Baseline informatiebeveiliging
(minimale maatregelen)

Universiteit Leiden

Versie beheer

Versie 0.1	9 september 2013	1e concept
Versie 0.2	23 september 2013	2e concept na review door Erik Adriaens
Versie 0.3	8 oktober 2013	3e concept na review door Maritta de Vries
Versie 0.4	20 november 2013	4e concept na review door informatiemanagers en ISSC
Versie 0.5	16 december 2013	Concept na verwerking opmerkingen OBV
Versie 1.0	11 februari 2014	Vastgesteld door het college (gelijk aan 0.5)

Managementsamenvatting

De baseline informatiebeveiliging (Minimale Maatregelen) vormt een uitwerking van het informatiebeveiligingsbeleid van de Universiteit Leiden en omvat maatregelen met betrekking tot inrichting en ontwikkeling van de informatievoorziening en beheer en onderhoud van de informatievoorziening.

Daarnaast worden een aantal maatregelen opgesomd dat voorziet in een basisniveau aan beveiliging voor de universitaire informatiesystemen. Met de vaststelling en invoering van deze Baseline wordt uitvoering gegeven aan de strategische beleidsuitgangspunten die zijn vastgelegd in het informatiebeveiligingsbeleid.

Zowel het informatiebeveiligingsbeleid als de baseline hebben betrekking op alle personen, 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 eenheden.

Onder de baseline vallen maatregelen die moeten worden geïmplementeerd op systemen die in risicoklasse 3 vallen. Aan systemen die in een hogere klasse vallen, zoals klasse 2 en 1, zullen extra eisen en dus aanvullende maatregelen worden gesteld.

Inhoudsopgave

1. Inleiding

1.1 Aanleiding

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, onderwijsinstellingen, virussen die ervoor zorgen dat geld van de rekening wordt afgeschreven, spam en phishing, etc. Hierdoor wordt duidelijk dat meer aandacht aan deze zaken moet worden besteed en dat maatregelen hiertegen in kaart moeten worden gebracht en geïmplementeerd om deze aanvallen af te slaan.

Dit document Baseline Informatiebeveiliging (Minimale Maatregelen) vormt een uitwerking van het Informatiebeveiligingsbeleid van de Universiteit Leiden en omvat maatregelen met betrekking tot inrichting en ontwikkeling van de informatievoorziening en beheer en onderhoud van de informatievoorziening.

Daarnaast worden een aantal maatregelen opgesomd dat voorziet in een basisniveau aan beveiliging voor de universitaire informatiesystemen. Met de vaststelling en invoering van deze Baseline wordt uitvoering gegeven aan de strategische beleidsuitgangspunten die zijn vastgelegd in het informatiebeveiligingsbeleid (separaat document).

1.2 Visie op beveiliging

In het informatiebeveiligingsbeleid is de visie genoemd. Kort samengevat komt het er op neer dat de Universiteit Leiden actief wil 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.

In een aantal punten samengevat betekent dit:

- Informatiebeveiliging is en blijft een verantwoordelijkheid van het lijnmanagement
- Het primaire uitgangspunt voor informatiebeveiliging blijft risicomanagement
- De klassieke ib aanpak waarbij inperking van mogelijkheden de boventoon voert maakt plaats voor veilig faciliteren
- De focus verschuift van netwerkbeveiliging naar gegevensbeveiliging
- Verantwoord en bewust gedrag van mensen is essentieel voor een goede informatiebeveiliging
- Informatiebeveiliging vereist een integrale aanpak

1.3 Standaarden

Het normenkader voor het informatiebeveiligingsbeleid en de baseline van maatregelen is gebaseerd op Code voor Informatiebeveiliging: NEN 27001:2005 en NEN 27002:2005.

1.4 Werkingsgebied baseline

Zowel het informatiebeveiligingsbeleid als de baseline hebben betrekking op alle personen, 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 eenheden.

Onder de baseline vallen maatregelen die moeten worden geïmplementeerd op systemen die in klasse 3 vallen. Aan systemen die in een hogere klasse vallen, zoals klasse 2 en 1, zullen extra eisen en dus aanvullende maatregelen worden gesteld.

1.5 Verantwoordelijkheid baseline

Het College van Bestuur is eindverantwoordelijk voor de baseline en heeft dit op [datum] vastgesteld. De securitymanager is verantwoordelijk voor het onderhoud. De informatie- of systeemeigenaar is aanspreekbaar op de toepassing van de baseline. De verantwoordelijkheden worden in het informatiebeveiligingsbeleid verder uitgewerkt.

1.6 Doelstelling baseline

De baseline heeft tot doel het waarborgen van de continuïteit van de bedrijfsvoering en het minimaliseren van de schade door het voorkomen van beveiligingsincidenten en het minimaliseren van eventuele gevolgen.

2.Basisbeveiligingsniveau

2.1 Het basisbeveiligingsniveau

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 ib 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 wijzgen 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	Fraudeuleuze transactie
	Onweerlegbaarheid	Verloochening	Ontkennen een bepaald bericht te hebben verstuurd
Vertrouwelijkheid	Exclusiviteit	Onthulling	Afluisteren van netwerk;hacking
		Misbruik	Privé-gebruik op grote mate

Het basisbeveiligingsniveau bestaat uit het volgende:

Klasse	Omschrijving	Maatregel
Niveau 3	Een inbreuk op de beschikbaarheid, exclusiviteit en integriteit van het systeem veroorzaakt geen (grote) verstoring.	Het systeem moet voldoen aan de minimale maatregelen (ib-baseline)

De waardering van de drie IB aspecten ziet er als volgt uit:

IB aspecten	Waardering (Laag, Midden, Hoog)
Beschikbaarheid	L
Vertrouwelijkheid	L
Integriteit	L

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 (aanvullende) maatregelen worden genomen.

2.2 Aanvullende maatregelen

Als de dataklasse wordt aangemerkt als niveau 2 of niveau 1 dan is een hoger beveiligings-niveau noodzakelijk. Een hoger niveau is nodig in situaties waarin bijvoorbeeld met vertrouwelijke gegevens wordt gewerkt of een hogere beschikbaarheid van het systeem of (hoge) integriteit van informatie vereist is. Aanvullende maatregelen kunnen ook betrekking hebben op privacybescherming. Dit is onder andere het geval indien bij verlies of onrechtmatig/onzorgvuldig gebruik van persoonsgegevens er extra negatieve gevolgen ontstaan voor de betrokken persoon.

De volgende maatregelen moeten worden genomen als uit de risicoanalyse blijkt dat het systeem een verhoogd of hoog risico heeft:

IB aspecten	Selectie uit de aanvullende maatregelen
Beschikbaarheid	Redundantie
	Noodstroomvoorziening
	Fail-over voorziening
	Continu bewaking en follow up
	Secure opslag van bronprogrammatuur
Vertrouwelijkheid	Encryptie datatransport
	Harde authenticatie
	Autorisatie naar rol
	Clear desk
	Gecontroleerde afvoer
Integriteit	Invoercontrole
	Autorisatie naar rol
	Training (kern) gebruikers
	Licentieservers
	Tegengaan van schaduwbestanden

Na afloop van de risicoanalyse stelt de securitymanager een rapport op met de classificatie. Deze rapportage wordt uitgebracht aan de systeemeigenaar zodat deze weet hoe de beveiliging het systeem ervoor staat en welke maatregelen zouden moeten worden genomen. Tevens worden aanbevelingen gedaan. Wijkt de eigenaar van dit advies af dan wordt dit aan de security manager voorgelegd.

Elk jaar wordt gekeken of er gebeurtenissen hebben plaatsgevonden die er toe leiden dat een risicoanalyse moet worden aangepast.

3.De baseline (set minimale maatregelen)

De onderstaande standaardset van minimale maatregelen is gebaseerd op de Code van Informatiebeveiliging. De maatregelen worden als eindresultaat beschreven waarop getoetst kan worden. Het is de verantwoordelijkheid van de systeemeigenaar of door het bestuur van de faculteit of eenheid de maatregelen te waarborgen.

Organisatie

1. De verschillende rollen -zoals gedefinieerd in het informatiebeveiligingsbeleid- zijn belegd.

2. Niemand in een organisatie mag op uitvoerend niveau rechten hebben om een gehele cyclus van handelingen in een kritisch informatiesysteem te beheersen. Dit in verband met het risico dat hij of zij zichzelf of anderen onrechtmatig bevoordeelt of de organisaties schade toebrengt. Dit geldt voor zowel informatieverwerking als beheeracties.

Classificatie en beheer van bedrijfsmiddelen

3. Er is een actuele registratie (met doel en eigenaar) van bedrijfsmiddelen die voor de organisatie een belang vertegenwoordigen zoals informatie(verzamelingen), software, hardware en diensten.

4. Voor elk bedrijfsproces, applicatie, gegevensverzameling is een verantwoordelijke lijnmanager benoemd.

5. Er zijn rubriceringsrichtlijnen opgesteld voor het classificeren van informatie.

6. Alle software moet – door de faculteit / eenheid zelf of het ISSC – gelicenseerd zijn. Illegale software is niet toegestaan.

7. Vastgoed is verantwoordelijk voor tekeningen van gebouwen met alle relevante details.

8. Het bestaan en de consequenties van de Gedragscode voor ICT voorzieningen wordt regelmatig onder de aandacht gebracht van alle gebruikers van Informatievoorzieningen van de Universiteit Leiden. In ieder geval wanneer medewerkers in dienst treden en wanneer studenten een studie beginnen aan de Universiteit Leiden.

9. De systeemeigenaar zorgt voor een exit-procedure waarmee toegangsrechten tot informatievoorzieningen van medewerkers en studenten die de universiteit/faculteit/het onderdeel verlaten worden ingetrokken.

10. Er zijn beveiligingsmaatregelen rondom (gevoelige) apparatuur en bestanden in een computerruimte genomen.

Beheer van communicatie- en bedieningsprocessen

11 Er zijn bedieningsprocedures bij het ISSC die informatie bevatten over opstarten, afsluiten, backuppen en herstelacties, afhandelen van fouten, beheer van logs, contactpersonen, noodprocedures en speciale maatregelen voor beveiliging.

12. Er zijn logisch gescheiden systemen voor Ontwikkeling, Test en/of Acceptatie en Productie (OTAP). De systemen en applicaties in deze zones beïnvloeden systemen en applicaties in andere zones niet.

13. De ICT-voorzieningen voldoen aan het voor de diensten overeengekomen niveau van beschikbaarheid.

14. Er zijn maatregelen genomen voor detectie, preventie en herstellen om te beschermen tegen malware (virussen, trojans, spam, etc.) op de infrastructuur.

15. Er is een data-backup policy die gedefinieerd is in dienstenniveauovereenkomsten (dno's).

16. Backup-media met een bewaartermijn langer dan 1 jaar worden tenminste éénmaal per jaar gecontroleerd op leesbaarheid. Bij twijfel over de kwaliteit van de media wordt deze gedupliceerd teneinde een kopie van goede kwaliteit te verkrijgen.

17. Tenminste de maand-backups worden off-site opgeslagen. Overige backups worden bewaard in een ruimte die zich niet in de nabijheid van de computerruimte(n) bevindt.

18. Wanneer vertrouwelijke gegevens worden uitgewisseld tussen twee systemen waarbij van een verbinding gebruik wordt gemaakt die geen eigendom is van de Universiteit, dienen deze gegevens versleuteld te worden verstuurd.

19. Wijzigingen aan IT-systemen worden conform ITIL gepland en goedgekeurd middels een change-procedure.

Toegangsbeveiliging

20. Er zijn formele procedures voor het registreren en afmelden van gebruikers vastgesteld, voor het verlenen en intrekken van toegangsrechten tot alle informatiesystemen en –diensten.

21. Anderen dan medewerkers van de betrokken ICT-afdeling mogen slechts toegang hebben tot serverruimten onder begeleiding van een medewerker van die ICT afdeling.

22. Alle standaard wachtwoorden moeten op alle systemen worden vervangen door niet-standaard wachtwoorden. Wachtwoorden worden eenzijdig versleuteld opgeslagen in een systeem.

23. Netwerken dienen beveiligd te zijn tegen ongeautoriseerde toegang.

24. Een wachtwoord bestaat uit minimaal 8 en maximaal 13 posities waarvan minimaal 1 kleine letter, 1 hoofdletter en 1 cijfer en is maximaal 182 dagen geldig. Er vindt momenteel een wijziging plaats van dit onderdeel in een nieuw beleid. Zodra de wijziging is vastgesteld wordt deze tekst vervangen.

25. Bij de inlogprocedure dient altijd gebruik te worden gemaakt van versleutelde netwerk-protocollen (https, imaps, pop3s).

26. Gebruikers nemen goede beveiligingsgewoontes in acht zoals het niet opschrijven van wachtwoorden, het nooit delen van het wachtwoord met anderen, het wijzigen van het wachtwoord indien het vermoeden bestaat dat het bekend is geworden aan een derde en het vergrendelen van de werkplek tijdens afwezigheid.

27. Er is een beleid met betrekking tot het gebruik van netwerken en netwerkdiensten. Gebruikers krijgen slechts toegang tot de netwerkdiensten die voor het werk noodzakelijk zijn.

28. BYOD (cq. privé) apparaten krijgen enkel toegang via speciaal daarvoor ingerichte beveiligde koppelvlakken.

29. Indien door de systeemeigenaar remote toegang wordt verleend tot (kritische) toepassingen dan vindt deze plaats voor (functionele) beheerders op basis van twee-factor authenticatie.

30. Mobiele apparaten van medewerkers (zoals een handheld computer, tablet, smartphone of laptop) waarop bedrijfsinformatie wordt opgeslagen zijn voorzien van een wachtwoord, versleuteling en anti-malware. Waar mogelijk wordt dit technisch afgedwongen. De ontsluiting van bedrijfsinformatie op mobiele apparatuur vindt - waar mogelijk - plaats op basis van zero footprint (wel online toegang; geen gegevens op het apparaat). Voor het geval dat zero footprint (nog) niet realiseerbaar is of functioneel onwenselijk is, geldt dat de gegevens versleuteld worden opgeslagen. Bij verlies of diefstal dienen de betreffende wachtwoorden onmiddellijk te worden gewijzigd.

Ontwikkeling en onderhoud van systemen

31. Alle informatiesystemen hebben een eigenaar, functioneel beheerder en een technisch beheerder.

32. Vóór invoering van een nieuw informatiesysteem wordt, middels een risicoanalyse, bepaald in welke risicocategorie de informatie die dit systeem verwerkt valt en wat de invloed van dit nieuwe systeem is op de bestaande omgeving. Hiervoor geldt de methodiek en de drie categorieën ‘basis risico’, ‘verhoogd risico’ en ‘hoog risico’.

33. Voor systemen die in de categorie ‘basis risico’ vallen volstaan de minimale maatregelen. Voor systemen die in de categorie ‘verhoogd risico’ en “hoog risico” vallen wordt een aanvullende risicoanalyse uitgevoerd die kan resulteren in aanvullende maatregelen.

34. Een informatiesysteem wordt pas onderdeel van de operationele IT omgeving na een formele goedkeuring en acceptatie van de systeemeigenaar en de ICT-afdeling.

35. Voor alle onderdelen in de totale informatievoorziening is een procedure ingericht die zorg draagt voor het tijdig en correct aanbrengen van veiligheidsupdates op systemen. Kritische patches (zo geclassificeerd door de softwareleverancier zoals Microsoft, Oracle (incl. SUN) etc.) dienen tenminste maandelijks te worden geïnstalleerd. Niet-kritische beveiligingspatches dienen tenminste driemaandelijks te worden geïnstalleerd.

36. De logfiles van alle werkplek-, server- en netwerksystemen worden op een centraal punt verzameld, en periodiek geautomatiseerd nagelopen op onregelmatigheden. Onregelmatigheden die geen duidelijke (onschuldige) verklaring kennen, worden als security incident aangemerkt, geregistreerd en onderzocht. Alle klokken op het netwerk moeten hierbij gelijk lopen vanwege het feit dat de timestamps (logboeken) met elkaar te vergelijken zijn.

37. Security incidenten worden geregistreerd in een systeem. Op verzoek kan er een rapportage worden gemaakt die een overzicht geeft van de security incidenten.

38. Voor de afhandeling van deze security incidenten is een verantwoordelijke aangewezen.

39. Er is een calamiteitenplan waarin activiteiten zoals het tegengaan van onderbreking van bedrijfsactiviteiten en bescherming van kritische bedrijfsprocessen tegen de gevolgen van omvangrijke storingen in informatiesystemen of rampen en om tijdig herstel te bewerkstelligen, worden beschreven.

Controle en naleving

40. Periodiek, tenminste één keer per jaar, wordt de gehele ICT (netwerk) omgeving door het ISSC gescand op aanwezigheid van zwakke plekken m.b.v. een vulnerabilityscanner. De security manager wordt van de resultaten in kennis gesteld.

41. De systeemeigenaar of de security manager kan – in overleg met het ISSC – penetratietesten laten uitvoeren op de gehele ICT (netwerk) omgeving.