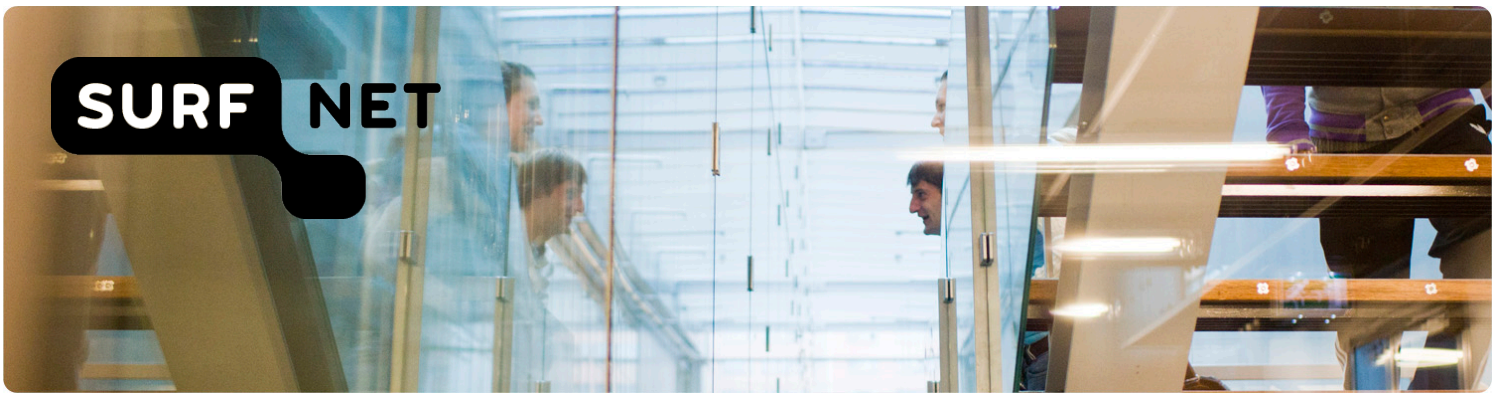

Informatiebeveiligingsbeleid XX

(Model beveiligingsbeleid uit het Framework Informatiebeveiliging Hoger Onderwijs)

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 SCIPR staat op www.surf.nl onder het thema ‘Beveiliging en Privacy’.

Management Samenvatting

Informatie technologie (IT) en informatie management (IM) zijn niet meer weg te denken anno nu. Bijna alle processen zijn afhankelijk van een goede en ongestoorde werking van IM en IT. Dat geldt net zo zeer voor het primaire proces, alsook voor secundaire processen, en ondersteunende processen als financieel management of personeelszaken. Zonder werkende IT geen research, geen onderwijs, geen productie, geen facturering, geen uitbetaalde salarissen, geen werkende toegangscontrole, enzovoorts.

Daarom is evident dat het hoogste management zich verantwoordelijk moet weten voor IM en IT. Niemand anders dan het bestuur heeft die eindverantwoordelijkheid. Het bestuur is dan ook niet alleen verantwoordelijk voor de inrichting en de *governance* van IM en IT – maar ook voor de ongestoorde en veilige werking ervan. We hebben het dan over informatiebeveiliging of IB. Dit is het onderwerp van dit beleid.

IB is direct gerelateerd aan de missie en prioriteiten van de organisatie. De mate waarin aandacht besteed wordt aan IB is afgeleid van de business impact die inbreuken op de informatiebeveiliging kunnen veroorzaken: er ligt dus altijd een *business case* aan ten grondslag. Het middel van de risicoanalyse bestaat ervoor om een inschatting van de risico's en business cases te maken, om daar vervolgens een passende IB-structuur en -maatregelen op te kunnen baseren.

Informatiebeveiliging gaat over alle IT- en informatiemiddelen en –processen, waarbij met name 3 aspecten van belang zijn:

1. **Beschikbaarheid**: werken de middelen/processen, zijn ze "in de lucht"?

2. **Integriteit**: is de inhoud van de informatiestromen beveiligd, dat wil zeggen is het zeker dat er niet mee geknoeid is of kan worden?

3. **Vertrouwelijkheid**: hebben alleen die mensen toegang tot bepaalde informatie die daartoe gemachtigd zijn, en is het voor anderen ontoegankelijk c.q. onleesbaar?

Een aanvullend aspect dat voor alle 3 van belang is, is *controleerbaarheid*: niet alleen "weten" of iets in orde is, maar dat ook achteraf kunnen "verifiëren".

Ten overvloede: IB is géén primair of secundair proces, géén *core business*, maar als je er niets aan doet gaat het wel **ten koste van** de *core business*: IB is **dus** een *business enabler* van de eerste categorie. Het bestuur van de organisatie moet dan ook zorgen voor een goede *governance*, inclusief *auditing* en *feedback*. We noemen deze *I-governance*. Deze is cruciaal en management *commitment* is daarbij essentieel.

Dit IB beleid wordt daarom door het bestuur van XX vastgesteld en gedragen en geldt voor de gehele organisatie, en allen die daarbij betrokken zijn in wat voor functie dan ook.

Betrokkenheid van het bestuur is dus noodzakelijk, maar niet voldoende. IB is namelijk nadrukkelijk **ieders** verantwoordelijkheid binnen XX. Dit zal worden uitgedragen zowel langs formele weg, als via bewustwordingscampagnes. Een speciale plek is er daarbij voor het lijnmanagement: die hebben de taak om randvoorwaardelijk en curatief toe te zien op goede IB.

Kortom, informatiebeveiliging zal het best werken wanneer de **hele** organisatie participeert. Dit is een continu proces. Dit beleid is daarvoor het uitgangspunt. Beschreven worden niet alleen de voornoemde aspecten, maar ook welke rollen ingevuld moeten worden, hoe IB onderdeel is van de *Planning & Control* cyclus, hoe beveiligingsincidenten aangepakt worden (en hoe ze beter te voorkómen), welke wettelijke randvoorwaarden bestaan, enzovoorts.

Qua rolverdeling springen een aantal cruciale rollen eruit:

- De CISO, de *Corporate Information Security Officer* van XX: een rol op strategisch niveau. De CISO heeft direct toegang tot het bestuur en is zelf geen lijnverantwoordelijke. Zijn taak is te waken over IB, lastige vragen te stellen, auditing voor te bereiden en beleid en aanbevelingen te formuleren.

- (C)ISM's: *(Corporate) information security managers* die op tactisch (en operationeel) niveau opereren en daarmee de verbindende schakel vormen tussen het strategische niveau waarop de CISO opereert, en de dagelijkse inrichting en uitvoering van IB.

- CSIRT: het C*omputer Security Incident Response Team* van XX, de brandweer van de IB, die net als de "gewone" brandweer zowel preventief als curatief opereert.

1 Inleiding

1.1 Algemeen

Onder informatiebeveiliging wordt verstaan het treffen en onderhouden van een samenhangend pakket aan maatregelen om de kwaliteitsaspecten beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening te waarborgen.

De kwaliteitsaspecten:

- **Beschikbaarheid**: werken de middelen/processen, zijn ze “in de lucht”?
- **Integriteit**: is de inhoud van de informatiestromen beveiligd, dat wil zeggen is het zeker dat er niet mee geknoeid is of kan worden?
- **Vertrouwelijkheid**: hebben alleen die mensen toegang tot bepaalde informatie die daartoe gemachtigd zijn, en is het voor anderen ontoegankelijk c.q. onleesbaar?

Hierbij gaat het ook om de controleerbaarheid[1] van de maatregelen die genomen zijn om deze kwaliteitsaspecten te borgen.

Informatiebeveiliging is een beleidsverantwoordelijkheid van het bestuur van XX. Zoals overal in de maatschappij is ook bij XX sprake van toenemende afhankelijkheid van informatie en computersystemen, waardoor nieuwe kwetsbaarheden en risico’s kunnen optreden. Het is van belang hiertegen adequate maatregelen te nemen. Immers, onvoldoende informatiebeveiliging kan leiden tot onacceptabele risico’s voor het bedrijfsproces van XX. Incidenten en inbreuken in deze processen kunnen leiden tot financiële schade en imagoverlies.

Informatiebeveiliging zelf is géén primair of secundair proces, géén *core business*, maar als je er niets aan doet gaat het wel **ten koste van** de *core business*: informatiebeveiliging is een *business enabler* van de eerste categorie.

XX heeft de ambitie om met het onderhavige beleidsdocument informatiebeveiliging structureel naar een hoog niveau te brengen en daar te houden door de aspecten *governance* (inclusief *auditing* en *feedback*), wet- en regelgeving, de organisatie van de beveiligingsfunctie en het informatie-beveiligingsbeleid – ook in hun onderlinge relatie – duidelijk te beschrijven en vast te stellen.

[1] Controleerbaarheid: de mate waarin het mogelijk is om achteraf parameters die van belang zijn voor beschikbaarheid, integriteit of vertrouwelijkheid te verifiëren. Zulke parameters zijn bijvoorbeeld *downtime*, toegang en transacties.

1.2 Doelgroep

Het informatiebeveiligingsbeleid bij XX **richt zich primair op** bestuur en hoger management, de beveiligingsorganisatie en leidinggevenden. Het **is van toepassing op** alle medewerkers, docenten, studenten, bestuurders, gasten, bezoekers en externe relaties. Kortom, op iedereen die - intern dan wel extern - op enige manier te maken heeft met (aspecten van) het bedrijfsproces bij XX.

1.3 Reikwijdte van het beleid

In deze paragraaf wordt beschreven wat de afbakening is van het toepassingsgebied van dit beleid.

Bij XX wordt informatiebeveiliging breed geïnterpreteerd en betreft dus alle vormen van informatie, niet alleen digitale informatie. Er bestaat een belangrijke relatie en een gedeeltelijke overlap met risico's zoals *safety*[2] (ARBO wetgeving), fysieke beveiliging en *business continuity*. Op strategisch niveau wordt aandacht geschonken aan deze raakvlakken en wordt zowel planmatig als inhoudelijk afstemming gezocht.

Nadrukkelijk zij vermeld dat er een trend is in de richting van "integrale veiligheid", waarin o.a. *safety* en informatiebeveiliging zijn begrepen. Deze trend is toe te juichen, omdat alle aspecten van beveiliging dan benaderd kunnen worden vanuit een overkoepelende risicoanalyse. Echter wordt informatiebeveiliging in de regel nog als apart onderdeel behandeld, waar dit beleid bij aansluit. Evenwel is dit beleid naadloos in een overkoepelend beleid voor integrale veiligheid in te passen, zodra deze ontwikkeling zich voordoet binnen XX.

Het informatiebeveiligingsbeleid binnen XX heeft betrekking op alle medewerkers, studenten, gasten, bezoekers en externe relaties, alsmede op alle instellingsonderdelen en dienstverlening. Tevens vallen onder het informatiebeveiligingsbeleid in beginsel alle door XX beheerde *devices*[3] van waaraf geautoriseerde[4] toegang tot (diensten van) het XX netwerk verkregen kan worden. Ondanks dat XX geen verantwoordelijkheid draagt ten aanzien van de onbeheerde *devices* valt het gebruik hiervan op het XX netwerk in combinatie met ICT-faciliteiten van XX ook onder dit informatiebeveiligingsbeleid.

Bij het informatiebeveiligingsbeleid ligt de nadruk op die toepassingen die vallen onder de verantwoordelijkheid van XX. Dit heeft zowel betrekking op gecontroleerde informatie, die door XX zelf is gegenereerd en wordt beheerd, als ook op niet-gecontroleerde informatie, bijv. uitspraken van medewerkers in discussies op elektronische platforms van XX, persoonlijke websites of *pages* op publieke fora, waarop XX kan worden aangesproken.

---

[2] *Safety* wordt als verzamelterm gebruikt voor de verschillende aspecten van personele veiligheid: Arbo en milieu, sociale veiligheid, bedrijfshulpverlening e.d.

[3] Alle *devices* met potentiële netwerktoegang: servers, werkstations, laptops, maar ook alle mobiele *devices* inclusief *smartphones*, *tablets* e.d.

[4] Ongeautoriseerde toegang is per definitie een beveiligingsincident – hiervoor geldt dat dit door de CSIRT functie van XX afgehandeld wordt, zodra het incident bekend is.

2 Doelstelling

Als *mission statement* geldt:

Het informatiebeveiligingsbeleid bij XX heeft als doel het waarborgen van de continuïteit van het bedrijfsproces[5] en het minimaliseren van de schade door het voorkómen van beveiligingsincidenten en het minimaliseren van eventuele gevolgen van deze incidenten.

Daarmee is informatiebeveiligingsbeleid direct ondersteunend voor de missie en het proces van de instelling als geheel. De eindverantwoordelijkheid ligt derhalve bij het bestuur van XX.

Uit dit *mission statement* komen de volgende afgeleide doelstellingen voort:

- Kader: het beleid biedt een kader om (toekomstige) maatregelen in de informatiebeveiliging te toetsen aan een vastgestelde best practice (of norm) en om de taken, bevoegdheden en verantwoordelijkheden in de instelling te beleggen.

- Normen: de basis voor de inrichting van het XX informatiebeveiligingsmanagement is dit beleidsdocument, waarvoor ISO 27001 (zie 7. Referenties) als inspiratie diende. Formele certificering conform ISO 27001 wordt voor XX niet als noodzakelijk gezien, inrichting van een goed ISMS[6] echter wel – dit beleid is daarvoor de basis.

- Maatregelen: maatregelen worden genomen op basis van *best practices* in de SURF doelgroep, waarbij het op ISO 27002 gebaseerde *Baseline Informatiebeveiliging* en het *Normenkader SURFaudit*[7] als uitgangspunt wordt genomen.

- Expliciet vastgestelde beveiligingsorganisatie: uitgangspunten en organisatie van informatiebeveiligingsfuncties zijn vastgelegd en worden gedragen door het bestuur, en afgeleid daarvan, door de hele instelling.

- Daadkrachtige procesbenadering: duidelijke keuzes in maatregelen, actieve controle op beleidsmaatregelen en de uitvoering daarvan.

- *Compliance*: het beleid biedt de basis om te voldoen aan wettelijke voorschriften.

---

[5] Onderwijs en onderzoek worden nadrukkelijk als onderdelen van het bedrijfsproces gezien.

[6] ISMS: Information Security Management System.

[7] Voor documenten zie www.surf.nl onder het thema Beveiliging en Privacy, informatiebeveiliging; volledige versies te verkrijgen via SURFibo lidmaatschap,

3 Beleidsprincipes informatiebeveiliging

3.1 Beleidsuitgangspunten en principes

Informatiebeveiligingsmanagement wordt als proces ingericht. XX kiest ervoor om de jaarlijkse planning en controlecyclus te baseren op “Plan, Do, Check, Act” (zie nevenstaande figuur). Hierin worden jaarlijks planningen gemaakt en uitgevoerd. De resultaten ervan worden geëvalueerd en vertaald naar nieuwe jaarplanningen. Deze planningen zullen als regel op strategisch niveau te vinden zijn in de XX planning, en meer in detail in de IT jaarplannen. In bijlage D worden de belangrijkste stappen van de inrichting van een ISMS geduid.

De beleidsuitgangspunten bij XX zijn:

- XX is pleitbezorger van goede beveiliging en privacy en de bijbehorende bewustwording.
- XX is een instelling met een open karakter. Adequate beveiliging is daarbij wel een randvoorwaarde. Er wordt van medewerkers, studenten en derden verwacht dat ze zich qua techniek en ook qua houding ‘fatsoenlijk’ gedragen (eigen verantwoordelijkheid). Niet acceptabel is dat door al dan niet opzettelijk gedrag onveilige situaties ontstaan die leiden tot schade en/of imagoverlies. Het is om deze reden dat er gedragscodes zijn geformuleerd en geïmplementeerd.
- Het succes van beveiliging staat of valt met goede communicatie. Goede communicatie wordt daarom actief bevorderd, op en tussen alle niveaus in de instelling.
- De beveiliging dient de volgende aspecten te waarborgen:
- Beschikbaarheid
- Integriteit
- Vertrouwelijkheid.
- Bij elke IT-inrichting wordt ter bevordering van informatiebeveiliging en privacy het principe van *least privileges* gehanteerd, wat wil zeggen dat er naar wordt gestreefd om steeds niet meer dan die rechten te verlenen die nodig zijn voor adequate functie- en bedrijfsuitoefening.

XX hanteert de volgende beleidsprincipes:

- Informatiebeveiliging is ieders verantwoordelijkheid. Verwachtingen t.a.v. individuen: communiceer met medewerkers, studenten en derden dat er van hen verwacht wordt dat ze actief bijdragen aan de veiligheid van geautomatiseerde systemen en de daarin opgeslagen informatie. Dat gebeurt in de aanstellingsbrief, tijdens functioneringsgesprekken, met een gedragscode, met periodieke bewustwordingscampagnes, in contracten met tijdelijk personeel en leveranciers, enzovoorts. Het zo nodig opleggen van sancties na overtredingen maakt het geheel geloofwaardig.

- Informatiebeveiliging is een lijnverantwoordelijkheid: dat betekent dat de leidinggevenden de verantwoordelijkheid dragen voor een goede informatiebeveiliging in hun groep, afdeling, faculteit, divisie, enzovoorts. Dit omvat ook de keuze van maatregelen en de uitvoering en handhaving ervan binnen de gestelde kaders.

- Informatiebeveiliging is een procesverantwoordelijkheid: dat betekent dat de procesverantwoordelijken de primaire verantwoordelijk dragen voor een goede informatiebeveiliging van de informatie waarvoor zij verantwoordelijk zijn (bronprocessen/systemen zoals HR en SIS en afgeleide processen/systemen zoals de Elektronische Leer Omgeving. Dit omvat ook de keuze van maatregelen en de uitvoering en handhaving ervan.

- Informatiebeveiliging is een continu proces. Regelmatige herijking van beleid en audits: technologische en organisatorische ontwikkelingen binnen en buiten XX maken het noodzakelijk om periodiek te bezien of men nog wel op de juiste wijze bezig is de beveiliging te waarborgen. De audits maken het mogelijk het beleid en de genomen maatregelen te controleren op efficiency (controleerbaarheid).

- Eigendom van informatie: XX is in beginsel eigenaar van de informatie die onder haar verantwoordelijkheid wordt geproduceerd. Daarnaast beheert XX informatie, waarvan het intellectueel eigendom toebehoort aan derden. Medewerkers, studenten en derden dienen goed geïnformeerd te zijn over de regelgeving voor het (her)gebruik van deze informatie.

- Waardering van informatie: iedereen behoort de waarde van informatie te kennen en daarnaar te handelen. Deze waarde wordt bepaald door de schade als gevolg van verlies van beschikbaarheid, integriteit en vertrouwelijkheid. Classificatie kan hierbij behulpzaam zijn.

- XX streeft ernaar om alle gegevens en systemen waarop dit informatiebeveiligingsbeleid van toepassing is te classificeren. Daarbij wordt gekeken naar de aspecten beschikbaarheid, integriteit en vertrouwelijkheid. Voor elk van deze aspecten wordt een klein aantal klassen gedefinieerd. Het niveau van de beveiligingsmaatregelen is afhankelijk van deze klassen. De huidige stand van zaken qua classificatie is te vinden in Bijlage B – Classificatie.

- Bij elke mutatie, zoals infrastructurele wijzigingen, (IT)projecten of de aanschaf van nieuwe systemen wordt reeds in het vroegst mogelijke stadium rekening gehouden met informatiebeveiliging.

4 Wet- en regelgeving

Hoe XX omgaat met relevante wet- en regelgeving staat beschreven in Bijlage C – Wet- en regelgeving.

5 Governance informatiebeveiligingsbeleid

Het goed, efficiënt en verantwoord leiden van een instelling wordt vaak aangeduid met de term *governance*. Het omvat vooral ook de relatie met de belangrijkste belanghebbenden van XX, zoals de proceseigenaren, medewerkers, studenten, klanten en derden. Een goede *governance* zorgt er voor dat alle belanghebbenden hun rechten en plichten kennen.

In dit hoofdstuk worden diverse rollen onderscheiden. Het aantal rollen is als regel groter dan het aantal personen dat die rollen vervult. De huidige *mapping* voor XX van rollen op functies c.q. functionarissen is te vinden in Bijlage A – Mapping Informatiebeveiligingsbeleid op XX.

5.1 Afstemming met samenhangende Risico's

Onderdeel van *governance* is dat aan alle soorten risico's en hun onderlinge verwevenheid passende aandacht geschonken wordt. Het is om die reden dat bij XX op strategisch niveau zowel aandacht geschonken wordt aan informatiebeveiliging, als aan *safety* (ARBO-veiligheid), fysieke beveiliging en *business continuity*. Immers, samenwerking op het gebied van deze risico's is een noodzakelijke voorwaarde voor goede *governance*. Dit wordt bevorderd door de planningscyclus voor deze gebieden zo veel mogelijk parallel te laten verlopen. Daardoor kan de gewenste kruisbestuiving optreden. Waar mogelijk en nodig wordt deze afstemming ook vertaald naar het tactische en operationele niveau. Zoals in 1.3. Reikwijdte van het beleid reeds opgemerkt bestaat er een trend richting "Integrale Veiligheid". Dit beleid, en o.a. ook *safety* kunnen daarin samen georganiseerd worden.

In dit hoofdstuk wordt verder ingegaan op de *governance* van de informatiehuishouding (verder *I-governance* te noemen) en de positionering van informatiebeveiliging daarin.

5.2 Inpassing in *I-governance*

In deze paragraaf wordt beschreven hoe informatiebeveiliging als onderdeel van *I-governance* is georganiseerd en wie waarvoor verantwoordelijk is. Van belang daarbij is om onderscheid te maken naar richtinggevend of strategisch, sturend of tactisch en uitvoerend niveau. Wat betreft de benaming van rollen wordt zoveel mogelijk aangesloten bij het PvIB.[8]

[8] Functies in de informatiebeveiliging. Platform voor Informatiebeveiliging (PvIB), 2006

De governance structuur samengevat in een tabel:

Niveau	Wat?	Wie?	Overleg	Documenten
Richtinggevend	**B**epalen IB strategie. **O**rganisatie t.b.v. IB inrichten. **IB** planning en control vaststellen. **B**usiness continuity management. **C**ommunicatie naar management en organisatie.	**bestuur**, i.h.b. de portefeuillehouder IB, op basis van advies CISO en directeur IT.	**bestuur** stelt vast. **S**trategisch IB overleg adviseert.	**IB** beleidsplan. **IB** *baselines* (basismaatregelen). ***B**usiness continuity plan*.
Sturend	**P**lanning & Control IB: voorbereiden normen en wijze van toetsen evalueren beleid en maatregelen begeleiding externe audits **C**ommunicatie naar proceseigenaren .	**P**roces eigenaren. **L**eidinggevenden. **C**ISO. **C**ISM.	**T**actisch IB overleg.	**R**isicoanalyses en audits inclusief SURFaudit. **J**aarplan en -verslag.
Uitvoerend	**I**mplementeren IB maatregelen. **R**egistreren en evalueren incidenten. **C**ommunicatie eindgebruikers.	**I**T i.s.m. proces eigenaren. **(C)I**SM. **CSIRT**.	**O**perationeel IB overleg. **CSIRT** overleg.	**SLA**'s (*security* paragraaf). **I**ncidentregistratie incl. evaluatie.

Op instellingsniveau is het bestuur juridisch gezien eindverantwoordelijk voor informatiebeveiliging. Deze verantwoordelijkheid wordt in de instelling verder belegd.

De *Corporate Information Security Officer* of CISO[9] is een rol op strategisch (en tactisch) niveau. Hij adviseert aan het bestuur. De CISO bewaakt de uniformiteit ten aanzien van informatiebeveiliging binnen de instelling en dient gevraagd zowel als ongevraagd het bestuur van advies[10]. (Een rol die op zich breder is dan *I-governance* maar die regelmatig door de *CISO* wordt uitgevoerd, is die van *Business Continuity* Manager (BCM) – eveneens een strategisch/tactische rol die tot doel heeft "*business continuity*" te bewaken en beter te beveiligen.)

De rol van *Corporate Information Security Manager* of CISM is vormgegeven op het stafniveau van XX. Deze vervult een rol bij de vertaling van de strategie naar tactische (en operationele) plannen. Dit doet hij samen met de CISO (vanwege de uniformiteit) en de proceseigenaren. Er is maar één CISO maar er kunnen decentraal meer *Information Security Managers* (ISM's) zijn.

Op operationeel niveau wordt overlegd met de functionele beheerders en relevante IT-functionarissen. Er wordt aandacht geschonken aan de implementatie van de informatiebeveiligingsmaatregelen.

De financiering van informatiebeveiliging wordt bij XX geregeld conform hieronder beschreven.

Algemene zaken, zoals het opstellen van een informatiebeveiligingsplan voor de instelling of een externe audit, worden uit de algemene middelen betaald. Algemene instellingsbrede bewustwordingscampagnes en trainingen worden eveneens uit deze middelen betaald.

De beveiliging van informatiesystemen, inclusief de kosten daarvan, zijn integraal onderdeel van verantwoord beheer van het betreffende informatiesysteem. Beveiligingskosten van werkplekken maken integraal onderdeel uit van de werkplekkosten. Voorlichting en training voor specifieke toepassingen of doelgroepen worden uit decentrale middelen betaald.

Hoe en waar de financiering ook geregeld is, de ervaring leert dat het **reserveren** van beveiligingsbudget bij het maken van jaarplannen essentieel is.

5.3 Documenten informatiebeveiliging

Voor informatiebeveiliging wordt bij XX dezelfde managementcyclus gevolgd, die ook voor andere onderwerpen geldt: visie/idee, beleid, analyse, plan implementatie, uitvoering, controles en evaluatie.

In het kader van informatiebeveiliging hanteert XX de volgende documenten:

1. Dit Informatiebeveiligingsbeleid:

Het Informatiebeveiligingsbeleid ligt ten grondslag aan de aanpak van informatiebeveiliging binnen XX. In het Informatiebeveiligingsbeleid worden de randvoorwaarden en uitgangspunten vastgelegd en wordt richting gegeven aan de vertaling van het beleid in concrete maatregelen. Om er voor te zorgen dat het beleid gedragen wordt binnen de instelling en die er ook naar handelt wordt het uitgedragen

---

[9] CISO staat voor "Corporate Information Security Officer" of "Chief Information Security Officer". Deze afkorting is internationaal te doen gebruikelijk en wordt daarom hier gehanteerd, ondanks dat we als volledige term voor "Information Security Officer" hebben gekozen.

[10] Bij overgang naar "Integrale Veiligheid" kan CISO vervangen worden door CSO of "Chief Security Officer" – die dan zowel over informatiebeveiliging, fysieke beveiliging en *safety* gaat.

door (of namens) het bestuur. Het informatiebeveiligingsbeleid wordt opgesteld door de CISO en vastgesteld door het bestuur.

2. Jaarplan/verslag:
   Elk jaar levert de CISO een jaarverslag en een jaarplan voor het volgende jaar in bij het bestuur. Het jaarplan is mede gebaseerd op de resultaten van de periodieke controles / audits. Er wordt o.a. ingegaan op incidenten, resultaten van risicoanalyses (incl. genomen maatregelen) en andere initiatieven die het afgelopen jaar hebben plaatsgevonden. Dergelijke verslagen kunnen geconsolideerd worden in de bestuurlijke Planning & Control-cyclus. Waar nodig wordt apart aandacht besteed aan specifieke systemen/applicaties.

3. Baseline van IT informatiebeveiligingsmaatregelen (basisniveau maatregelen):

Deze baseline beschrijft de maatregelen die minimaal nodig zijn om XX breed een minimaal niveau van informatiebeveiliging te kunnen waarborgen. Dit vloeit voort uit het beleid of uit besluiten die door het bestuur genomen zijn. Deze basis maatregelen dienen dus overal in de instelling genomen te worden. De baseline wordt gemaakt door de (C)ISM('s) in overleg met de CISO en goedgekeurd door het bestuur. Wanneer er systemen zijn die na een risicoanalyse hogere beveiligingseisen nodig hebben, dan worden aanvullende maatregelen genomen.

4. Policies:
   Gedragscodes en richtlijnen voor medewerkers, studenten en derden, al dan niet voor specifieke doelgroepen, op het gebied van informatiebeveiliging. Met name:

- Acceptable use policy, voor het veilig gebruik van IT-voorzieningen, e-mail en Internetgebruik;
- RFC-2350 voor de lokale CSIRT (zie hoofdstuk 6. Melding en afhandeling van incidenten (CSIRT));
- Richtlijn Privacy (zie paragraaf 5.6. Organisatie van de informatiebeveiligingsfunctie);
- Richtlijn Authenticatie;
- Richtlijn Autorisatie;
- Toepassing van cryptografische hulpmiddelen;
- Richtlijn classificatie
- Richtlijn responsible disclosure;
- IT Lifecycle management[11] ;
- Integriteits-/gedragscode voor ICT-functionarissen.

[11] Bijvoorbeeld: bij de aanschaf van hard/software dient beveiliging tijdens de hele *lifecycle* van aanbesteding, via testen en implementatie, en wijzigingsbeheer tot aan afvoer en vernietiging meegenomen te worden.

Daarnaast is informatiebeveiliging een vast onderdeel van de volgende documenten:

5. Business Continuity Plan:
   Business Continuity Management (BCM) is de benaming van het proces dat potentiële bedreigingen voor een instelling identificeert en bepaalt wat de impact op de “operatie” van de instelling is als deze bedreigingen daadwerkelijk manifest worden. Het product van BCM bestaat uit een samenhangend stelsel van maatregelen, die zowel preventief, detectief, correctief als repressief werkzaam zijn. Disaster Recovery is derhalve onderdeel van BCM. Het Business Continuity Plan wordt opgesteld op initiatief van de Business Continuity Manager, in samenwerking met het bestuur, de CISO, de proceseigenaren, het hoofd IT en het hoofd Facilitaire Zaken.

6. Diensten overeenkomsten (SLA’s), inhuur- en uitbestedingscontracten:

Bij de inhuur van personeel, maar ook bij de inkoop van middelen (met name hardware, software en applicatie/cloud platforms), wordt expliciet aandacht aan informatiebeveiliging besteed onder andere door dit beleid ook toe te passen op externen, en door beveiliging standaard onderdeel van de inkoopvoorwaarden te maken. Afspraken worden in een contract met de leverancier vastgelegd. In deze contracten zit standaard een informatiebeveiligingsparagraaf, waarin de verantwoordelijkheden van de leverancier zijn opgenomen. Als basis hiervoor dient het SURF Juridisch Normenkader Cloudservices Hoger Onderwijs[12].

5.4 Controle, naleving en sancties

Bij XX is de CISO verantwoordelijk voor de interne audits en voor de controle op de uitvoering van de informatiebeveiligingsjaarplannen. De CISM(‘s) ondersteunen daarbij.

Interne controles vinden jaarlijks plaats en hebben bij voorkeur een divers karakter (*brainstorms*, steekproeven, *penetration testing*, testen van *policies*, informatiebeveiliging/CSIRT *firedrills*).

De bedrijfskritische informatiesystemen van XX worden intern geaudit. Deze audits richten zich op de classificatie van de in het informatiesysteem vastgelegde gegevens, op de inventarisatie van de risico’s, op de genomen beveiligingsmaatregelen en op de samenhang tussen deze drie onderwerpen. Elk informatiesysteem wordt tenminste eens per twee jaar geaudit. Indien een informatiesysteem wordt vervangen of indien zich significante wijzigingen voordoen in de implementatie van de beveiliging wordt op dat moment een audit uitgevoerd.

De externe controle wordt in een cyclus van 4 jaar uitgevoerd door een onafhankelijke partij. Dit is qua tijdsplanning gekoppeld met het accountantsonderzoek en wordt zoveel mogelijk gecoördineerd met de normale *Planning & Control* cyclus.

[12] https://www.surf.nl/binaries/content/assets/surf/nl/kennisbank/2013/juridisch-normenkader-cloudservices-hoger-onderwijs.pdf

Het *Normenkader SURFaudit* wordt gebruikt als uitgangspunt voor interne en externe controles. Voor de audits van specifieke onderdelen of informatiesystemen kunnen aanvullende, meer gedetailleerde, normen worden vastgesteld.

De bevindingen van de interne en externe controles, evenals mogelijke externe eisen t.a.v. beveiliging, zijn input voor de nieuwe jaarplannen van XX. Deze kunnen ook tot wijziging van dit beleid leiden.

De naleving bestaat uit concreet toezicht op de dagelijkse praktijk van het informatiebeveiligingsmanagement proces. Van belang hierbij is dat leidinggevenden (inclusief onderwijsverantwoordelijken) de medewerkers en studenten aanspreken in geval van tekortkomingen. Voor de bevordering van de naleving van de Wbp is de “Functionaris Gegevensbescherming” (FG) verantwoordelijk.

Mocht de naleving ernstig tekort schieten, dan kan XX de betrokken verantwoordelijke medewerkers of studenten een sanctie opleggen, binnen de kaders van arbeids- en studieovereenkomsten en de wettelijke mogelijkheden. Dit is primair een verantwoordelijkheid van de verantwoordelijke leidinggevenden en het bestuur.

5.5 Bewustwording en training

Beleid en maatregelen zijn niet voldoende om risico’s op het terrein van informatiebeveiliging uit te sluiten. De mens zelf creëert de grootste risico’s. Daarom wordt bij XX het bewustzijn voortdurend aangescherpt, zodat kennis van risico’s wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd. Onderdeel van het beleid zijn regelmatig terugkerende bewustwordingscampagnes voor medewerkers, studenten, derden en met name operationele beheerders. Verhoging van het beveiligingsbewustzijn is zowel een verantwoordelijkheid van de leidinggevenden, als de CISO en de CISM(‘s); uiteindelijk is hiervoor het bestuur verantwoordelijk. Dit alles laat onverlet dat elke beveiliging faalt als deze niet gedragen wordt door de medewerkers – elke XX medewerker is mede verantwoordelijk voor goede beveiliging. Dit is een cruciaal onderdeel van bewustwording en wordt randvoorwaardelijk ondersteund in het personeelsbeleid.

5.6 Organisatie van de informatiebeveiligingsfunctie

Om informatiebeveiliging gestructureerd en gecoördineerd op te pakken worden bij XX een aantal rollen onderkend die aan functionarissen in de bestaande instelling zijn toegewezen. Zie Bijlage A – Mapping Informatiebeveiligingsbeleid op XX voor de huidige “mapping” van deze rollen binnen XX.

Bestuur

Het bestuur is verantwoordelijk voor de informatiebeveiliging binnen XX en stelt het beleid en de basis maatregelen op het gebied van informatiebeveiliging vast. Informatiebeveiliging komt zo vaak als nodig en minimaal 3x per jaar op de agenda van het bestuur. Het bestuur wijst één van haar leden aan als **portefeuillehouder informatiebeveiliging**.

De inhoudelijke verantwoordelijkheid voor informatiebeveiliging is door de portefeuillehouder gemandateerd aan de CISO[13]. Deze heeft de opdracht om op de informatiebeveiliging van de gehele instelling toe te zien.

Business Continuity Manager (BCM)

De BCM draagt zorg voor het definiëren, doen opzetten en controleren van processen die de continuïteit van de instelling(sprocessen) waarborgen. Deze functie is significant breder dan alleen IT beveiliging.

Corporate Information Security Officer (CISO)

De CISO is een rol op strategisch (en tactisch) niveau. Hij adviseert aan het bestuur. De CISO formuleert het beveiligingsbeleid, helpt bij een juiste vertaling daarvan naar instellingsonderdelen, ziet toe op de (uniforme) naleving ervan en rapporteert over lacunes, inconsistenties en onvolkomenheden. Hij heeft de bevoegdheid om onderzoek te doen of laten doen (audits) en informatie op te vragen en in principe ook te krijgen, tenzij privacy in het geding is – in alle bijzondere gevallen beslist het bestuur. De CISO kan zowel gevraagd als ongevraagd van advies dienen. Idealiter valt de CISO daarom ook direct onder het bestuur, en niet onder bijvoorbeeld de CIO of CFO – de belangen van de CIO of CFO kunnen namelijk soms in conflict zijn met die van de CISO.

(Corporate) Information Security Manager (C)ISM

De CISM vervult een rol bij de vertaling van de strategie naar tactische (en operationele) plannen. Dit doet hij samen met de CISO (vanwege de uniformiteit) en met de aren. Tevens adviseert de CISM over specifieke informatiebeveiligingsmaatregelen in projecten – variërend van allerhande staande projecten tot acquisities van bijvoorbeeld software of hardware. Er kunnen decentraal meer dan één functionarissen zijn met de rol Information Security Manager.

Proceseigenaar

Een proceseigenaar is iemand die verantwoordelijk is voor een van de primaire of ondersteunende processen, al dan niet gebruikmakend van meerdere systemen.

Systeemeigenaar

Een systeemeigenaar is iemand die verantwoordelijk is voor een belangrijk systeemplatform of applicatie, waarmee 1 of meerdere processen worden ondersteund.

Leidinggevende (inclusief onderwijsverantwoordelijken)

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

- er voor te zorgen dat hun medewerkers c.q. studenten op de hoogte zijn van (de voor hen relevante aspecten van) het beveiligingsbeleid;

[13] In die gevallen waar de CISO zelf bestuurslid is, kan deze niet tegelijk de portefeuillehouder zijn binnen het bestuur. De slager moet niet zijn eigen vlees keuren.

- toe te zien op de naleving van het beveiligingsbeleid door medewerkers en studenten;
- periodiek het onderwerp informatiebeveiliging onder de aandacht te brengen in werkoverleggen;
- als aanspreekpunt beschikbaar te zijn voor alle personeel gerelateerde informatiebeveiligingszaken.

De leidinggevende kan hierin ondersteund worden door de CISO.

Interne IT-auditor

De interne IT-auditor controleert jaarlijks het goed en betrouwbaar functioneren van de interne IT-organisatie. Dit omvat o.a.: de structuur en verantwoordelijkheden van die IT-organisatie, de hardware, de systeem software en -applicaties, het interne- en (indien aanwezig) externe netwerk, veiligheids- en calamiteiten systemen.

De interne auditor rapporteert aan de CIO[14] en de CISO.

Functionaris Gegevensbescherming (FG of Privacy Officer)

De FG houdt binnen XX toezicht op de toepassing en naleving van de Wbp. De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie in de instelling.

CSIRT-coördinator

De CSIRT-coördinator bij XX wordt benoemd door het bestuur op advies van de CISO. Hij is verantwoordelijk voor *information security incident management* binnen de instelling, en is in dat kader ook bevoegd het tijdelijk isoleren van computersystemen of netwerksegmenten te gelasten. De CSIRT-coördinator werkt voor het uitvoeren van deze taken samen met andere, formeel benoemde, CSIRT-leden.

5.7 Overleg

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

Op **strategisch** niveau wordt richtinggevend gesproken over *governance* en *compliance*, alsmede over doelen, scope en ambitie op het gebied van informatiebeveiliging. Dit gebeurt in het bestuur, geadviseerd door de CISO.

Op **tactisch** niveau wordt de strategie vertaald naar plannen, te hanteren normen, evaluatiemethoden, e.d. Deze plannen en instrumenten zijn sturend voor de uitvoering. Dit tactisch overleg wordt uitgevoerd door de CISO en (C)ISM('s) in overleg met betrokken functionarissen zoals de CSIRT-coördinator en proceseigenaren.

[14] Bij afwezigheid van een CIO aan de portefeuillehouder IT in het bestuur.

Op **operationeel** niveau worden de zaken besproken die het dagelijkse bedrijfsproces aangaan in de zin van uitvoering en implementatie.

Voor alle drie de typen overleg geldt dat het zoveel mogelijk ingepast moet worden in bestaande overlegvormen met hetzelfde karakter. Zo zal op strategisch niveau niet alleen over informatiebeveiliging gesproken worden, maar ook over andere risico's waarmee XX te maken kan krijgen, zoals bijvoorbeeld financieel, personeel en commercieel.

6 Melding en afhandeling van incidenten (CSIRT)

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

Het is van belang om te leren van incidenten. Incidentregistratie en periodieke rapportage over opgetreden incidenten horen thuis in een volwassen informatiebeveiligingsomgeving. XX maakt daartoe gebruik van een CSIRT-meldpunt en heeft bekend gemaakt hoe dat is te benaderen.

Elke medewerker, student en derde is zelf verantwoordelijk voor het signaleren en melden van incidenten en inbreuken op informatiebeveiliging. Incidenten en inbreuken dienen direct gemeld te worden aan het CSIRT-meldpunt.

De incidenten worden afgehandeld en worden in het relevante operationeel overleg besproken en, als bedrijfsproces, financiën of goede naam in gevaar zijn, ook in het bestuur. Bij constatering van verontrustende trends kan hierop meteen worden ingespeeld, bijvoorbeeld door het nemen van extra maatregelen of een bewustwordingscampagne.

Het doel van de CSIRT is het zo mogelijk voorkomen van informatiebeveiligingsincidenten en deze te bestrijden zo ze zich voordoen en daarmee de continuïteit van XX te ondersteunen en haar reputatie te beschermen. De CSIRT houdt zich ook bezig met beveiligingsincidenten buiten XX als daar eigen medewerkers in enige rol bij betrokken zijn. In zulke gevallen wordt in principe gebruik gemaakt van de diensten van SURFcert, die wereldwijd in verbinding staat met andere CSIRT’s.

De leden van de CSIRT zijn in die rol benoemd door het bestuur en opereren in haar opdracht.

De CSIRT stelt een *charter* op waarin doelgroep, opdracht, bevoegdheden, escalaties, werkwijze (inclusief omgang met vertrouwelijkheid) en samenstelling zijn uitgewerkt. Daarin wordt o.a. vastgesteld wordt dat de CSIRT voor XX als geheel werkzaam is en haar opdracht direct van het bestuur van XX krijgt. Tevens worden directe escalaties naar het bestuursniveau (via de CISO) vastgelegd, evenals directe contacten met de afdelingen c.q. personen die binnen XX zorg dragen voor contacten met de pers, en voor juridische kwesties.

De CSIRT is gerechtigd het tijdelijk isoleren van systeem/netwerkgebruikers, computersystemen of netwerksegmenten te gelasten ten einde haar taak uit te kunnen voeren.

7 Referenties

- HORA: Toolbox Hoger Onderwijs Referentie Architectuur

http://www.wikixl.nl/wiki/hora/index.php/Hoofdpagina

- ISO 27001 : NEN-ISO/IEC 27001:2013 nl

http://www.nen.nl/NEN-Shop/Norm/NENISOIEC-270012013-nl.htm

- ISO 27002 : NEN-ISO/IEC 27002:2013 nl

http://www.nen.nl/NEN-Shop/Norm/NENISOIEC-270022013-nl.htm

- Normenkader SURFaudit: http://www.surf.nl/diensten-en-producten/surfaudit/normenkader-surfaudit/index.html - volledige versie te verkrijgen via SCIPR lidmaatschap, https://www.surf.nl/over-surf/samenwerking/nationale-samenwerking/scipr/index.html

- RFC-2350

http://www.ietf.org/rfc/rfc2350.txt

8 Vaststelling & Wijziging

Het Informatiebeveiligingsbeleid beleid wordt jaarlijks geëvalueerd op initiatief van de CISO van XX.

Dit beleid, versie %versienummer% , is vastgesteld door het bestuur van XX op %datum%.

Bijlage A – Mapping Informatiebeveiligingsbeleid op XX

NOTA BENE : Dit model be leid is het eenvoudigst toe te passen door de generieke rollen die in het beleid zijn benoemd in deze bijlage te vertalen naar de voor uw instelling geldende rollen/namen: daarbij 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 deze bijlage leeg te laten – het nadeel daarvan is dat versie management lastiger is wanneer dit model beleid in de nabije toekomst weer verbeterd wordt: met de lokale vertaalslag in deze bijlage A is dat eenvoudiger.

Rollen uit Informatiebeveiligingsbeleid	**Gewenste Invulling**
bestuur	
Binnen bestuur: portefeuillehouder Informatiebeveiliging	
Business Continuity Manager = BCM	
Information Security Officer = CISO	
Information Security Manager = CISM	
Proceseigenaren	
Leidinggevenden	
Functionaris gegevensbescherming	
Interne IT-auditor	
CSIRT-coördinator	

Bijlage B – Classificatie

Bij XX zijn alle gegevens waarop dit informatiebeveiligingsbeleid van

toepassing is, geclassificeerd. Het niveau van de beveiligingsmaatregelen is afhankelijk van de klasse.

De classificatie van informatie is afhankelijk van de gegevens in het informatiesysteem en wordt bepaald op basis van risicoanalyses.

Daarbij zijn de volgende aspecten van belang:

B = Beschikbaarheid	Is de informatie/functie aanwezig/bruikbaar/leesbaar?
I = Integriteit	Is de informatie/functie betrouwbaar/compleet/onaangetast?
V = Vertrouwelijkheid	Hebben alleen rechthebbenden toegang tot de informatie/functie?

Hierbij gaat het ook om de controleerbaarheid[15] van de maatregelen die genomen zijn om deze kwaliteitsaspecten te borgen.

Ten aanzien van de beschikbaarheidseisen (B) worden de volgende klassen onderscheiden:

Classificatie B	**Definitie**
Niet vitaal (Laag)	• algeheel verlies of niet beschikbaar zijn van deze informatie gedurende langer dan 1 week brengt geen merkbare (meetbare) schade toe aan de belangen van XX, haar medewerkers of haar studenten of klanten
Vitaal (Middel)	• algeheel verlies of niet beschikbaar zijn van deze informatie gedurende langer dan 1 dag brengt merkbare schade toe aan de belangen van XX, haar medewerkers of haar studenten of klanten
Zeer vitaal (Hoog)	• algeheel verlies of niet beschikbaar zijn van deze informatie gedurende langer dan 1 uur brengt merkbare schade toe aan de belangen van XX, haar medewerkers of haar

[15] Controleerbaarheid: de mate waarin het mogelijk is om achteraf parameters die van belang zijn voor beschikbaarheid, integriteit of vertrouwelijkheid te verifiëren. Zulke parameters zijn bijvoorbeeld *downtime*, toegang en transacties.

	studenten of klanten

De tussen haken genoemde classificaties zijn alternatieven die soms elders worden gehanteerd.

Voor zowel vertrouwelijkheid (V) als integriteit (I) wordt de volgende indeling gevolgd: (NB: de classificering voor vertrouwelijkheid kan dus anders zijn dan voor integriteit, het is **geen** gecombineerde classificatie.)

Classificatie I of V	**Definitie**
Openbaar (Publiek) (Laag)	• Iedereen mag de gegevens inzien, bijvoorbeeld de algemene website van de instelling • Een geselecteerde groep mag deze gegevens wijzigen
Intern (Gevoelig) (Middel)	• Iedereen die aan de instelling is verbonden als medewerker of derde mag deze gegevens inzien; toegang kan zowel binnen als buiten de instelling (remote) worden verleend • Een geselecteerde groep mag deze gegevens wijzigen
Kritiek (Hoog)	• Er is expliciet aangegeven wie welke rechten heeft t.a.v. de raadpleging en de verwerking van deze gegevens,

De tussen haken genoemde classificaties zijn alternatieven die soms elders worden gehanteerd.

Ten aanzien van alle aspecten BIV kunnen in bijzondere gevallen, bijvoorbeeld als gevolg van externe eisen, zwaardere klassen worden vastgesteld door het bestuur. De CISO zorgt ervoor dat zulke bijzondere klassen als uitzondering worden aangemerkt en behandeld.

Bijlage C – Wet- en regelgeving

Bij XX wordt op de volgende wijze omgegaan met relevante wet- en regelgeving:

C.1. Wet Bescherming Persoonsgegevens (Wbp)

XX heeft de wettelijke *privacy* vereisten met betrekking tot beveiliging ingebed in dit beleid. Handelen conform dit beleid leidt in beginsel tot voldoen aan de beveiligingsvereisten uit de wet.

C.2. Wettelijke Bewaartermijnen

XX houdt zich aan de wettelijke voorschriften ten aanzien van bewaartermijnen, zoals die bijvoorbeeld in de Archiefwet zijn vastgelegd.

Dit betreft alle informatie zoals die bijvoorbeeld is vastgelegd in (gedigitaliseerde) documenten, informatiesystemen, websites, e-mail enzovoorts. Dit is onderdeel van de jaarlijkse externe accountantsrapportages.

C.3. Auteurswet

XX respecteert auteursrechten en handelt daarnaar.

C.4. Telecommunicatiewet

Omdat de doelgroep van XX voldoende afgebakend is worden de netwerkvoorzieningen van XX niet aangemerkt als een openbaar netwerk in de zin van de Telecommunicatiewet.

C.5. Wet Computercriminaliteit

De Wet Computercriminaliteit richt zich op de strafrechtelijke probleemgebieden in relatie tot het computergebruik. De wet bestaat uit artikelen die op diverse plekken zijn toegevoegd aan het WvS. De extra artikelen houden zich bezig met:

- Vernieling en onbruikbaar maken
- Aftappen van gegevens
- *Denial of service*, verstikkingsaanval
- Computervredebreuk
- Wat is computercriminaliteit
- Diensten afnemen zonder betalen
- Malware, kwaadaardige software

Evenwel zorgen het naleven van dit informatiebeveiligingsbeleid en het implementeren van basismaatregelen ervoor dat XX een basisniveau van beveiliging heeft. Indien er aanvallen op XX plaatsvinden die die beveiliging significant doorbreken en die vallen onder de Wet Computercriminaliteit, zal XX in beginsel aangifte doen. De CSIRT-coördinator en CISO adviseren hierover aan het bestuur – alleen het bestuur kan het besluit tot aangifte nemen.

Bijlage D: schematisch overzicht inrichting ISMS

Voor de inrichting van het ISMS zijn allerlei vereisten gesteld (voorbereidende fase):

- Begrip van de context van de organisatie: externe en interne omgeving;
- Begrip van de behoeften en verwachtingen van belanghebbende partijen;
- Een goede beschrijving van de scope van het ISMS: wat valt er onder en wat doet niet mee;
- Leiderschap en commitment, zonder welke informatiebeveiliging in een organisatie niet serieus genomen kan worden.

Vervolgens moet het ISMS gedefinieerd worden (Plan):

- Beleid;
- Scope;
- Bedrijfsmiddelen (Assets);
- Risico's en kansen;
- Middelen;
- Competenties;
- Bewustzijn;
- Communicatie;
- Gedocumenteerde informatie.

Bij de uitvoering van het ISMS (Do) gaat het om:

- de operationele planvorming en beheersing;
- risicobeoordeling(en);
- risicobehandeling.

De Check-fase omvat de evaluatie van de werking van het ISMS:

- bewaking, meting, analyse en evaluatie;
- interne audit;

- management review;

Op basis van de uitkomsten van de Check-fase worden verbeteringen doorgevoerd (Act). Door herhaling van deze cyclus zal de organisatie werken aan voortdurende verbeteringen van het ISMS en is de organisatie ‘in control’.