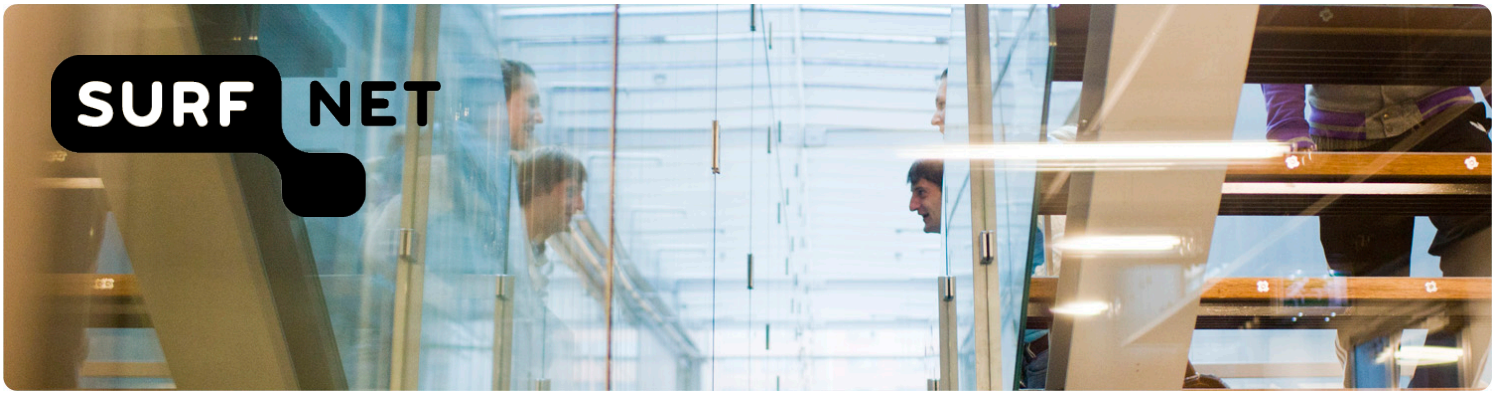

Leidraad Informatiebeveiligingsbeleid XX

Toelichting bij het gebruik van 'Informatiebeveiligingsbeleid XX'

Auteur(s): SCIPR (SURFibo)

Versie: 2.0

Datum: 1 mei 2015

Moreelsepark 48
3511 EP Utrecht

Postbus 19035
3501 DA Utrecht

088 - 787 30 00
admin@surfnet.nl
www.surfnet.nl

ING Bank NL54INGB0005936709
KvK Utrecht 30090777
BTW NL 0089.60.173.B01

Inhoudsopgave

SURF Community voor Informatiebeveiliging en PRivacy, voorheen SURFibo) is een Community of Practice met als doelen het actief stimuleren van en richting geven aan informatiebeveiliging en privacy binnen het hoger onderwijs (universiteiten, hogescholen, onderzoeksinstellingen en universitair medische centra). Dit doet SCIPR onder andere door het leveren van praktisch bruikbare adviezen, beleid en leidraden.

Meer informatie over SURFibo staat op www.surf.nl onder het thema 'Beveiliging en Privacy'.

1 Inleiding

1.1 Aanleiding

De Leidraad Informatiebeveiligingsbeleid XX, bestaande uit het Informatiebeveiligingsbeleid XX en de onderhavige toelichting, die in 2010 zijn opgenomen in het “Framework Informatiebeveiliging Hoger Onderwijs”, zijn toe aan een review. De belangrijkste redenen hiervoor zijn:

1. Gewijzigde wet- en regelgeving;

2. De opkomst van nieuwe technologieën, zoals de *cloud*, *Bring Your Own Device*, e.d., en

3. De professionalisering van het vakgebied.

1.2 Doelstelling

SURibo wil met deze leidraad en het modelbeveiligingsbeleid een handvat bieden aan degenen die, binnen een instelling voor hoger onderwijs, een informatiebeveiligingsbeleid willen ontwikkelen of verbeteren. Doel is het beschrijven van een *good practice* voor informatie-beveiligingsbeleid in het Hoger Onderwijs. Daarmee is het model en deze leidraad geen dwingend voorschrift.

Lokale organisatie en/of afwijkende werkwijzen kunnen er toe leiden dat het modelbeleid deels herschreven moet worden om aan de lokaal geldende normen te voldoen.

1.3 Doelgroep

De leidraad en het model beveiligingsbeleid zijn in eerste instantie bestemd voor degenen binnen een instelling die gemandateerd zijn om het informatiebeveiligingsbeleid te formuleren en te onderhouden. Uiteindelijk is het bestuur verantwoordelijk voor de vaststelling van het beleid. De *Information Security Officer* zal daarbij een belangrijke adviserende en voorbereidende rol hebben.

In tweede instantie vormt de leidraad een hulpmiddel om te komen tot concrete invulling van het informatiebeveiligingsbeleid. De informatiebeveiligingsorganisatie vindt een kant en klaar sjabloon voor de formulering van het instellingsbeleid, dat eenvoudig overgenomen kan worden.

1.4 Afbakening

Het informatiebeveiligingsbeleid, met daarin ook de beschrijving van de informatiebeveiligingsorganisatie, vormt in feite de basis voor informatiebeveiliging. Daarnaast wordt doorgaans aandacht besteed aan risicoanalyse en de selectie van basismaatregelen, classificatie van informatie en diverse gedragscodes. Deze vormen een verbijzondering van en aanvulling op het beleidsdocument. Waar mogelijk wordt verwezen naar dit soort documenten.

1.5 Verantwoording

SURFibo heeft de instellingen in het hoger onderwijs aangeschreven met het verzoek hun beleidsdocumenten ter beschikking te stellen als input voor de review van de Leidraad. Tevens is gebruik gemaakt van een aantal documenten op het gebied van informatiebeveiliging, zoals de Code voor Informatiebeveiliging (ISO/IEC 27001 en 2) en het Normenkader Informatiebeveiliging Hoger Onderwijs.

Op basis van de analyse van deze documenten heeft een aantal interviews plaatsgevonden, waarin geïnventariseerd is welke wijzigingen de instellingen hadden aangebracht ten opzichte van de leidraad uit 2010, alsmede welke wensen er leefden voor verdere verbetering van de leidraad.

De resultaten van deze interviews zijn gepresenteerd in een workshop Informatiebeveiligingsbeleid in het SURFibo-beraad van begin december 2013. De nu voorliggende versie is het resultaat van die workshop. Deze is *gereviewd* door een kleine begeleidingsgroep en is aan SURFibo aangeboden ter vaststelling.

2 Werkwijze: hoe gebruikt u de Leidraad Informatiebeveiligingsbeleid XX

Het Informatiebeveiligingsbeleid XX is het eenvoudigst toe te passen door “XX” overal te vervangen door de naam van de eigen instelling en door de generieke rollen die in het beleid zijn benoemd in appendix A te vertalen naar de voor uw instelling geldende rollen/namen: daar kunnen desgewenst ook meerdere rollen aan één functionaris gegund worden.

(Natuurlijk is het ook mogelijk om deze vertaalslag direct in het beleid zelf te doen en Annex A leeg te laten, maar het nadeel daarvan is dat versiemanagement lastig is wanneer het informatiebeveiligingsbeleid XX in de nabije toekomst weer verbeterd wordt: met de lokale vertaalslag in Annex A is dat eenvoudiger.)

Er worden generieke termen gebruikt, zoals bijvoorbeeld “bestuur”. De mapping van deze generieke termen op de eigen termen zal per instelling verschillen.

Overal waar “hij”, “hem” of “zijn” staat geschreven mag dit worden opgevat als “zij/hij”, “haar/hem” of “haar/zijn”.

Engelse termen die nog geen gemeengoed zijn in het Nederlands worden – net als in deze toelichting – cursief weergegeven.

SURFibo realiseert zich dat er bij individuele instellingen meer aanpassingen nodig kunnen zijn, bijvoorbeeld omdat het eigen beleid minder strikt geformuleerd is of andere accenten kent.

Het invullen van een CSIRT is ook zo’n *best practice*. Een instelling hoeft geen eigen CSIRT te hebben, maar dient wel de afhandeling van *security* incidenten geregeld te hebben, en een duidelijk aanspreekpunt voor *security* incidenten, zowel intern als extern. Het afhandelen van *security* incidenten zou ook in samenwerking met andere partijen opgezet of ingekocht kunnen worden.

De Leidraad Informatiebeveiligingsbeleid XX en het model beveiligingsbeleid staan niet op zichzelf. In het “Framework Informatiebeveiliging Hoger Onderwijs” zijn op dit moment een aantal documenten beschikbaar waaronder :

4. Starterkit Informatiebeveiliging
5. Starterkit Business Continuity Management
6. Starterkit Identity Management
7. Starterkit RBAC
8. Starterkit CERT-vorming (CSIRT)
9. Leidraad Classificatie
10. Leidraad voor het opstellen van een *Acceptable Use Policy*

11. Leidraad integriteitscode
12. Leidraad Functieprofiel
13. Leidraad Informatiebeveiligingsarchitectuur
14. Leidraad Veilig toetsen
15. *Baseline* Informatiebeveiliging
16. Cloud Normenkader
17. Normenkader Informatiebeveiliging HO / SURFaudit

Zie voor het actuele overzicht van het Framework en alle documenten
https://www.edugroepen.nl/sites/SURFibo

3 Gebruikte documenten

Bij de review van de Leidraad uit 2010 is gebruik gemaakt van de volgende documenten.

Nr.	Instelling	Titel	Versie, datum
1	Fontys Hogescholen	Informatiebeveiligingsbeleid Fontys Hogescholen	Versie 1.0, mei 2013
2	Hogeschool Inholland	Informatiebeveiligingsnorm Hogeschool Inholland	Versie 1.3, 1 oktober 2013
3	Universiteit Twente	Informatiebeveiligingsbeleid Universiteit Twente	21 september 2011
4	Universiteit Leiden	Beleid informatiebeveiliging voor onderwijs, onderzoek en bedrijfsvoering bij de Universiteit Leiden	Versie 0.6, 4 november 2013
5	Universiteit Maastricht	Informatiebeveiligingsbeleid UM	Versie 2.1, 17-06-2013
6	Hanzehogeschool	Informatiebeveiligingsbeleid Hanzehogeschool 2010-2014	Versie 3.0, maart 2010
7	NEN	NEN-ISO/IEC 27001	2005 en 2013
8	NEN	NEN-ISO/IEC 27002	2005 en 2013
9	SURF	Normenkader SURF-audit	2011

4 Interviews

De volgende personen zijn geïnterviewd t.b.v. de review van het modelbeleid.

Nr.	Instelling	Geïnterviewde	Datum
1	Fontys Hogescholen	Jeroen de Schipper	25-11-2013
2	Universiteit Maastricht	Bart van den Heuvel	25-11-2013
3	Hanzehogeschool	Elma Middel	02-12-2013
4	Universiteit Twente	Wim Koolhoven, Peter Peters en Marc Berenschot	02-12-2013
5	Universiteit Utrecht	René Ritzen	Eindredactie 1 mei 2015

5 Begeleidingsgroep

De volgende personen zullen het concept van het herziene modelbeleid en leidraad beoordelen:

Nr.	Instelling	Persoon
1	Hogeschool Windesheim	Anita Polderdijk
2	Universiteit Utrecht	René Ritzen
3	Erasmus Universiteit	Peter Oost
4	Universiteit van Amsterdam	Bart Visser
5	Hogeschool Arnhem Nijmegen	Stefan Arts
6	Radboud Universiteit	Jean Popma