Informatiebeveiligingsbeleid

Universiteit Leiden

Versie 9
juni 2004

Inhoudsopgave

1 Inleiding 3
1.1 Opbouw beleid 3
1.2 Status 4
1.3 Begripsbepalingen 4
1.4 Onderhoud van het beleid 5
1.5 Doelstelling van het beleid 5
1.6 Reikwijdte van het beleid 5
2 Beleidsrichtlijnen 7
2.1 Organisatie informatiebeveiliging 7
2.1.1 Rollen en verantwoordelijkheden 7
2.1.2 Planvorming en planning 8
2.1.3 Financiering 8
2.2 Waardering van informatie 9
2.3 Verwachtingen t.o.v. individuen 9
2.4 Toegang tot informatie 9
2.5 Wet en regelgeving 10
2.5.1 Wet computercriminaliteit 10
2.5.2 Wet Bescherming Persoonsgegevens 11
2.5.3 Telecommunicatiewet 11
2.5.4 Auteurswet 11
2.5.5 Archiefwet 12
2.6 Controle en naleving 12

Het College van Bestuur besluit,

1 Inleiding

Dit document bevat het beleid ten aanzien van informatiebeveiliging voor de Universiteit Leiden. Evenals vele andere organisaties is de Universiteit in toenemende mate afhankelijk van informatie en (veelal geautomatiseerde) informatievoorzieningen. Deze afhankelijkheid brengt nieuwe kwetsbaarheden en risico's met zich mee. Kwetsbaarheden en risico's die met geschikte maatregelen beperkt dienen te worden ten einde onderwijs en onderzoek op een hoogwaardig academisch niveau te kunnen waarborgen.

Het informatiebeveiligingsbeleid beschrijft dat en hoe informatie en informatievoorzieningen dienen te worden beveiligd en hoe op een veilige wijze met informatie dient te worden omgegaan. Uitgangspunt daarbij is dat evenwicht tussen vrijheid van handelen en veiligheid van informatie bewaard blijft. Dat evenwicht kan voor verschillende groepen binnen de universiteit anders liggen.

Het informatiebeveiligingsbeleid wordt op verschillende niveaus vorm gegeven. In de volgende paragrafen wordt de opbouw beschreven.

1.1 Opbouw beleid

Onderstaand schema geeft weer hoe het Universitair Informatiebeveiligingsbeleid is opgebouwd.

A - Universitaire beleidsrichtlijnen
(dit document)

Eigenaar	College van Bestuur. Versie en wijzigingsbeheer door Informatiemanagement in de persoon van de Security Manager.
Doel	Richting geven en kaders stellen.
Status	Toepassen is verplicht en verklaren wat niet toegepast kan worden en waarom is noodzakelijk. Securitymanager beoordeelt of verklaring voldoende is en legt eventueel voor aan College van Bestuur.
Inhoud	Benoeming van aandachtsgebieden, toedeling van verantwoordelijkheden en beschrijving van hoofdprocessen

B - Universitaire Minimum Maatregelen

Eigenaar	Informatiemanagement in de persoon van de Security Manager.
Doel	Voorzien in een mimimaal vereist beveiligingsniveau.
Status	De maatregelen zijn verplicht. Afwijken mag alleen met toestemming van het College van Bestuur.
Inhoud	Beveiligingsmaatregelen, voortvloeiend uit de beleidsrichtlijnen, noodzakelijk om universiteitsbreed een minimaal niveau van beveiliging te garanderen.

C – Informatiebeveiligingsplan eenheid

Eigenaar	Bestuur van de eenheid
Doel	Beschrijven van de maatregelen die de eenheid heeft genomen om een adequaat niveau van beveiliging te realiseren met toepassing van de richtlijnen.
Status	Het hebben en naleven van een Informatiebeveiligingsplan is verplicht.
Inhoud	1. Overzicht van welke minimum maatregelen wordt afgeweken (inclusief motivatie); 2. Een overzicht van extra genomen maatregelen 3. Beschrijving van de manier waarop de verschillende maatregelen zijn geïmplementeerd.

1.2 Status

Dit beleid treedt in werking op 8 juli 2004 en kan worden aangehaald als "Informatiebeveiligingsbeleid van de Universiteit Leiden".

1.3 Begripsbepalingen

Onderstaande tabel geeft weer op welke wijze begrippen gebruikt in documenten aangaande informatiebeveiliging geïnterpreteerd dienen te worden.

Informatie en gegevens	Strikt genomen is er een verschil tussen de begrippen "gegevens" en "informatie". In het kader van informatiebeveiliging is dit verschil veelal onbelangrijk. In dit document zullen deze begrippen als uitwisselbaar worden beschouwd.
Informatiesysteem	Systeem voor de verwerking en/of overdracht van informatie. Dit omvat zowel geautomatiseerde systemen (bijvoorbeeld een computerapplicatie) als niet-geautomatiseerde systemen (bijvoorbeeld een kaartenbak). In principe wordt met het begrip "informatiesysteem" verwezen naar het gehele systeem.

	In het geval van de kaartenbak omvat dit dan de bak, de kaarten een eventuele index-kaart etc. In het geval van de computerapplicatie omvat dit de applicatie zelf, het host-systeem waarop de applicatie draait, de terminal die wellicht gebruikt wordt om de applicatie te benaderen, het communicatie netwerk dat hierbij gebruikt wordt etc.
Systeem	Het begrip “systeem” kan verwijzen naar “informatiesysteem” maar wordt met name in de ICT wereld ook veelal geïnterpreteerd als verwijzing naar een “computersysteem” (het fysieke apparaat). Ter voorkoming van misverstanden zal dit begrip niet op zichzelf gebruikt worden.
ICT	Informatie en Communicatie Technologie, technologie, gericht op het digitaal exploiteren van gegevens
Informatievoorziening	Middel om in informatie te voorzien. Een informatiesysteem is per definitie een informatievoorziening. Een poster aan de muur eveneens, maar een poster is geen informatiesysteem.
Eenheid	Een organisatorische eenheid op welke dit informatiebeveiligingsbeleid van toepassing is.

1.4 Onderhoud van het beleid

De organisatie zelf, de bedrijfsprocessen, de informatievoorziening en daarmee de informatiebeveiliging zijn voortdurend aan verandering onderhevig. Dit vraagt van de organisatie een alerte en anticiperende houding ten opzichte van de informatiebeveiliging. Allerlei ontwikkelingen en gebeurtenissen kunnen van invloed zijn op de informatiebeveiliging en daarmee op de in dit document beschreven aanpak van informatiebeveiliging.

Dit beleid dient dan ook jaarlijks op inhoud, uitvoerbaarheid en implementatiestatus te worden beoordeeld en, indien nodig, aangepast. De inhoudelijke toetsing en bijstelling van het beleid vindt plaats binnen het Beveiligingsoverleg, dat gevoerd wordt door de Security Manager en de Security Officers. De redactie en het versiebeheer van het document ligt bij Informatie Management. Dit proces van controle en beheer is een continu proces, echter jaarlijks wordt expliciet een revisie uitgevoerd. Hierover wordt gerapporteerd aan het College van Bestuur.

1.5 Doelstelling van het beleid

Het doel van het beleid is het bereiken en handhaven van de continuïteit van de primaire (bedrijfs)processen van de Universiteit. Deze processen zijn ruwweg te omschrijven als het geven van onderwijs en het doen van onderzoek.

1.6 Reikwijdte van het beleid

Dit beleid heeft betrekking op:

- De beveiliging van informatie die ontleend kan worden aan gegevensverzamelingen van de Universiteit, gegevensverzamelingen van derden welke de Universiteit in haar beheer heeft en/of informatie die

ontleend kan worden aan het gebruik van universitaire informatievoorzieningen;
- De beveiliging van persoonsgegevens die worden verwerkt door de Universiteit;
- De beveiliging van de [*geautomatiseerde*] informatiesystemen van de Universiteit en andere Universitaire informatievoorzieningen;
- De beveiliging van de ICT-voorzieningen die (mede) gebruikt worden voor gegevensverzamelingen, informatiesystemen en –voorzieningen van de Universiteit.

Dit beleid geldt voor alle onderdelen van de Universiteit Leiden en voor de diverse ‘inwonende organisaties’ voorzover zij gebruikmaken van gegevensverzamelingen, informatiesystemen van de Universiteit.

Verder dient notie genomen te worden van het feit dat het beleid locatie onafhankelijk is. Ook indien men als student, onderzoeker of medewerker werkzaamheden verricht op een locatie die niet tot de Universiteit behoort, maar waarbij men wel met informatie of informatievoorzieningen van de Universiteit werkt, dient men dit beleid te respecteren.

2 Beleidsrichtlijnen

2.1 Organisatie informatiebeveiliging

2.1.1 Rollen en verantwoordelijkheden

Ten behoeve van de organisatie van informatiebeveiliging is een drietal rollen expliciet gedefinieerd:

Portefeuillehouder informatiebeveiliging

Iedere eenheid, alsmede de Universiteit als geheel, kent een portefeuillehouder informatiebeveiliging op het hoogste bestuurlijke niveau. Deze persoon is eindverantwoordelijke voor de invoering en uitvoering van het informatiebeveiligingsbeleid binnen zijn eenheid en aansprakelijk voor schade als gevolg van het niet of niet correct naleven van het informatiebeveiligingsbeleid.

Security Manager

De Security Manager ziet organisatiebreed toe op de naleving van het informatiebeveiligingsbeleid en daaruit voortvloeiende maatregelen, zorgt voor onderzoekt en adviseert in complexe beveiligingsvraagstukken, initieert security audits (indien van toepassing ook risico analyses), organiseert bedrijfsbrede security awareness programma's en opleidingen en vervult een adviserende rol naar directie en bestuur. Tevens zorgt de Security Manager voor heldere communicatie bij incidenten op het vlak van informatiebeveiliging. Deze rol heeft een strategisch karakter.

Deze rol zal worden ingevuld door de afdeling Informatiemanagement van het Bestuursbureau. De uitvoerende functionaris rapporteert aan de portefeuillehouder informatiebeveiliging in het Universiteitsbestuur.

Security Officer

Bij iedere eenheid is de verantwoordelijkheid voor het samenstellen van het Informatiebeveiligingsplan en het uitvoeren of doen uitvoeren van de daaruit voortvloeiende activiteiten toegewezen aan de Security Officer.

De Security Officer is een rol, waarbij de uitvoerende functionaris rapporteert aan de portefeuillehouder informatiebeveiliging van het bestuur van de eenheid.

Voor het overige worden beveiligingstaken beschouwd als een onderdeel van het takenpakket van bestaande functies. Daartoe worden in werkafspraken met functionarissen vastgelegd welke taken dat zijn. Dit geldt in het bijzonder voor verplichtingen betreffende geheimhouding, integriteit en/of beschikbaarheid van informatie welke voortvloeien uit contracten met derden (bijv. 3de geldstroom onderzoek).

Hierbij geldt in beginsel dat de persoon die het contract sluit verantwoordelijk is voor de naleving van de contractuele verplichtingen. Voorzover verplichtingen betrekking hebben op de geheimhouding, integriteit en/of beschikbaarheid van informatie, dient dit kenbaar gemaakt te worden aan de Security Officer van het onderdeel waartoe deze persoon behoort.

De praktische uitwerking van het beleid dient zoveel mogelijk ingebed te worden in de reguliere bedrijfsvoering.

2.1.2 Planvorming en planning

Alle eenheden maken als onderdeel van het jaarplan een informatiebeveiligingsplan waarin uiteengezet wordt op welke wijze zij invulling geven aan het Informatiebeveiligingsbeleid. Ieder jaar wordt door de Security Manager in overleg en overeenstemming met de Security Officers een minimaal niveau van beveiliging vastgesteld, dat voor het daarop volgende jaar bindend wordt voor alle eenheden bij het vaststellen van de jaarplannen op het gebied van beveiliging. Dit minimale niveau is onderdeel van het geconsolideerde jaarplan informatiebeveiliging.
Het jaarplan Informatiebeveiliging bestaat uit

- De verzameling minimale maatregelen voor het betreffende jaar
- Een samenvatting van de Informatiebeveiligingsplannen van de eenheden
- Een samenvatting van de gevallen waarin niet voldaan wordt aan het minimale niveau

Het geconsolideerde jaarplan informatiebeveiliging is onderdeel van het Jaarplan ICT en wordt voorgelegd aan het ICT beraad dat hierover advies uitbrengt aan het College van Bestuur.

Erkend wordt dat informatiebeveiliging verder gaat dan alleen ICT en wellicht niet thuis hoort in het Jaarplan ICT, echter gezien de huidige inrichting van de organisatie lijkt vooralsnog het Jaarplan ICT het meest geschikte onderkomen voor het jaarplan informatiebeveiliging.

2.1.3 Financiering

Informatiebeveiliging kost geld en in veel gevallen is de persoon die de waarde van informatie vast kan stellen (de gemandateerde eigenaar) niet dezelfde persoon die beschikking heeft over het benodigde budget voor de juiste beveiliging van die informatie.

De financiering van beveiligingsmaatregelen is in beginsel een interne aangelegenheid van de verschillende eenheden. In geval een eenheid niet in staat is of meent te zijn de kosten te dragen voor de minimale maatregelen die zij krachtens dit beleid zou moeten nemen kan zij zich wenden tot het College van Bestuur.

Indien het College van mening is dat de betreffende eenheid inderdaad niet in staat geacht moet worden de maatregel op eigen kracht door te voeren, kan het College besluiten te voorzien in een financieringsmogelijkheid dan wel besluiten dat de maatregel(en) niet hoeft/hoeven te worden ingevoerd.

In het laatst genoemde geval is het bestuur van de betreffende eenheid niet langer aansprakelijk indien schade ontstaat als gevolg van het niet doorvoeren van de benodigde maatregel(en).

2.2 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 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.

2.3 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 gegeven wordt en 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.

2.4 Toegang tot informatie

Alle gegevens waarop dit beleid van toepassing is (zie paragraaf 1.6) is geclassificeerd in één van onderstaande klassen:

- Publiek
- Intern
- Beperkte toegang

Voor Publieke gegevens gelden de volgende basisprincipes:

- iedereen mag deze gegevens inzien;
- een geselecteerde groep mag deze gegevens wijzigen;

Voor Interne gegevens gelden de basis principes:

- iedereen die aan de Universiteit is verbonden als medewerker, student of onderzoeker mag deze gegevens inzien;
- een geselecteerde groep mag deze gegevens wijzigen;

Voor gegevens met een Beperkte toegang classificatie geldt dat expliciet dan wel impliciet aangegeven is wie welke rechten heeft t.a.v. de verwerking van deze gegevens. Impliciet kan dit worden aangegeven door bijvoorbeeld het toepassen van authenticatie en autorisatie technieken in een informatiesysteem (indien het systeem geen toegang geeft, behoort de gebruiker van het systeem niet tot de groep die rechten heeft gekregen). Expliciet kan dit worden aangegeven door in papieren rapporten bijvoorbeeld een distributielijst op te nemen.

Voorts dienen informatiebronnen en -systemen in beginsel alleen voor de doelgroep bereikbaar[1] te zijn. Indien dit niet mogelijk is dient bij de beveiliging van de informatiebron of het informatiesysteem rekening gehouden te worden met het extra risico dat dit met zich mee brengt.

Autorisaties dienen in overeenstemming te zijn met de binnen de universiteit geldende en in gebruik zijnde functiescheiding.

2.5 Wet en regelgeving

De Universiteit Leiden wil maatschappelijk verantwoord handelen. Daartoe zijn richtlijnen en gedragscodes opgesteld, die deels van toepassing zijn op specifieke beroepsgroepen, en voor het overige van toepassing zijn op iedereen die werkt of studeert aan de Universiteit Leiden of gebruik maakt van de informatievoorzieningen van de Universiteit. Met name gelden in dit verband de volgende richtlijnen en codes

- Acceptabel gebruik van informatievoorzieningen
- Het Studentenstatuut
- Integriteitcodes voor wetenschappelijke onderzoekers

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

- de Wet computercriminaliteit;
- de Wet bescherming persoonsgegevens;
- de Telecommunicatiewet;
- de Auteurswet;
- de Archiefwet.

Slechts indien hiertoe gesommeerd door een vertegenwoordiger van de rechterlijke macht in de functie van rechter-commissaris[2] of hoger zal het College van Bestuur van de Universiteit Leiden medewerking verlenen aan verstrekking van informatie aangaande gebruik van informatievoorzieningen door individuele of groepen gebruikers.

2.5.1 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:

- het binnendringen in een daartegen beveiligd computersysteem (computervredebreuk);
- het wederrechtelijk wijzigen en toevoegen van gegevens in een computer, ook als ze niet beveiligd zijn;

[1] Bereikbaar is niet hetzelfde als toegankelijk. Voor klanten van een bank is de kluis onbereikbaar (men kan er niet bij in de buurt komen) én dus ook ontoegankelijk. Voor medewerkers van de bank is de kluis misschien wel bereikbaar, maar daarmee nog niet per sé toegankelijk.

[2] Een vordering van de officier van justitie is voor de rechter-commissaris een voorwaarde voor bevoegdheidsuitoefening.

- het opzettelijk of door nalatigheid beschadigen of onbruikbaar maken of storen van een computersysteem

Naleving van dit informatiebeveiligingsbeleid en implementatie van de minimum maatregelen moet leiden tot een niveau van beveiliging dat als voldoende mag worden gezien in het kader van de wet computercriminaliteit.

2.5.2 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.

Het niet naleven van deze wet kan leiden tot het opleggen van sancties aan de Universiteit. Naleving van dit informatiebeveiligingsbeleid en implementatie van de minimum maatregelen moet leiden tot voldoen aan de Wet Bescherming Persoonsgegevens.

2.5.3 Telecommunicatiewet

De Telecommunicatiewet regelt allerlei zaken met betrekking tot gegevensverkeer over openbare netwerken. In het kader van informatiebeveiliging zijn vooral het beschermen van de persoonlijke levenssfeer van gebruikers en de regelgeving voor het bevoegd aftappen van openbare telecommunicatie netwerken van belang.

Met betrekking tot het laatste punt is nog geen duidelijkheid in hoeverre dat in de huidige situatie daadwerkelijk van belang is voor de Universiteit. De wet spreekt over “openbare netwerken” in de zin van “een telecommunicatienetwerk waarmee aan het publiek de mogelijkheid tot overdracht van signalen tussen netwerkaansluitpunten ter beschikking gesteld wordt”.

De heersende opvatting (o.a. bij de I-groep) is dat hiervan geen sprake is zolang alleen rechtspersonen uit de Surfdoelgroep worden toegelaten op het netwerk. Dan is immers geen sprake van toegang voor het publiek. Hieromtrent is echter nog weinig tot geen jurisprudentie in het Nederlands recht. Het wordt vrijwel zeker van belang op het moment dat de Universiteit netwerk diensten gaat aanbieden aan rechtspersonen die niet tot de Surfdoelgroep behoren.

Indien de regelgeving omtrent het aftappen van telecommunicatie netwerken van kracht wordt voor de Universiteit kan dit aanzienlijke (financiële) consequenties hebben. Terughoudendheid met het aanbieden van toegang tot het netwerk van de Universiteit aan rechtspersonen die niet behoren tot de SURF doelgroep is daarom geboden.

2.5.4 Auteurswet

De Auteurswet regelt het auteursrecht van originele werken op het gebied van letterkunde, wetenschap en kunst. Deze wet is ook van toepassing op originele programmatuur, inclusief de daarbij behorende documentatie.

Deze wet verbiedt o.a. het verspreiden van originele werken zonder dat daarvoor toestemming is verkregen van de eigenaar van de auteursrechten.

Het directe gevolg voor de Universiteit is dat men de ongeoorloofde verspreiding van auteursrechterlijk beschermde werken door studenten, onderzoekers en medewerkers zoveel mogelijk tegen gaat en hier zelf geen deel aan neemt. Een gevolg hiervan is dat de Universiteit het gebruik van software zonder het bezitten van de juiste licenties tegen gaat.

2.5.5 Archiefwet

De Archiefwet en het Archiefbesluit geven voorschriften over de wijze waarop omgegaan moet worden met informatie vastgelegd in (gedigitaliseerde) documenten, informatiesystemen, websites etc. De Universiteit valt onder de werkingssfeer van deze wetgeving. De uitvoering van deze wet is geregeld middels de Regeling Archiefbeheer Universiteit Leiden .

2.6 Controle en naleving

De uitvoering van de jaarplannen t.b.v. informatiebeveiliging wordt jaarlijks geëvalueerd. Dit gebeurt in het voorjaar ten tijde van het accountantsonderzoek en wordt zoveel mogelijk gecoördineerd met de normale Planning & Control cyclus.

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.