Beleid informatiebeveiliging voor onderwijs, onderzoek en bedrijfsvoering bij de Universiteit Leiden

Universiteit Leiden

Versiebeheer

Versie 0.1	29 Juli 2013	1e concept
Versie 0.2	5 Augustus 2013	2e concept na input van Jan-Willem Brock. Tevens opgenomen trends na bespreking met Johan Detollenaere. Input van Erik Adriaens
Versie 0.3	20 Augustus 2013	3e concept na input Jan-Willem Brock
Versie 0.4	4 september 2013	4e concept na input Maritta de Vries
Versie 0.5	21 oktober 2013	5e concept na input Erik Adriaens, Johan Detollenaere en Gerrit Vooijs
Versie 0.6	4 november 2013	6e concept na input Jan van der Boon
Versie 0.7	20 november 2013	7e concept na input Daniel Mandel, André Morsman, Peter Magielse, informatie-managers en Rinke Betten.
Versie 0.8	16 december 2013	Aangepast n.a.v. bespreking OBV
Versie 1.0	11 februari 2014	Definitief. Vastgesteld door het college (gelijk aan 0.8)

Lijst met afkortingen

AIC: De afdeling Audit en Interne Controle
Baseline: document met ib (basis)maatregelen
BB: Bestuursbureau
BCI: Begeleidingscommissie ICT
Business Continuity: calamiteitenmaatregelen
BV: Bedrijfsvoering
CERT-team: Computer Emergency Response Team (team van ISSC)
CvIB: Code voor Informatiebeveiliging
DDoS: Distributed Denial of Service aanvallen
FB: Functioneel Beheer
IB: Informatiebeveiliging
IM: De afdeling Informatiemanagement
ISO: International Standards Organisation
ISSC: ICT Shared Service Centre
LDE: De universiteiten Leiden, Delft en Erasmus Rotterdam
LIACS: Leiden Institute of Advanced Computer Science
Malware: verzamelnaam voor virussen, Trojans, spam, etc.
NCSC: Nationaal Cyber Security Centrum
NEN: Normen voor standaardisatie
OBV: Het overleg van de directeuren Bedrijfsvoering
PID: Project Initiation Documentation
Rasci: Responsible/Accountable/Sign Off/Consulted/Informed
R&O: Resultaat en Ontwikkelingsgesprek
SAP: Business Management Software
SURFibo: Het informatiebeveiligingsorgaan van SURF
ULCN: Leids Identity Management systeem
Wbp: Wet bescherming persoonsgegevens

Managementsamenvatting

De Universiteit Leiden wil actief bijdragen aan de veiligheid en de veiligheidsbeleving van alle aan de universiteit verbonden studenten, onderzoekers en medewerkers en gasten. Niet omdat het onveilig is, maar om een veilige omgeving te kunnen waarborgen. Veiligheid is een randvoorwaarde voor een goed academisch klimaat waarbinnen betrokkenen zich kunnen ontplooien. Als onderzoeksinstelling wil de Universiteit ook bijdragen aan het ontwikkelen en verbeteren van de beveiliging van de maatschappij.

Dagelijks wordt in het nieuws melding gemaakt van hackers die in systemen zijn doorgedrongen of die via malware gegevens uit systemen hebben gehaald en geopenbaard. Bij de organisaties waarbij dit geschiedt kan imagoschade optreden en de continuïteit in gevaar komen. Om dit te voorkomen is een actueel informatie-beveiligingsbeleid belangrijk. Betrouwbare informatie voor onderwijs, onderzoek en bedrijfsvoering is van essentieel belang voor een kwalitatief hoogwaardige en efficiënte dienstverlening aan studenten, onderzoekers en medewerkers. Tevens biedt het een randvoorwaarde voor een succesvolle samenwerking met externe partners.

Naast onderwijs en bedrijfsvoering krijgt onderzoek meer aandacht als onderwerp in de informatiebeveiliging. Bescherming van gegevens in systemen is belangrijk om onderzoeksopdrachten goed te kunnen uitvoeren maar ook om de wetenschappelijke integriteit te kunnen waarborgen.

Voor het informatiebeveiligingsbeleid gelden o.a. de volgende uitgangspunten:

- De Universiteit Leiden is een open instelling. Dit open karakter kenmerkt zowel het onderwijs als het onderzoek.
- Om te borgen dat personen (medewerkers, studenten, gasten, externen) – al dan niet opzettelijk – de continuïteit van de universiteit in gevaar brengen zijn processen, procedures, richtlijnen en gedragscodes geformuleerd en geïmplementeerd.
- De implementatie van deze maatregelen kan organisatorisch of technisch zijn
- Informatiebeveiliging wordt in grote mate gedreven door opgelegde wetgeving en wordt – hoewel de doelstellingen onderschreven worden – vaak als last ervaren. Naast beveiligen is uitleg en bewustwording dus een belangrijk onderdeel.
- Het in dit beleid vastgestelde basisniveau geldt voor alle informatie en informatiesystemen, zowel in eigen beheer als uitbesteed

Een belangrijk onderdeel van informatiebeveiliging is te kijken naar het belang van gegevens in de informatiesystemen. Met behulp van een risicoanalyse wordt gekeken naar beschikbaarheid, de vertrouwelijkheid en de integriteit van een systeem of onderzoeksinformatie. Met behulp van een vragenlijst wordt een rating aan deze onderwerpen gegeven en wordt bepaald of een systeem of onderzoeksinformatie een normaal risico (basisrisico), verhoogd risico of hoog risico loopt. Naar gelang het risico worden er extra maatregelen genomen.

Inhoudsopgave

1. Inleiding

1.1 Algemeen

Informatiebeveiliging is een actueel onderwerp. Elke dag wordt in de media bericht over onderwerpen zoals botnets, het aftappen van informatie door (buitenlandse) overheden, DDOS aanvallen op banken, virussen die ervoor zorgen dat geld van de rekening wordt afgeschreven, spam en phishing en andere malware Hierdoor wordt duidelijk dat meer aandacht aan deze zaken moet worden besteed en dat maatregelen moeten worden genomen om deze aanvallen af te slaan.

Het Nederlandse kabinet heeft door bovenstaande ontwikkelingen dan ook aanleiding gezien om een Nationaal Cyber Security Centrum (NCSC) in te richten. Deze heeft als taak om de weerbaarheid te vergroten van de Nederlandse samenleving in het digitale domein door het geven van adviezen hoe systemen beter te beveiligen. Van instellingen zoals de Universiteit Leiden wordt verwacht deze adviezen over te nemen in het eigen beleid.

Informatiebeveiliging is bij de Universiteit Leiden niet alleen een ondersteunend proces. Bij het onderzoek naar ontwikkelingen op het gebied van computers en software spelen kennisinstituten ook een rol. Denk bijvoorbeeld aan het LIACS, waar onderzoek wordt verricht naar algoritmen voor informatiebeveiliging en het International Centre for Counter-Terrorism (ICCT) waar cyber-security een van de aandachtspunten is.

De Universiteit Leiden is net als vele andere organisaties in toenemende mate afhankelijk van informatie die is opgeslagen in (veelal geautomatiseerde) systemen. Deze afhankelijkheid brengt nieuwe kwetsbaarheden en risico's met zich mee, die met geschikte maatregelen beperkt dienen te worden. Onvoldoende informatiebeveiliging kan immers leiden tot onacceptabele risico's bij de uitvoering van onderwijs en onderzoek en de bedrijfsvoering van de universiteit. Incidenten en inbreuken in deze processen kunnen leiden tot financiële schades en imagoschade. Het College van Bestuur (CvB) wil daarom systematisch aandacht aan de beveiliging van de informatievoorziening besteden.

Het vorige informatiebeveiligingsbeleid en de daarvan afgeleide baseline (minimale maatregelen) dateren van 2010 en zijn aan herziening toe. Herziening is wenselijk omdat er steeds nieuwe trends en ontwikkelingen plaatsvinden die van invloed zijn op informatiebeveiliging. Tevens is het governancemodel uitgebreid en is het beleid met betrekking tot business continuïteit toegevoegd.

Het beleid en de baseline van minimale maatregelen zijn opgesteld onder verantwoordelijkheid van de afdeling Informatiemanagement van het Bestuursbureau, in nauw overleg met de informatiemanagers van de faculteiten, de security officer van het ISSC en de beveiligingsmanager van Vastgoed. Dit beleid met betrekking tot informatiebeveiliging is één van de vier prioriteiten in de ICT-infrastructuur en ICT-dienstverlening zoals verwoord in het ICT meerjarenplan 2012-2015.

1.2 Trends

In deze paragraaf worden een aantal trends besproken op het gebied van informatiebeveiliging in relatie tot onderwijs, onderzoek en bedrijfsvoering.

1.2.1 Onderwijs

In het onderwijs zijn een aantal trends zichtbaar zoals digitaal onderwijs en het meenemen van eigen apparaten door studenten (zgn. Bring-Your-Own-Device.).

Het ontvangen van digitaal onderwijs door studenten wordt steeds belangrijker. Colleges worden live opgenomen en studenten kunnen deze terugzien. Het is ook mogelijk om colleges aan binnen- en buitenlandse universiteiten te volgen in open courseware en in massive open online courses (MOOCs). De wetgeving waar deze informatie onder valt is afhankelijk van het land waar deze data staat of passeert en waar de bedrijven die diensten verlenen gevestigd zijn. De Amerikaanse Patriot Act is veruit de bekendste wet, maar ieder land kent wetten die het mogelijk maken om de informatie die eigendom is van de Universiteit Leiden op te vragen. Deelnemers uit tientallen landen aan “The law of the European Union” is positief vanuit publicitair oogpunt, maar een risico als het gaat om informatiebeveiliging.

Onze eigen docenten en studenten werken en leven ook steeds meer digitaal met een steeds grotere diversiteit aan apparatuur en applicaties (apps). Het is niet mogelijk om de honderden modellen apparaten of de miljoenen applicaties (apps) vooraf te controleren.

1.2.2 Onderzoek

In het onderzoek zijn industriële spionage en Big Data ontwikkelingen die voor de informatiebeveiliging van belang zijn.

Industriële spionage is van alle tijden en het verkrijgen van intellectueel eigendom kan een land of organisatie een voorsprong geven in het ontwikkelen van bepaalde producten. De Universiteit Leiden geeft onderwijs maar verricht ook onderzoek en hierbij speelt de waarde van informatie een rol. Als deze waarde hoog is, is het interessant voor derden om deze informatie illegaal te verkrijgen. De vraag is dan hoe deze informatie beschermd moet worden. Moeten personen uit bepaalde gebieden op de wereld worden geweerd?

Big Data kan vooral worden gevonden bij de faculteit Wiskunde en Natuur-wetenschappen van de universiteit. Het beheersen van grote hoeveelheden data en het beveiligen ervan is een onderzoeksgebied waar ook de universiteit op wetenschappelijk vlak actief op is.

Ten slotte is het verschuiven van universitaire financiering van eerste naar tweede en derde geldstroom en toename van het belang van valorisatie een trend. Waar onderwijs een "open tenzij" uitgangspunt kent, is dat voor onderzoek en zeker valorisatie misschien wel het omgekeerde.

1.2.3 Bedrijfsvoering

Als trends in de bedrijfsvoering kunnen worden genoemd het tijd-, plaats- en apparaatonafhankelijk werken (tegenwoordig ook het Nieuwe Werken genoemd). Dit kan thuiswerken zijn maar ook op een andere locatie onafhankelijk van de werkplek. Daarnaast wordt er in toenemende mate gebruik gemaakt van mobiele apparaten als tablets, smartphones en laptops. Bij deze vormen van consumerisation speelt de locatie waar de gegevens worden opgeslagen een rol : op het apparaat of op de werkplek en hoe deze gegevens worden beveiligd.

Trends in de computercriminaliteit zijn het toenemende gebruik van phishing, botnets, malware. Phishing richt zich in Nederland naast de bancaire sector ook op andere sectoren. De computer van de eindgebruiker wordt besmet - via een bestand in een e-mail of bij bezoek van een bepaalde website - met een programma dat zich nestelt in de webbrowser. Als eenmaal de computer besmet is dan kan de aanval beginnen. In het geval van een bank kan de crimineel de communicatiestroom tussen klant en bank onderschep[en en de transactie wijzigen.

Afgelopen jaar waren botnets opnieuw een belangrijk gereedschap voor internet-criminelen. Enorme hoeveelheden computers kwamen onder controle van criminelen via besmetting van de pc door het aanklikken van attachments in e-mails. Vanuit botnets wordt spam verstuurd, phishing verricht of creditcardgegevens gestolen. Daarnaast wordt ook gehandeld in gestolen identiteitsgegevens en worden botnets te huur aangeboden. Voor veel van de transacties op de ondergrondse markt wordt betaald met gestolen creditcard-gegevens.

Naast bovenstaande methoden blijven de virussen en andere malware een belangrijk aandachtspunt. De aanvallen worden steeds verfijnder en geraffineerder. De aanvallers gebruiken niet alleen aanvallen die gericht zijn op een specifiek slachtoffer op basis veel persoonlijke informatie (ransomware) maar misbruiken bijvoorbeeld ook websites van kranten die veel bezoekers trekken om zoveel mogelijk computers te besmetten.

De laatste jaren is er meer aandacht voor privacy op het internet. Met name social media als Facebook en Twitter krijgen het te verduren omdat zij steeds meer gebruikersgegevens bewaren en opslaan en de daarbij behorende risico’s toenemen. Alsmede de uitwisseling van gegevens naar derden. De gebruikers krijgen dit in de gaten en worden kritischer.

Bij Hacktivisme worden computers en netwerken ingezet om een ideologisch of politiek doel te bereiken. Meestal gebeurt dit door websites van tegenstanders te beschadigen of onbereikbaar te maken.

1.2.4 Analyse van bedreigingen

Zoals in bovenstaande trends wordt aangetoond evolueren bedreigingen in steeds hoger tempo. Denk hierbij aan extremistische acties, DDoS aanvallen op systemen maar ook aan niet ICT-bedreigingen zoals het kraken van kluizen om examens of tentamens vooraf te scannen. Binnen dit kader, vraagt de toenemende groei en daaraan gerelateerde complexiteit van de Universiteit Leiden een gezamenlijke inventarisatie en analyse van mogelijke dreigingen. Deze inventarisatie heeft in 2013 plaatsgevonden met de managers bedrijfsvoering van de faculteiten, managers van expertise centra, UB en het Bestuursbureau. Hieruit kwamen de volgende toprisico's naar voren: diverse vormen van hacking, stroomuitval, DDoS aanvallen, spionage, reputatieschade voor onderwijs, onderzoek en integriteit. Verder acties van studentenverenigingen, waterschade en het lekken van informatie. De ICT-bedreigingen van deze risico's zullen in de baseline worden voorzien van maatregelen.

1.3 Samenhang tussen informatiebeveiliging en bescherming persoonsgegevens

Gegevensbescherming richt zich op de zorgvuldige omgang met persoonsgegevens. Dit zijn gegevens van studenten, medewerkers en gasten. De maatregelen die in het kader van informatiebeveiliging worden getroffen leveren een bijdrage aan de bescherming van gevoelige persoonsgegevens.

Binnen de Universiteit Leiden is de securitymanager verantwoordelijk voor de coördinatie van alle activiteiten die betrekking hebben op informatiebeveiliging. De functionaris gegevensbescherming houdt toezicht op de regels voor gegevens-bescherming en deze functie is belegd bij de afdeling Juridische Zaken.

1.4 Samenhang tussen informatiebeveiliging, fysieke beveiliging en arbo-wetgeving

Integrale veiligheid is een aanpak om grip te krijgen op alle incidenten en veiligheidsrisico's in een organisatie. Deze worden in samenhang met elkaar gebracht en er worden gepaste maatregelen genomen om de risico's te bestrijden of te verminderen. Integrale veiligheid maakt gebruik van gemeenschappelijke processen zodat een overkoepelend beeld van de veiligheidssituatie ontstaat, ongeacht of er sprake is van arbo-, safety, security of IT risico's. Integrale veiligheid maakt beheersing en besturing van alle veiligheidsfuncties beter en levert concurrentievoordeel op.

In Leiden wordt steeds meer samengewerkt tussen de domeinen informatie, vastgoed en arbo. Een voorbeeld hiervan is het beleid met betrekking tot Business Continuity Management. Er worden calamiteitenplannen opgesteld voor de gehele universiteit met deze onderdelen.

1.5 Doelstelling informatiebeveiligingsbeleid

Het informatiebeveiligingsbeleid heeft als doel het waarborgen van de continuïteit van de informatiesystemen en het minimaliseren van de schade door het voorkomen van beveiligingsincidenten en het minimaliseren van eventuele gevolgen.

Het informatiebeveiligingsbeleid biedt o.a. een kader om (toekomstige) maatregelen in de informatiebeveiliging te toetsen aan een vastgestelde best practice of norm. Voor de norm geldt dat het beleid is gebaseerd op de Code voor Informatiebeveiliging. Deze code is een NEN norm en beschrijft normen en maatregelen die van belang zijn voor het realiseren van een afdoende niveau van informatiebeveiliging. Tevens wordt aandacht besteed aan de wettelijke voorschriften die in acht moeten worden genomen. Via de beschrijving van de governance wordt de organisatorische inbedding verkregen.

1.6 Reikwijdte van het beleid

Het informatiebeveiligingsbeleid heeft betrekking op alle personen (in- en externe medewerkers, studenten, gasten, bezoekers en relaties), procedures en processen en informatie en informatiesystemen (zowel in eigen beheer als uitbesteed). Onder de informatiesystemen vallen de basisinfrastructuur (met onder andere netwerken, werkplekken en opslag), concernsystemen en specifieke systemen van faculteiten en eenheden. Mobiele apparaten vallen ook onder het beleid. Hiervoor is o.a. een handreiking informatiebeveiligingsbeleid samengesteld waarin nadere maatregelen worden genoemd.

Er is een belangrijk relatie en een gedeeltelijke overlap met aanpalende beleidsterreinen zoals safety (arbo- en milieuwetgeving), security (fysieke beveiliging) en business continuity. Op al deze terreinen wordt aandacht geschonken aan deze raakvlakken en wordt zowel planmatig als inhoudelijk afstemming gezocht.

Het informatiebeveiligingsbeleid heeft zowel betrekking op gecontroleerde informatie, die door de instelling zelf is gegenereerd en wordt beheerd, als ook op niet-gecontroleerde informatie (uitspraken van studenten in discussies, persoonlijke websites op zakelijke persoonlijke pagina’s) waarop de instelling kan worden aangesproken.

1.7 Verantwoordelijkheid informatiebeveiligingsbeleid

Het College van Bestuur is eindverantwoordelijk voor het informatiebeveiligingsbeleid en heeft dit beleid vastgesteld. De securitymanager is verantwoordelijk voor het onderhoud van dit beleid. Informatiebeveiliging is een gedeelde verantwoordelijkheid, waarbij de informatie- of systeemeigenaar aanspreekbaar is op de toepassing van het beleid. De verantwoordelijkheden worden in hoofdstuk 5 verder uitgewerkt.

1.8 Ondersteunende documenten

Dit informatiebeveiligingsbeleid wordt verder uitgewerkt in een aantal documenten:

1. De baseline van minimale maatregelen waaraan systemen moeten voldoen
2. Risicoanalysedocument ter bepaling van risico's en maatregelen
3. De gedragscode voor studenten en medewerkers binnen de universiteit
4. Richtlijnen en procedures
5. Handreiking met vertaling naar producten en diensten

1.9 Inhoud informatiebeveiligingsbeleid

In hoofdstuk 2 worden de uitgangspunten en principes van het beleid vastgelegd. In hoofdstuk 3 wordt aandacht besteed aan wet- en regelgeving. Hoofdstuk 4 beschrijft de Business Continuity. Hoofdstuk 5 de organisatie van informatiebeveiliging en tenslotte hoofdstuk 6 beschrijft hoe met incidenten wordt omgegaan.

2. Visie, ambitie, beleidsuitgangspunten en beleidsprincipes

2.1 Visie

Als maatschappelijk betrokken instelling, volgt de Universiteit Leiden veranderingen in de wereld en in de directe omgeving van de universiteit nauwgezet. Niet alleen vanuit de kernactiviteiten – onderwijs en onderzoek – maar ook in het licht van wat deze ontwikkelingen betekenen voor de organisatie en haar kernwaarden. Maatschappelijke en technologische ontwikkelingen hebben direct invloed op de situatie van de universiteit. Nieuwe ontwikkelingen bieden kansen voor exploratie maar ook risico's. Door het open karakter van de instelling is het een spiegel van de samenleving. De universiteit is daarom als organisatie dan ook zeker niet immuun voor veranderingen in risico's en risicoperceptie.

De geschetste uitdagingen van de moderne maatschappij zoals mondialisering, technologische voortschrijding en individualisering, als ook het veranderende denken over veiligheid, kunnen onze kernwaarden als "open" en "persoonlijk" ongunstig beïnvloeden, evenals concrete organisatiedoelen zoals het willen bieden van een "bruisende en veilige campus". De mate waarin de samenleving risico's accepteert neemt in het algemeen – maar zeker voor veiligheidsrisico's – af. Organisaties zijn met een terugtredende overheid sterker dan voorheen op zichzelf aangewezen. Zij zullen zelf maatregelen moeten nemen om risico's te voorkomen en crises te beheersen. Zij worden daar ook actief op bevraagd. Ook stelt de omgeving steeds hogere eisen aan het niveau en de kwaliteit van onze veiligheid en zelfredzaamheid.

De Universiteit Leiden wil actief bijdragen aan de veiligheid en de veiligheidsbeleving van alle aan de universiteit verbonden medewerkers, studenten en gasten. Niet omdat het onveilig is, maar om een veilige omgeving te kunnen blijven waarborgen. Veiligheid is een randvoorwaarde voor een goed academisch klimaat waarbinnen betrokkenen zich ongehinderd kunnen ontplooien. Als onderzoeksinstelling wil de Universiteit ook bijdragen aan het ontwikkelen en verbeteren van de beveiliging van de maatschappij.

2.2 Ambitie

"We willen de informatieveiligheid van studenten, medewerkers en gasten waarborgen door verdere versterking van maatregelen om daarmee onderwijs en onderzoek in de toekomst te kunnen blijven garanderen en ervoor te zorgen dat incidenten beperkt blijven en dat de gevolgen hiervan worden geminimaliseerd."

Het streven is om het huidige niveau van veiligheid te behouden en te verhogen waar het mogelijk is. Dit is geen gemakkelijke opgave. Maatschappelijk ontwikkelingen zoals verwoord in de paragraaf van hoofdstuk 1 over trends stellen de universiteit voor nieuwe uitdagingen. Bovendien moet de universiteit voldoen aan geldende wet- en regelgeving, dat op het gebied van informatiebeveiliging toeneemt. Maar waar nodig willen we ook eigen keuzes kunnen maken die aansluiten bij onze ambities.

2.3 Kenmerken van de organisatie die van invloed zijn op de veiligheidssituatie

De volgende kenmerken zijn van invloed op onze veiligheidssituatie:

- Het open karakter van de universiteit als onderwijsinstelling
- De omvang en diversiteit van de medewerkers-, studentenpopulatie en gasten
- De digitalisering van informatie
- Het belang van academische vrijheid en autonomie
- Het tijd-, plaats- en apparaatonafhankelijk werken
- De toename van mobiele apparaten (tablets, smartphones, etc.)
- De afname van privacybewustzijn (informatie op Facebook)
- Intellectueel eigendom wordt steeds interessanter wat landen tot industriële spionage verleidt
- Door onderzoek (voor externe partijen) neemt de hoeveelheid vertrouwelijke data toe (gesloten karakter)

Omdat een aantal van bovenstaande kenmerken ertoe kan leiden dat er meer informatie openbaar wordt dan gewenst is, is het belangrijk dat deze goed wordt beveiligd en dat het bewustzijn wordt verhoogd bij de gebruikers. Dit beleid hanteert hiertoe een aantal beleidsuitgangspunten en beleidsprincipes.

2.4 Beleidsuitgangspunten

Security management wordt als continu proces ingericht. Dat houdt in dat de jaarlijkse planning- en controlecyclus als uitgangspunt wordt genomen. Hierin worden jaarplannen opgesteld en uitgevoerd. De resultaten ervan worden geëvalueerd en vertaald naar nieuwe jaarplannen.

De beleidsuitgangspunten zijn:

- De Universiteit Leiden is een open instelling. Dit open karakter kenmerkt zowel het onderwijs als het onderzoek.
- Om te borgen dat personen (medewerkers, studenten, gasten, externen) – al dan niet opzettelijk – de continuïteit van de universiteit in gevaar brengen zijn processen, procedures, richtlijnen en gedragscodes geformuleerd en geïmplementeerd.
- De implementatie van deze maatregelen kan organisatorisch of technisch zijn
- Informatiebeveiliging wordt in grote mate gedreven door opgelegde wetgeving en wordt – hoewel de doelstellingen onderschreven worden – vaak als last ervaren. Naast beveiligen is uitleg en bewustwording dus een belangrijk onderdeel.
- Het in dit beleid vastgestelde basisniveau geldt voor alle informatie en informatiesystemen, zowel in eigen beheer als uitbesteed. Er vindt geen compensatie plaats voor informatie en informatiesystemen die een lager beveiligingsniveau kennen (gedeelde lasten). De aanvullende maatregelen die horen bij een hoger niveau zijn voor rekening van de systeemeigenaar.

- Voor medewerkers geldt dat bij aanname, tijdens het dienstverband en bij uitdiensttreding de leidinggevende de medewerker wijst op zijn rechten en plichten voor informatiebeveiliging. Voor studenten en onderzoekers geldt dat zij aan het begin van de studie of werk worden geïnformeerd over deze rechten en plichten. Wanneer geconstateerd wordt dat een persoon (student, onderzoeker, medewerker, gast) – al dan niet bewust – het informatiebeveiligingsbeleid niet nakomt is men verplicht deze persoon hierop aan te spreken en hiervan melding te maken volgens een vastgelegde procedure.
- Bij een overtreding van het IB-beleid kan het College van Bestuur een sanctie opleggen.
- Alle faculteiten en eenheden hebben adequate maatregelen (zowel technisch, procedureel als organisatorisch) getroffen voor de personen, informatie en informatiesystemen waarvoor zij verantwoordelijk zijn om de continuïteit van de bedrijfsprocessen te waarborgen. Zij hebben een medewerker – de informatiemanager/security officer - aangewezen die het beleid handhaaft en rapporteert over het nakomen van het beleid en over beveiligingsincidenten. Het bestuur van de faculteit of eenheid is eindverantwoordelijk voor de invoering en uitvoering van het informatiebeveiligingsbeleid binnen haar eenheid en aansprakelijk voor schade als gevolg van het niet of niet correct naleven van het informatie-beveiligingsbeleid.
- De beveiliging dient de volgende aspecten te waarborgen:
    - Beschikbaarheid (de mate waarin gegevens of functionaliteit op de juiste momenten beschikbaar zijn voor gebruikers)
    - Integriteit (de mate waarin gegevens of functionaliteit juist ingevuld zijn of niet aangetast)
    - Vertrouwelijkheid (de mate waarin de toegang tot gegevens of functionaliteit beperkt is tot degenen die daartoe bevoegd zijn)
    - Het basisniveau van beveiliging is vertaald naar de maatregelen zoals genoemd in de baseline (minimale maatregelen).

2.5 Beleidsprincipes

De beleidsprincipes zijn:

- Informatie betreffende de primaire processen en bedrijfsvoering is open waar het kan; gesloten waar het moet
- Op een verantwoorde wijze omgaan met vertrouwen als basis
- Informatiebeveiliging is een lijnverantwoordelijkheid
- Security management is als een instellingsbreed proces ingericht. De jaarlijkse planning- en controle cyclus (plan, do, check, act) is gebaseerd op ISO 27001
- De universiteit is eigenaar van informatie die onder haar verantwoordelijkheid is geproduceerd en daarmee verantwoordelijk voor de beveiliging hiervan
- Bij (ICT)-projecten betreffende primaire processen en bedrijfsvoering wordt vanaf het begin rekening gehouden met (informatie)beveiliging. In ieder Plan van Aanpak staat een passage hoe de gevolgen voor (informatie)beveiliging.
- Technische beveiliging is end-to-end en gebaseerd op meerdere strategieën. Door deze beveiliging is de universiteit beter in staat sneller te reageren op

bijvoorbeeld cyberaanvallen. Er kan naadloos worden overgegaan van analyse en classificatie van dreigingen naar bescherming en het stoppen hiervan.
- Binnen elk bedrijfsproces is sprake van risico's op het gebied van beschikbaarheid, integriteit en/of vertrouwelijkheid. Pas als deze risico's inzichtelijk zijn kan het management keuzes maken m.b.t. te implementeren maatregelen die het restrisico voor de instelling voldoende laag maken.

Enkele van bovenstaande principes zullen hierna kort worden toegelicht.

2.5.1 Informatiebeveiliging is een lijnverantwoordelijkheid

Het universitair IB-beleid vormt het kader. Van de systeemeigenaren en de door het faculteitsbestuur aangewezen directeuren wordt verwacht dat zij hieraan nader invulling geven. Zij zijn immers verantwoordelijkheid voor de correcte uitvoering van de aan hen opgedragen bedrijfsprocessen met de daarbij behorende informatievoorziening en voor het goed functioneren daarvan en hiermee dus óók voor de informatiebeveiliging. Zij laten risicoanalyses uitvoeren waaruit maatregelen kunnen voortkomen die door ISSC en anderen worden geïmplementeerd. Zij blijven de primaire verantwoordelijkheid dragen voor het kiezen, uitvoeren en handhaven van deze maatregelen.

2.5.2 Verwachtingen t.o.v. individuen

De Universiteit Leiden is een open gemeenschap die functioneert op basis van vertrouwen. Van iedereen die in deze gemeenschap werkt of studeert wordt verwacht dat hij of zij zich actief zal inspannen om zowel te beveiligen in eigen belang als in het belang van de universiteit.
Een ieder heeft de taak om op een verantwoorde wijze om te gaan met vertrouwen. Zowel het vertrouwen dat ontvangen wordt en dat niet beschaamd moet worden, als het vertrouwen dat niet achteloos gegeven mag worden.

Beveiligen is een integraal onderdeel van de normale werkzaamheden, een kwaliteitsaspect waarmee rekening gehouden moet worden bij alle werkzaamheden. Dat betekent dat duidelijk gemaakt moet worden welke beveiligingstaken een integraal onderdeel vormen van de takenpakketten van functies.

2.5.3 Informatiebeveiliging is een continu proces

Om informatiebeveiliging adequaat gestalte te geven, dient een samenhangend pakket beveiligingsmaatregelen te worden gemaakt en onderhouden. Dit is een proces dat begint bij het specificeren van de beveiligingseisen en –randvoorwaarden, waarop het beleid gestoeld wordt, en het inrichten van de organisatie die verantwoordelijk is voor informatiebeveiliging. Vervolgens wordt bepaald welke bedreigingen tot onacceptabele risico’s leiden en met welke maatregelen deze risico’s gereduceerd kunnen worden. Op basis van deze informatie wordt een pakket maatregelen geselecteerd en vervolgens geïmplementeerd. Na het implementeren van de maatregelen door de systeemeigenaar dient het naleven ervan te worden bewaakt. Bovendien dient geëvalueerd te worden of het geïmplementeerde pakket maatregelen blijft voldoen aan de beveiligingseisen en –randvoorwaarden en of de relevante risico’s voldoende gereduceerd worden.

Er vindt door de security manager een regelmatige herijking plaats van beleid, en monitoring op basis van risicoanalyses en audits. Technologische en organisatorische ontwikkelingen binnen en buiten de instelling maken het noodzakelijk om periodiek te bezien of we op de juiste wijze bezig zijn de informatiebeveiliging te waarborgen. De audits op concernsystemen maken het mogelijk het beleid en de genomen maatregelen te controleren op efficiency (controleerbaarheid).

Het IB-beleid en de minimale maatregelen wordt ten minste vierjaarlijks op inhoud, uitvoerbaarheid en implementatiestatus beoordeeld en opnieuw vastgesteld. Het IB-beleid voorziet daarnaast in audits en periodieke risicoanalyses op de systemen.

Risicoanalyses worden – onder eindverantwoordelijkheid van de systeemeigenaar – door de security manager uitgevoerd bij de initiële oplevering en bij grote wijzigingen aan het systeem. Met risicoanalyses wordt geborgd dat:

- het gewenste niveau van informatiebeveiliging wordt vastgesteld in de vorm van een dataclassificatie m.b.t. bedrijfsprocessen.
- er maatregelen worden vastgesteld behorend bij het vastgestelde beveiligingsniveau
- indien er veranderingen plaatsvinden in de context deze jaarlijks worden beoordeeld en het niveau en de maatregelen worden aangepast indien van toepassing.

Voor auditing geldt dat er onder verantwoordelijkheid van de auditafdeling AIC door de afdeling IM wordt meegewerkt aan de audits. Elk jaar vinden er diverse audits plaats op (concern)systemen.

2.5.4 Eigendom van informatie

De Universiteit Leiden is als rechtspersoon eigenaar van alle informatie die onder haar verantwoordelijkheid wordt geproduceerd. Daarnaast beheert de Universiteit een veelheid aan informatie, of de toegang daartoe, waarvan het eigenaarschap (auteursrecht) aan derden toebehoort. Een voorbeeld hiervan is de online inhoud van tijdschriften die via de Digitale Bibliotheek kan worden ontsloten. De Universiteit dient ervoor te zorgen dat beveiliging van deze informatie goed geregeld is en dat al haar medewerkers en studenten voldoende zijn geïnformeerd over de regelgeving omtrent het (her)gebruik van deze informatie.

2.5.5 Waardering van informatie

Beveiligen gebeurt met een duidelijk beeld voor ogen van de waarde van datgene wat beveiligd wordt. Dat betekent dat bewustzijn van die waarde en van de risico's van mogelijke schade de grondslag is van het beleid en sturend moet zijn in het nemen van maatregelen. Het is de taak van de verantwoordelijke bestuurder of directeur in iedere faculteit en eenheid om ervoor te zorgen dat dit bewustzijn aanwezig is.

Alle informatie heeft een eigenaar. De waarde van de informatie wordt vastgesteld door de eigenaar. De waarde wordt bepaald door de schade die verlies van beschikbaarheid, integriteit en vertrouwelijkheid toebrengt aan de mogelijkheid tot het kunnen verzorgen van onderwijs en onderzoek op een hoogwaardig academisch niveau.

2.5.6 Projecten en informatiebeveiliging
Bij projecten, zoals infrastructurele wijzigingen of de aanschaf van nieuwe systemen, wordt vanaf de start rekening gehouden met informatiebeveiliging.

2.6 Classificatie van gegevens en systemen

Alle gegevens in systemen waarop dit informatiebeveiligingsbeleid van toepassing is, worden geclassificeerd. Het niveau van de beveiligingsmaatregelen is afhankelijk van de klasse.

De classificatie van informatie is afhankelijk van de gegevens in informatiesystemen en wordt bepaald op basis van risicoanalyses. Hierbij zijn de volgende aspecten van belang:

a. beschikbaarheid
b. integriteit
c. vertrouwelijkheid

Beschikbaarheid is de mate waarin gegevens of functionaliteit op de juiste momenten beschikbaar zijn voor gebruikers.
Integriteit is de mate waarin gegevens of functionaliteit juist ingevuld zijn.
Vertrouwelijkheid is de mate waarin de toegang tot gegevens of functionaliteit beperkt is tot degenen die daartoe bevoegd zijn.

Aspecten en kenmerken van informatiebeveiliging en daaraan gerelateerde bedreigingen:

Aspect	Kenmerk	Bedreiging	Voorbeelden van bedreiging
Beschikbaar-heid	Tijdigheid	Vertraging	Overbelasting van infrastructuur
	Continuïteit	Uitval	Defect in infrastructuur
Integriteit	Correctheid	Wijziging	Ongeautoriseerd wijzigen van gegevens; virusinfectie; typefout
	Volledigheid	Verwijdering	Ongeautoriseerd wissen van gegevens
		Toevoeging	Ongeautoriseerd toevoegen van gegevens
	Geldigheid	Veroudering	Gegevens niet up-to-date houden
	Authenticiteit	Vervalsing	Frauduleuze transactie
	Onweerlegbaarheid	Verloochening	Ontkennen een bepaald bericht te hebben verstuurd
Vertrouwelijkheid	Exclusiviteit	Onthulling	Afluisteren van netwerk; hacking
		Misbruik	Privé-gebruik op grote

			mate

2.6.1 Classificatie gegevens in concernsystemen

Welk beveiligingsniveau geschikt is voor een bepaald informatiesysteem hangt af van de classificatie van de informatie die het systeem verwerkt. De classificatie dient door of namens de eigenaar van het betreffende informatiesysteem te worden bepaald. Dat gebeurt met behulp van schadescenario's.

Het gaat om de volgende schadescenario's:

- schade aan het (hoofd)bedrijfsproces
- directe financiële schade
- (inbreuk op) overeenkomsten
- reputatieschade
- persoonsschade
- (inbreuk op) wet- en regelgeving

Bij elk van deze schadescenario's wordt gekeken naar de informatiebeveiligings-aspecten beschikbaarheid, vertrouwelijkheid en integriteit en wordt gekeken of de impact laag/midden/hoog is.

Voor elk van deze kwaliteitsaspecten bestaat een gestructureerde vragenlijst. Op basis van de antwoorden op deze vragen wordt periodiek voor elk systeem een risicoanalyse opgesteld. Die analyse leidt er toe dat elke systeem wordt ingedeeld in een risicoklasse: (zie hieronder): basis (normaal) risico, verhoogd risico (gevoelig) en hoog risico (kritiek).

Onderstaande tabel geeft weer welk beveiligingsniveau bij welke klassen van informatie hoort.

Risicoklasse	Omschrijving	Maatregel	Systemen
Basis risico (niveau 3)	Een inbreuk op de beschikbaarheid, exclusiviteit en integriteit veroorzaakt geen (grote) storing.	Het systeem moet voldoen aan de minimale maatregelen (IB-baseline)	Planon, Converis
Verhoogd risico (niveau 2)	Een inbreuk op de beschikbaarheid, exclusiviteit en integriteit veroorzaakt geen verstoring van ernstige aard	Het systeem moet voldoen aan de minimale maatregelen en extra maatregelen	SAP, Blackboard, Docman
Hoog risico (niveau 1)	Een inbreuk op de beschikbaarheid, exclusiviteit en integriteit veroorzaakt een verstoring van ernstige aard zodat de voortgang van primaire processen in gevaar kunnen komen.	Het systeem moet voldoen aan de minimale maatregelen en extra (zware) maatregelen.	ULCN, uSis, (Web CMS), netwerk-systemen

Het baselineniveau is het niveau van het basisrisico. Dit betekent dat een risicoclassificatie is gemaakt en dat beschikbaarheid, vertrouwelijkheid en integriteit op het niveau laag staan. Voor dit niveau zijn maatregelen opgesteld waaraan elk systeem moet voldoen. Als het systeem een verhoogd risico of hoog risico heeft dan moeten extra maatregelen worden genomen.

2.6.2 Classificatie gegevens in systemen ten behoeve van onderzoek

De classificatie van gegevens in een systeem dat voor onderzoek wordt gebruikt wordt in principe op dezelfde wijze verricht als de classificatie van gegevens in concern-systemen.

Het gaat hierbij om de schadescenario's:

- schade aan het (hoofd)bedrijfsproces
- directe financiële schade
- (inbreuk op) overeenkomsten
- imagoschade
- persoonsschade
- (inbreuk op) wet- en regelgeving

Bij elk van deze schadescenario's wordt gekeken naar de informatiebeveiligings--aspecten beschikbaarheid, vertrouwelijkheid en integriteit en wordt gekeken of de impact laag/midden/hoog is. Uiteindelijk worden de gegevens in het systeem ingedeeld in één van de risicoklassen en moeten de maatregelen hierop worden aangepast.

De procedure verschilt in die zin dat bij concernsystemen de security manager of security officer van het ISSC de risicoanalyse verricht en bij systemen ten behoeve van onderzoek zal dit door de informatiemanager/security officer van de desbetreffende faculteit worden verricht.

Bij onderzoeken met een hoog risicoprofiel zal de facultaire informatiemanager/security officer een risicoanalyse verrichten samen met degene die voor het onderzoek verantwoordelijk is. De security manager voorziet de informatiemanager van een methodiek om deze analyse te verrichten. Na de indeling in de risicoklasse zullen maatregelen moeten worden genomen waarbij de baseline als leidraad geldt.

2.6.3 Vertrouwelijke gegevens in papieren documenten

Voor gegevens in vertrouwelijke (papieren) documenten geldt dat vooraf is bepaald wie toegang krijgt tot deze documenten en hoe de gegevens fysiek worden verstrekt. Na gebruik worden de dossiers meteen weer opgeborgen in een afgesloten kast. Als een andere – niet bevoegde – medewerker inzage in vertrouwelijke documenten nodig heeft dan dient dit onder toezicht van de verantwoordelijke beheerder te geschieden.

2.7 Audits

Audits op systemen vinden plaats op basis van de auditkalender. De frequentie wordt bepaald op basis van de classificatie van het systeem. Die wordt in de projectfase uitgevoerd en geeft een beeld van kwetsbaarheid en afhankelijkheid van het systeem. In de auditkalender staan alle concernsystemen (dit zijn systemen die universiteitsbrede processen ondersteunen). De normenkaders waar tegen getoetst wordt zijn SURF (o.b.v. Code voor Informatiebeveiliging) en KPMG (SAP en uSis). Beide kennen dezelfde bronnen en een vervanging door één normenkader is op termijn wenselijk.

3. Wet en regelgeving

Voor het universitaire IB-beleid is wet- en regelgeving van toepassing. Daarnaast zijn er interne richtlijnen en gedragscodes opgesteld voor iedereen die werkt of studeert aan de Universiteit Leiden of gebruik maakt van de informatievoorzieningen van de Universiteit. Deze wettelijke voorschriften en interne regelgeving worden hier kort toegelicht.

3.1 Wettelijke voorschriften

Algemene wettelijke voorschriften dienen opgevolgd te worden. Dat geldt in dit verband in het bijzonder voor:

- Wet op het Hoger onderwijs en Wetenschappelijk onderzoek
- Wet Bescherming persoonsgegevens
- Archiefwet
- Auteurswet
- Telecommunicatiewet
- Wet Computercriminaliteit

Wet op het Hoger onderwijs en Wetenschappelijk onderzoek

De Universiteit Leiden heeft een kwaliteitszorgsysteem, waarin (onder meer) het zorgvuldig omgaan met gegevens in de studentenadministratie en met de studieresultaten is gewaarborgd. Daarnaast worden integriteitscodes voor wetenschappelijk onderzoek nageleefd en toegepast.

Wet Bescherming Persoonsgegevens

De Wet Bescherming Persoonsgegevens stelt eisen aan de opslag en verwerking van persoonsgegevens in het bijzonder aan de juistheid en nauwkeurigheid van persoonsgegevens en de eisen voor het uitvoeren van passende technische en organisatorische maatregelen om persoonsgegevens te beveiligen tegen verlies en onrechtmatige verwerking. Naleving van dit informatiebeveiligingsbeleid en implementatie van de minimale maatregelen moet leiden tot voldoen aan de Wet Bescherming Persoonsgegevens.

Archiefwet

De Universiteit Leiden houdt zich aan de voorschriften uit de Archiefwet en het Archiefbesluit over de wijze waarop omgegaan moet worden met informatie vastgelegd in – gedigitaliseerde - documenten, informatiesystemen, websites, e.d.

Auteurswet

De Auteurswet regelt het auteursrecht van originele werken op het gebied van letterkunde, wetenschap en kunst. Dit betekent dat de Universiteit geen originele werken

verspreidt zonder dat daarvoor toestemming is verkregen van de eigenaar van de auteursrechten. Dit betekent dat het gebruik van illegale software wordt bestreden.

Telecommunicatiewet

De Telecommunicatiewet regelt allerlei zaken met betrekking tot gegevensverkeer over openbare netwerken. Zolang het netwerk niet openbaar is, is de Telecommunicatiewet niet van toepassing.

Wet Computercriminaliteit

De Wet Computercriminaliteit richt zich op de strafrechtelijke probleemgebieden in relatie tot het computergebruik. De Wet Computercriminaliteit schrijft voor dat "enige beveiliging" vereist is alvorens er sprake *kan zijn* van het eventueel strafrechtelijk vervolgen van delicten jegens de Universiteit en het eventueel vrijwaren van bestuurders van de Universiteit.

In de wet zijn strafbepalingen opgenomen met betrekking tot o.a.:

- het binnendringen in een daartegen beveiligd computersysteem (computervredebreuk);
- het wederrechtelijk wijzigen en toevoegen van gegevens in een computer, ook als ze niet beveiligd zijn;
- het opzettelijk of door nalatigheid beschadigen of onbruikbaar maken of storen van een computersysteem

Meldplicht datalekken

Naar verwachting zal in 2013 de Wet bescherming persoonsgegevens en de Telecommunicatiewet worden aangepast in verband met de invoering van een meldplicht bij de doorbreking van maatregelen voor de beveiliging van persoonsgegevens (meldplicht datalekken).

Door een beveiligingsfout kunnen grote hoeveelheden persoonsgegevens op straat belanden. De toezichthouder – het College bescherming persoonsgegevens (Cbp) – ontvangt dan een melding. Daarnaast ontvangt in veel gevallen ook degene wiens persoonsgegevens het betreft een melding, indien de inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer.

Dit betekent dat, ingeval van een datalek, het incident responseteam van de Universiteit Leiden dit lek meldt bij het Cbp en meteen aangeeft wat de gevolgen zijn en welke maatregelen er zijn getroffen om deze gevolgen te verhelpen. Het ISSC heeft voor deze meldplicht procedures ingericht .

3.2 Overige richtlijnen en landelijke afspraken

Een deel van de richtlijnen van de universiteit is in samenspraak met SURF opgesteld. De voornaamste documenten en richtlijnen zijn:

Algemene richtlijnen:

1. De Code voor Informatiebeveiliging (NEN-ISO/IEC 27001/27002)
2. Richtlijn “Risicoanalyses informatiesystemen”

Universitaire richtlijnen:

3. Gedragscodes voor studenten en medewerkers: zoals acceptabel gebruik van informatievoorzieningen, Studentenstatuut)
4. Integriteitcodes voor wetenschappelijke onderzoek
5. Het wachtwoordenbeleid
6. Het Identity Management beleid (ULCN)

SURF-IBO en SURFnet richtlijnen:

7. SURF-IBO richtlijnen m.b.t. informatiebeveiliging
8. Toepasbare Best Practices van SURF-IBO
9. SURFnet voorwaarden voor aansluiting van de Universiteit op SURFnet
10. Surffederatie afspraken

Andere richtlijnen:

11. Studielink afspraken

4. Business Continuity

4.1 Definitie

De business continuity richt zich – net als verzekeringen – op het identificeren van potentiële bedreigingen, de impact op de organisatie bij optreden ervan (schade) en de kosten van de maatregelen om dit te voorkomen. In de literatuur gaat business continuity over het overleven van een crisis of calamiteit, verderop in deze notitie wordt ook de business continuity bij lichtere bedreigingen (cq. incidenten) behandeld.

Een voorbeeld: het risico bestaat dat er brand optreedt in het Snelliusgebouw, dat het ULCN-systeem verwoest. De impact hiervan is dat de wachtwoorden van gebruikers niet meer gecontroleerd kunnen worden en de gebruikers niet meer bij hun bestanden, e-mail en bedrijfstoepassingen kunnen. Dit duurt zo lang voort tot er nieuwe hardware is gevonden (gekocht?), deze geplaatst is in een ander gebouw en de back-ups zijn teruggezet (enkele dagen). De schade van deze calamiteit worden bepaald aan de hand van productiviteitsverlies en imagoschade. Maatregelen kunnen pragmatisch en goedkoop zijn, zoals de inzet van USB-sticks om bestanden zonder wachtwoord te bewaren, of het dubbel uitvoeren van het ULCN-systeem op een andere locatie.

Als er meer dan één systeem uitgevallen is, dan moet worden bepaald in welke volgorde de systemen worden hersteld. Middels de sourcingstrategie kan op spreiding van het risico gestuurd worden. Maar dit levert ook een extra complexiteit op: doordat verschillende systemen in een keten werken kan een uitbestede en beschikbare dienst (zoals Blackboard) niet benaderbaar zijn doordat een interne dienst (ULCN) niet beschikbaar is. Goed inzicht in dergelijke onderlinge afhankelijkheden is randvoorwaardelijk voor een goede business continuity strategie.

4.2 Beleid

Voor de bestaande voorzieningen heeft de Universiteit Leiden er voor gekozen om zich niet te verzekeren voor crises op het gebied van ICT. Dit geldt voor zowel de interne (shared) diensten bij het ISSC als het uitbestede beheer van Blackboard, uSis en SAP. Voor het ISSC geldt dat in geval van een calamiteit op basis van de vakkundigheid van de ICT-medewerkers zo snel als mogelijk de herstelacties uitgevoerd worden. De prioriteit wordt hierbij bepaald door de specialisten op basis van beschikbare mensen en middelen (hardware, back-ups en beschrijvingen).

Bij de besluitvorming omtrent contracten, nieuwe systemen en grote vernieuwingen wordt een scenario op basis van gegarandeerd herstel binnen één week opgeleverd, zodat het CvB op basis van de kosten een expliciete afweging kan maken.

4.3 Maatregelen

De universiteit heeft belangrijk voorwerk verricht voor de randvoorwaarden die horen bij de huidige strategie van niet verzekeren, maar van een “in control”-situatie is nog geen sprake. Op centraal en decentraal management niveau worden trainingen en workshops gehouden voor crisisbeheersing. Voor uSis, Blackboard en SAP is het vraagstuk rondom calamiteiten onderdeel van de contractafspraken en kan bij een heronderhandeling of nieuwe aanbesteding worden aangepast.

Gelukkig komen calamiteiten maar zelden voor, daardoor zijn de afspraken over het serviceniveau (zogenaamde dienstniveau-overeenkomsten – DNO – of service level agreements) minstens zo belangrijk. Serviceniveau afspraken richten zich op gewone verstoringen (incidenten), waarbij calamiteiten bijna altijd uitgesloten worden van de garanties. Ook de serviceniveau’s van de verschillende systemen en onderdelen van de ICT-infrastructuur zijn nog onvoldoende in relatie bekeken. Hierbij geldt dat een gebruiker weinig gebaat is bij een beschikbaarheid van 99.7% van Blackboard als het netwerk of ULCN een veel lagere beschikbaarheid kennen.

5. Governance informatiebeveiligingsbeleid

De term governance heeft betrekking op het goed, efficiënt en verantwoord leiden van een organisatie. Het omvat de processen, de overleggen, de taken en verantwoordelijkheden van de belanghebbenden, zoals de eigenaren, werknemers, studenten, andere afnemers en de samenleving als geheel..

In dit hoofdstuk wordt de governance van informatiebeveiliging beschreven. Het is van belang dat de taken, verantwoordelijkheden en bevoegdheden met betrekking tot dit beleidsterrein eenduidig zijn toegewezen. Deze toewijzing heeft tot doel te voorkomen dat zaken dubbel worden uitgevoerd of dat de uitvoering van beveiligingstaken achterwege blijft.

5.1 IB governance

In deze paragraaf wordt beschreven hoe de governance van de informatiebeveiliging is georganiseerd en wie waarvoor verantwoordelijk is.

	CvB	Security manager IM	Security Officer ISSC	IMers eenheden / fac. Security off.	Beveiligingsmanager VG	Hoofd AIC	Hoofd IM	Hoofd JZ	Hoofden FB	Systeemeigenaar
Beleidsontwikkeling										
- IB-visie	A	R	C	C	C	C	S	I	I	I
- dreigingsanalyse	I	C	C	C	R	I	C	C	C	C
- classificatie van concerninformatie – systemen	I	R	C	C	C	S	I	C	C	A
- classificatie van facultaire systemen		I	C	R	I	I	S	I		
- opstellen en onderhouden hoofdstuk ICT binnen integraal crisismanagementplan	A	C	C	I	R	I	S	I	I	I
- opstellen en onderhouden prioritering informatiesystemen	I	R	C	C	I	I	A	I	C	C
- opstellen en onderhouden privacy verklaring		C	I	I	I	I	I	R	I	I
- Opstellen en onderhouden gedragscode	I	R	C	I	I	I	A	C	I	I
Opstellen baseline	I	R	C	C	C	C	A	I	I	I

	CvB	Security manager IM	Security Officer ISSC	IMers eenheden / fac. Security off.	Beveiligingsmanager VG	Hoofd AIC	Hoofd IM	Hoofd JZ	Hoofden FB	Systeemeigenaar
Advisering over IB-beleid										
- Advisering aan projecten		R	C	C	C		S	C	C	A
- Advisering aan eenheden		C	C	R	C		I	C	I	I
- beantwoorden vragen fac. informatiemanagers		R	C	I	C		A	C	I	I
risicoanalyse systeem		R	C	C	I	I	I	I	C	A
Regie										
- coördinatie grote IB-incidenten en calamiteiten	I	C	C	I	C	I	S	I	R	A
- coördinatie kleine IB-incidenten		I	R	I			S		C	A
- evaluatie van grote IB-incidenten	I	R	C	I	I		A	I	C	C
- coördinatie universiteitsbrede IB-processen		R	C	I	C	I	A	I	C	I
Auditing										
- auditkalender ICT	A	R	C	I	I	C	S	I	C	C
- uitvoeren audits	I	R	C	C	I	A	I	I	C	C
- uitvoeren risicoanalyse		R	C	C	I	I	A	I	C	C
- bewaken opvolgen aanbevelingen	I	C	C	C	C	I	C	I	R	A

Tabel 1: Governance

Legenda
R = responsible = verantwoordelijk voor de uitvoering
A = accoubntable = eind verantwoordelijk
S = sign-off = verantwoordelijk voor proces
C = consulted = geconsulteerd bij het proces
I = informed = geïnformeerd over de uitkomsten

5.2 Organisatie van de informatiebeveiligingsfunctie

Om informatiebeveiliging gestructureerd en gecoördineerd op te pakken worden taken, bevoegdheden en verantwoordelijkheden toegewezen. In dit hoofdstuk wordt ingegaan op de organisatie van de informatiebeveiligingsfunctie. Door de separate beschrijving van de informatiebeveiligingsfunctie in dit hoofdstuk kan de indruk ontstaan dat hiervoor een afzonderlijke organisatie moet worden ingericht. Dit is niet het geval. Het gaat erom taken, bevoegdheden en verantwoordelijkheden toe te wijzen aan functionarissen binnen de bestaande organisatiestructuur. Voor de meeste Security Officers die zich bezighouden met informatiebeveiliging zal het onderwerp geen fulltime job zijn, maar onderdeel uitmaken van hun takenpakket.

College van Bestuur
Het College van Bestuur is eindverantwoordelijk voor de informatiebeveiliging binnen de universiteit en stelt het beleid en de minimale maatregelen op het gebied van informatie-beveiliging vast. De inhoudelijke verantwoordelijkheid voor informatiebeveiliging is via de directeur Bedrijfsvoering van het Bestuursbureau gemandateerd aan het hoofd van de afdeling Informatiemanagement. Deze functionaris belast de Security Manager met de opdracht om informatiebeveiliging conform dit beleid uit te (doen) voeren.

Systeemeigenaar
De systeemeigenaar is er verantwoordelijk voor dat de applicatie en de informatie die daarin verwerkt wordt een goede ondersteuning biedt aan het proces waarvoor deze verantwoordelijk is. Dit betekent dat de systeemeigenaar ervoor zorgt dat zowel nu als in de toekomst de applicatie blijft beantwoorden aan de eisen en wensen van de gebruikers en aan wet- en regelgeving. Uiteraard moet de applicatie voldoen aan het informatiebeveiligingsbeleid en tenminste de minimale maatregelen.

Als uit een risicoanalyse blijkt dat er een verhoogd of hoog risico is, dan zijn er meer maatregelen noodzakelijk. De systeemeigenaar kan hiervan echter afwijken maar dan moet dit met redenen zijn omkleed en aan de Security Manager bekend worden gemaakt. De Security Manager bekijkt dit en zal het vastleggen. Hij zal de directeur BV van het Bestuursbureau aan het CvB adviseren over de risico's die als gevolg hiervan ontstaan.

Portefeuillehouder informatiebeveiliging
Iedere faculteit en eenheid, alsmede de Universiteit als geheel, kent een portefeuillehouder informatiebeveiliging op het hoogste bestuurlijke niveau. Deze directeur is door het bestuur van de faculteit of eenheid gemandateerd voor de invoering en uitvoering van het informatiebeveiligingsbeleid binnen zijn faculteit of eenheid. Binnen het CvB is de portefeuillehouder bedrijfsvoering tevens verantwoordelijk voor informatiebeveiliging.

Security Manager (bij het Bestuursbureau/IM)
De Security Manager ziet organisatiebreed toe op de naleving van het IB-beleid en daaruit voortvloeiende maatregelen, zorgt voor onderzoek en adviseert in complexe beveiligingsvraagstukken, initieert risicoanalyses en security audits, organiseert bedrijfsbrede security awareness programma's en vervult een adviserende rol naar directie en bestuur.

Deze rol heeft een strategisch karakter en wordt ingevuld door de afdeling Informatiemanagement van het Bestuursbureau. De Security Manager rapporteert via het hoofd informatiemanagement aan de directeur Bedrijfsvoering van het Bestuursbureau en aan het College van Bestuur.

Security Officers (faculteiten en eenheden)
De Security Officer is binnen zijn faculteit of eenheid het aanspreekpunt voor informatiebeveiligingsvraagstukken. Bij faculteiten zal dit in de praktijk zal dit meestal de informatiemanager zijn. Hij/zij is verantwoordelijk voor de implementatie en naleving van het informatiebeveiligingsbeleid en de minimale maatregelen voor systemen waarvan de betreffende faculteit het eigenaarschap heeft. Hiertoe kan behoren het (laten) uitvoeren van risicoanalyses voor informatiesystemen, het opstellen van informatiebeveiligings-rapportages en zorgen voor vergroting van het beveiligingsbewustzijn.

Verder signaleert de Security Officer incidenten en adviseert hoe ze op te lossen. Tevens is hij/zij aanspreekpunt voor de eigen organisatie voor eventuele interne en externe contacten. Security Officer is een rol, waarbij de functionaris rapporteert aan de portefeuillehouder informatiebeveiliging binnen de eigen organisatie.

De Security Officer van het ISSC heeft een aantal extra taken. De security officer verricht samen met de security manager risicoanalyses op de (concern) systemen. Tevens wordt de security manager ingelicht als de minimale maatregelen van de operationele (concern)systemen niet worden nageleefd en vertaalt deze naar risico's voor de dienstverlening van het ISSC. De security officer ISSC is ook de voorzitter van het CERT-team dat de binnengekomen security-incidenten afhandelt of doorstuurt naar de desbetreffende security officers van de faculteiten en expertisecentra. Ten slotte is de security officer ook Site Security contact voor verzoeken van SURFnet .

Beveiligingsmanager VG
De beveiligingsmanager Vastgoed heeft zijn eigen beleid en maatregelen ten aanzien van fysieke beveiliging. Hij is tevens verantwoordelijk voor het opstellen en onderhouden van het crisismanagementplan en voor het coördineren van grote IB-incidenten en calamiteiten. Verder is hij verantwoordelijk voor de dreigingsanalyse en wordt geïnformeerd en geconsulteerd bij onderdelen van IB-beleidsontwikkeling , regie en auditing.

Hoofd AIC
Het hoofd van de afdeling Audit en Interne Controle is verantwoordelijk voor controle, toetsing en beoordeling van de kwaliteit van administraties en de uitvoering van het financieel-economische beleid, door middel van audits op specifieke onderwerpen. In het kader van de jaarrekeningcontrole wordt onder zijn leiding de audits op financiën, bedrijfsvoering en automatisering verricht. Deze laatste audits worden verricht door de security manager op SAP en uSis. Daarnaast vindt er nog een SURFaudit plaats.

Hoofd IM
De sectie ICT-beleid van de afdeling Informatiemanagement is verantwoordelijk voor het informatiebeleid van de universiteit. Jaarlijks wordt de ICT-projectenkalender opgesteld waarin het ICT-meerjarenplan wordt vertaald in concrete ICT-projecten. Eén van de taken van de afdeling is informatiebeveiliging. De security manager verricht zijn taken onder leiding van het hoofd IM. Over alle taken van de security manager in het

governance IB-model wordt het hoofd geïnformeerd of geconsulteerd of is hij/zij verantwoordelijk voor het proces.

Hoofd JZ
Het hoofd Juridische Zaken en de security manager hebben werkzaamheden die elkaar overlappen op voornamelijk het privacygebied en het opstellen en onderhouden van de gedragscode voor het gebruik van informatievoorzieningen. Voor privacybeleid is juridische zaken verantwoordelijk en voor de gedragscode de security manager. De rol van functionaris gegevensbescherming is bij Juridische Zaken belegd.

Hoofden FB
De hoofden functioneel beheer zijn verantwoordelijk voor het functioneel beheer van systemen als SAP, uSis en andere (concern) systemen. Risicoanalyses of audits op systemen zullen met medewerking van deze hoofden worden verricht. Uiteindelijk zullen zij de resultaten hiervan bespreken met de systeemeigenaren en zijn zij dan ook verantwoordelijk voor het uitvoeren van geaccepteerde aanbevelingen.

5.3 Afstemming met aanpalende beleidsterreinen

Onderdeel van de governance is dat aan alle soorten risico's en hun onderlinge verwevenheid passende aandacht geschonken wordt. Het is om die reden dat op strategisch niveau zowel aandacht geschonken wordt aan informatiebeveiliging als aan fysieke beveiliging, ARBO-veiligheid en bedrijfcontinuïteit. Immers, samenwerking tussen deze disciplines is een noodzakelijke voorwaarde voor governance.

Dit is vormgegeven door de planningscyclus voor deze aspecten parallel te laten verlopen. Dat biedt handvatten om onderlinge interferentie op te merken en te behandelen. Waar wenselijk en mogelijk wordt deze afstemming ook vertaald naar het tactische en operationele niveau, maar alleen daar waar het toegevoegde waarde biedt.

5.4 Bewustwording

Veel gebruikers en beheerders van informatie zijn zich niet bewust van de risico's die men in het kader van informatiebeveiliging loopt of zijn zich niet voldoende bewust van de verantwoordelijkheid die zij dragen ten opzichte van de informatie waar zij toegang toe hebben. Helaas is dit een vruchtbare voedingsbodem voor incidenten. Onderzoek geeft aan dat de meerderheid van beveiligingsincidenten zijn oorsprong vindt binnen de eigen organisatie. Daarom is bewustwording of liever bewustmaking een belangrijk instrument bij informatiebeveiliging. De security manager is verantwoordelijk voor het bewustwordingsproces en ontwikkelt jaarlijks een campagne hiervoor.

5.5 Controle en naleving

De uitvoering van de informatiebeveiliging wordt jaarlijks geëvalueerd. Dit gebeurt in het najaar in het kader van het accountantsonderzoek en wordt zoveel mogelijk afgestemd met de normale Planning & Controlcyclus.

Daarnaast wordt onder leiding van SURF-IBO elke twee jaar een SURF-audit verricht. Het raamwerk voor de evaluatie is gebaseerd op de Code voor Informatiebeveiliging van het Nederlands Normalisatie-instituut. De in de Code genoemde onderwerpen vormen het uitgangspunt bij het beoordelen van de beveiligingssituatie van de universiteit.
De SURF-audit bestaat uit drie onderdelen: het informatiebeveiligingsbeleid, afspraken, incidentenregistratie- en afhandeling en het Identity Management-beleid.

5.6 Sancties

Bij schending van de regels ten aanzien van informatiebeveiliging kunnen door of namens het College van Bestuur maatregelen worden getroffen. Maatregelen kunnen bijvoorbeeld zijn blokkering van de toegang tot het netwerk of specifieke netwerkdiensten. Ingeval van "spamming" (het verzenden van zeer grote aantallen ongewenste en ongevraagde e-mails) kan de overtreder de toegang tot e-mailvoorzieningen geweigerd worden.

Voor alle gebruikers van de Leidse informatievoorzieningen is een gedragscode beschikbaar die is gepubliceerd via de universitaire website (http://media.leidenuniv.nl/legacy/lei_gedragsregels_iv_nl_v3.pdf. Deze code is van toepassing op zowel studenten, medewerkers als derden.

Bij constatering van overtreding van de gedragsregels kan het College van Bestuur op voorstel van de portefeuillehouder informatiebeveiliging van de faculteit of eenheid waar de overtreding is begaan een disciplinaire sanctie opleggen.

Ingeval de Universiteit Leiden wordt aangesproken bij overtreding van intellectuele eigendomsrechten of andere regelgeving dan wel bij schending van rechten van anderen, kan de Universiteit Leiden eventuele schade verhalen op de schadeveroorzakende gebruiker. Indien schade wordt geleden als gevolg van misbruik van computer- en netwerkvoorzieningen kan de Universiteit Leiden deze verhalen op de schadeveroorzakende gebruiker.

6. Melding en afhandeling van incidenten

Incidentenbeheer en –registratie hebben betrekking op de wijze waarop geconstateerde dan wel vermoede inbreuken op de informatiebeveiliging door medewerkers gemeld worden en de wijze waarop deze worden afgehandeld.

Elke faculteit en eenheid is zelf verantwoordelijk voor het signaleren en melden van incidenten met en inbreuken op de informatiebeveiliging. Medewerkers kunnen incidenten met betrekking tot gegevens of personen melden aan de security officer/informatiemanager van hun faculteit. De Security Officer kan het incident zelf of met behulp van anderen oplossen, waarna het incident kan worden afgemeld.

Security incidenten zoals phishing of spam kunnen worden gemeld bij het CERT van het ISSC via abuse@leidenuniv.nl.

Het Computer Emergency Response Team (CERT) richt zich op de technische aspecten van informatiebeveiliging en is verantwoordelijk voor:

- Het verzamelen van informatie over potentiële ICT-beveiligingsincidenten en beveiligingslekken
- Het centraal registreren van ICT-beveiligingsincidenten
- Het analyseren en beoordelen van de aard, omvang en oorzaak van het ICT-beveiligingsincident
- Het organiseren van de evaluatie van de afhandeling van ICT-beveiligingsincidentendie de universiteit niet overstijgen. Gebeurt dit wel dan zal de Security Manager het voortouw nemen.
- Het adviseren van de staande organisatie over de te nemen preventieve en herstelacties bij ICT-beveiligingsincidenten van beperkte omvang
- Het adviseren van het crisisteam over de te nemen preventieve en herstelacties bij ICT-beveiligingsincidenten van grote omvang
- Het informeren en instrueren van de direct betrokkenen over de uit te voeren preventieve en herstelacties
- Het centraal informeren van gebruikers over ICT-beveiligingsincidenten
- Het coördineren van de uitvoering van preventieve- en herstelacties

De volgende incidenten worden o.a. geregistreerd:

- Niet verklaarbare onregelmatigheden in logfiles van systemen en applicaties;
- Falen van een integriteitcontrole t.b.v. een informatiesysteem of informatiebron;
- Verlies van een informatiebron;
- Ongeplande uitval van informatiesystemen langer dan vijf minuten waarvan de Security Officer oordeelt dat dit een incident is
- (vermoedelijke) inbraak op een systeem;
- (vermoeden van) misbruik van een systeem of gegevens door een legitieme gebruiker;
- (vermoeden van) een grote virusuitbraak op het universitaire- en/of lokale netwerk;
- (mogelijk) zeer bedreigende virusuitbraak op het Internet.

Bovenstaande incidenten worden geregistreerd en afgehandeld en dienen als input voor de incidentrapportages.