossing van problemen die tot incidenten hebben geleid of door de incidenten zijn veroorzaakt (of het bieden van ondersteuning daarbij);
- het geven van voorlichting en het doen van algemene aanbevelingen aan netwerkbeheerders, systeembeheerders, ontwikkelaars en eindgebruikers door het verspreiden van informatie;
- het leveren van managementrapportages aan het afdelingshoofd Information Technology over de beveiligingsincidenten en het doen van voorstellen tot betere preventie of curatie.

TiU-CERT levert de volgende diensten:

- afhandelen van binnenkomende e-mails;
- afhandelen van binnenkomende telefonische meldingen;
- inrichten en operationeel houden van een meldpunt voor alle beveiligingsincidenten en het coördineren en bewaken van een adequate afhandeling daarvan;
- geven van voorlichting aan IT-gebruikers, –ontwikkelaars en –beheerders over preventie van incidenten en actuele bedreigingen;
- adviseren over instelling brede beveiligingsaspecten;
- periodiek opstellen van managementrapportages.

Het CERT behandelt meldingen vertrouwelijk en verstrekt alleen informatie over beveiligingsincidenten als dat noodzakelijk en relevant is voor de oplossing van een incident.

De dienstverlening van TiU-CERT bij de universiteit is gedocumenteerd en door het College van Bestuur bekrachtigd.