ROSA-katern

Kaders voor privacy en informatiebeveiliging in de onderwijsketen

Maart 2015, Versie 1.0

Inhoud

1. Inleiding

1.1 Aanleiding

In het onderwijsdomein wordt op allerlei manieren samengewerkt. Mede door deze steeds intensiever wordende ketensamenwerking verloopt de informatiehuishouding binnen het onderwijs meer en meer digitaal. In combinatie met aanscherpende wet- en regelgeving, een toenemend privacybewustzijn in de maatschappij, en de wil vanuit het onderwijs om de zaken goed te regelen leidt dat tot een groeiende behoefte om op een verantwoorde en betrouwbare wijze gegevens te gebruiken en uit te wisselen.

Wanneer de betrouwbaarheid van de informatievoorziening onvoldoende kan worden gewaarborgd, dan brengt dat risico's met zich mee op het gebied van informatiebeveiliging en privacybescherming. Publicaties in 2014 van SURF (Cyberdreigingsbeeld sector hoger onderwijs en wetenschappelijk onderzoek) en PWC (Nulmeting privacy beveiliging primair en voortgezet onderwijs) geven aan dat deze risico's voor alle onderwijssectoren in Nederland gelden. Weliswaar zijn sommige privacy- en informatiebeveiligingsrisico's sectorspecifiek, maar veel risico's gelden voor alle onderwijssectoren. Deze risico's kunnen leiden tot diverse vormen van schade of beschadiging:

Voor de sector:

- afnemend vertrouwen in verstrekte diploma's
- dalend vertrouwen in 'het onderwijs' door afstraling van privacy- en beveiligingsincidenten op een hele onderwijssector;

Voor de onderwijsinstelling:

- boetes wegens het overtreden van wet- en regelgeving;
- imagoschade, met als gevolg dalende leerlingaantallen en gederfde inkomsten;
- verstoorde onderwijs(logistieke) processen doordat gegevens niet kloppen of doordat processen niet goed verlopen;
- gederfde inkomsten door bekostiging op grond van onjuiste gegevens;
- extra administratieve lasten door verscherpt toezicht;
- extra administratieve lasten en/of boetes als gevolg van juridische geschillen.

Voor de onderwijsvolger:

- verlies aan zelfstandigheid, bijvoorbeeld door beperking van de mogelijkheid om handelingen uit te voeren: onder toezichtstelling, ouderlijke inmenging, uit-huis-plaatsing;
- stigmatisering, bijvoorbeeld op een bepaalde manier behandeld worden op basis van bepaalde kenmerken: dommerik, hulpbehoevend, beperkt, kampbewoner;
- ongelijke behandeling, bijvoorbeeld in verband met achtergrond of land van herkomst;
- beperking van bewegingsvrijheid, bijvoorbeeld beperkt worden in de toegang tot bepaalde gebieden, etablissementen of ruimtes op basis van gedragingen;
- ongewenst vindbaar zijn, bijvoorbeeld door uit de ouderlijke macht gezette ouders.

Om deze risico's af te dekken moeten onderwijsinstellingen met andere ketenpartijen dus samenhangende maatregelen nemen die zorgen voor veilig gebruik van - vaak privacygevoelige - gegevens. Het is daarom belangrijk dat er kennis gedeeld wordt en dat ketenpartijen samen optrekken om te werken aan een veiliger keten.

1.2 Doel

Vraagstukken rondom privacy en beveiliging beperken zich al lang niet meer tot individuele organisaties. Het onderwijs werkt in hoge mate in ketens, waarbij de veiligheid van de keten bepaald

wordt door de sterkte van de zwakste schakel. Het heeft geen zin om op één plaats in de keten hoge muren rond informatie op te werpen, als verderop in de keten niet hetzelfde niveau van privacybescherming en informatiebeveiliging wordt gehanteerd.

Om ketenbreed de beveiliging van informatie en de bescherming van privacy te waarborgen, moeten alle ketenpartijen zich daarom committeren aan een aantal kaders over hoe om te gaan met informatiebeveiliging en privacy.
Het katern Privacy en beveiliging biedt deze kaders op het gebied van privacy en beveiliging voor ict-voorzieningen die binnen het onderwijs gebruikt worden. Deze kaders zijn gebaseerd op generieke risico's die relevant zijn voor informatiebeveiliging in het onderwijsdomein.

1.3 Doelgroep

Het katern maakt onderdeel uit van de Referentiearchitectuur Onderwijs (ROSA), waarin ook andere architectuurkaders staan geformuleerd die betrekking hebben op *bovensectorale* gegevensuitwisseling binnen het onderwijs. Met bovensectoraal wordt gedoeld op de uitwisseling tussen onderwijssectoren onderling of de uitwisseling met DUO of andere gemeenschappelijke marktpartijen, zoals leveranciers van leerlingadministratiesystemen (LAS), uitgeverijen en distributeurs.

Met het katern hebben opdrachtgevers binnen de keten een instrument in handen om de juiste kaders te stellen aan de voorziening voor het veilige digitaal uitwisselen van gegevens binnen de onderwijsketen.

1.4 Opbouw

Risico's kunnen per type gegeven of proces verschillen. Daarom wordt in hoofdstuk 2 onderscheid gemaakt tussen een basisniveau en additionele kaders die betrekking hebben op specifieke processen of gegevens.
Voor de te nemen maatregelen zijn in hoofdstuk 3 verwijzingen naar toetsingskaders opgenomen voor zowel Verantwoordelijken (lees: onderwijsinstellingen) als Bewerkers (lees: leveranciers/uitgeverijen). Met behulp van de toetsingskaders kan worden vastgesteld of aan de benodigde beheersmaatregelen wordt voldaan.
Het katern bevat als bijlage ook een begrippenlijst, om het gebruik van dezelfde begrippen ten aanzien van privacy en informatiebeveiliging binnen het onderwijs te bevorderen.

1.5 Verantwoording

Het katern Privacy en beveiliging is opgesteld binnen het Samenwerkingsplatform Informatie Onderwijs (SION), in samenwerking met SURF, Studielink, saMBO-ICT,, Kennisnet, DUO en het ministerie van OCW. Het katern maakt onderdeel uit van de Referentiearchitectuur Onderwijs (ROSA). De inhoud van het katern is afgestemd met andere initiatieven binnen de keten, waaronder de werkgroep SURFibo in het hoger onderwijs en de taskforce informatiebeveiliging in het mbo.

1.6 Status

Het katern vormt evenals de overige onderdelen van de ROSA architectuur een streefbeeld voor de keten. Partijen streven ernaar om hieraan te voldoen en leggen uit waarom ze hier (nog) niet aan kunnen voldoen. De kaders zijn daarmee richtinggevend.

2. Gemeenschappelijke kaders

De kaders in dit hoofdstuk vormen het 'basisniveau privacy en beveiliging' voor het onderwijs. Een belangrijk onderdeel van de kaders omvat de wijze waarop we elkaar in het onderwijsdomein kunnen aanspreken op het voldoen aan het basisniveau. Daartoe zijn toetsingskaders beschikbaar, waarmee objectief kan worden vastgesteld op welk volwassenheidsniveau een organisatie (zoals een instelling, een leverancier, of een bewerker die namens de instelling optreedt) zich bevindt.

2.1 Basisniveau privacy en informatiebeveiliging

Het basisniveau omvat zaken op het gebied van privacy en beveiliging die hoe dan ook geregeld moeten zijn. De kaders in het basisniveau zijn dus in elke situatie binnen het onderwijs van toepassing en zijn gericht op:

- Informatiebeveiliging door ketenpartijen.
- Ketenbrede waarborging van vertrouwelijkheid en integriteit;
- Ketenbrede waarborging van beschikbaarheid in ketenprocessen;
- Ketenbrede waarborging van controleerbaarheid;
- Ketenbrede governance van privacy- en beveiligingsmaatregelen

Vertrouwelijkheid, integriteit en beschikbaarheid

In de opzet van het basisniveau wordt gerefereerd aan de termen 'vertrouwelijkheid', 'integriteit' en 'beschikbaarheid'. Dit zijn drie algemeen geaccepteerde aspecten van informatiebeveiliging die tezamen de betrouwbaarheid van de informatievoorziening bepalen. Zij worden als volgt gedefinieerd:

- **Vertrouwelijkheid** betreft het waarborgen dat informatie alleen toegankelijk is voor degenen die hiertoe zijn geautoriseerd. Met 'toegang hebben tot' wordt zowel het raadplegen als het muteren, toevoegen en/of vernietigen van informatie bedoeld.
- **Integriteit** betreft het waarborgen van de juistheid, volledigheid en tijdigheid van informatie. Informatie waarvoor de integriteit op orde is, is dus informatie die 'klopt'. Merk op dat een aantasting van vertrouwelijkheid (waardoor onbevoegden bijvoorbeeld mutaties kunnen doorvoeren) kan leiden tot een aantasting van integriteit.
- **Beschikbaarheid** betreft het waarborgen dat geautoriseerde gebruikers op de juiste momenten toegang hebben tot informatie en aanverwante bedrijfsmiddelen. Aantasting van beschikbaarheid kan bijvoorbeeld leiden tot aantasting van de continuïteit van bedrijfs- en/of ketenprocessen.

Voor elk van deze aspecten moet vastgesteld kunnen worden of er in voldoende mate invulling aan is gegeven. Een vierde aspect dat in dat verband van belang is, is dan ook het aspect van 'controleerbaarheid':

- **Controleerbaarheid** betreft het waarborgen dat vastgesteld kan worden dat in voldoende mate invulling is gegeven aan de aspecten vertrouwelijkheid, integriteit en beschikbaarheid. Daartoe moet kennis kunnen worden verkregen over de structurering en werking van de informatievoorziening.

Informatiebeveiliging en privacybescherming door individuele partijen in het onderwijsdomein

Van alle partijen in het onderwijsdomein mag worden verwacht dat zij serieus met informatiebeveiliging omgaan. Het volgende kader helpt ons bij de interne organisatie van onze informatiebeveiliging:

1. **Ketenpartijen conformeren zich - voor zover mogelijk - aan de 'Code voor informatiebeveiliging' (ISO 27001/27002)**
   ISO/IEC 27001/27002 is een internationale standaard die voorziet in eisen voor het vaststellen, implementeren, bijhouden en continu verbeteren van een managementsysteem voor informatiebeveiliging. Met behulp van beheersdoelstellingen wordt in deze standaard aangegeven wat er binnen een organisatie moet worden bereikt op het gebied van informatiebeveiliging. Voorbeelden van beheersdoelstellingen uit ISO zijn het hebben van een beveiligingsbeleid, het uitvoeren van risicoanalyses en het vaststellen van en handelen naar een

passend beschermingsniveau van informatie binnen de organisatie. De standaard biedt een reeks van beheersmaatregelen die kunnen worden toegepast om de beheersdoelstellingen te realiseren.
Voor het in het onderwijsdomein gewenste basisniveau gelden de beheersdoelstellingen uit ISO/IEC 27001/27002 onverkort als kaders voor informatiebeveiliging door individuele ketenpartijen. Een overzicht van deze doelstellingen is opgenomen in de Bijlage: Doelstellingen uit ISO/IEC 27001/27002.

Ketenbrede waarborging van vertrouwelijkheid en integriteit

We zijn als onderwijsketen gezamenlijk verantwoordelijk voor de vertrouwelijkheid en integriteit van informatie die door de keten heen gebruikt wordt. Eén zwakke schakel kan alle maatregelen elders in de keten teniet doen. De volgende kaders helpen ons om de vertrouwelijkheid en integriteit ketenbreed te waarborgen:

2. **Ketenpartijen voorkomen onrechtmatige toegang tot of verspreiding van gegevens**
   Gegevens worden zo opgeslagen en getransporteerd dat onrechtmatige toegang of verspreiding onmogelijk wordt gemaakt. Daarbij worden maatregelen genomen die passen bij de vertrouwelijkheidsclassificatie van die gegevens.
3. **Ketenpartijen voorkomen aantasting van de integriteit van gegevens**
   Gegevens worden zo opgeslagen en getransporteerd dat aantasting van de juistheid, volledigheid en/of tijdigheid onmogelijk worden gemaakt. Daarbij worden maatregelen genomen die passen bij de integriteitsclassificatie van die gegevens.
4. **Ketenpartijen zorgen dat handelingen herleidbaar zijn**
   Handelingen rondom gegevens zijn te herleiden naar personen.
5. **Ketenpartijen waarborgen de toewijzing van persoonsgebonden gegevens**
   In elk ketenproces zijn waarborgen geïmplementeerd waardoor binnen dat proces met voldoende mate vastgesteld en verzekerd kan worden dat persoonsgebonden gegevens aan de juiste persoon zijn toegewezen.
6. **Ketenpartijen voeren proactief technisch beheer uit**
   De in de onderwijsketen gebruikte systemen worden proactief technisch beheerd. Onderdeel van proactief technisch beheer is het bewust afwegen van risico's van het gebruik van verouderde software.
7. **Ketenpartijen gebruiken technieken voor veilig programmeren**
   De in de onderwijsketen gebruikte systemen, worden ontwikkeld met gebruikmaking van technieken voor veilig programmeren. De gebruikte technieken passen bij de benodigde vertrouwelijkheids- integriteits- en beschikbaarheidsniveaus.
8. **Ketenpartijen bewaren gegevens niet langer dan strikt noodzakelijk**
   Zodra het, vanuit het oogpunt van (keten)procesuitvoering, mogelijk is worden gegevens direct vernietigd. Wanneer gegevens in een andere (primaire) bron beschikbaar zijn, worden de gegevens in beginsel uit die bron geraadpleegd; het 'lokaal' opslaan van die gegevens wordt zo veel mogelijk vermeden. Daar waar de wet restricties of verplichtingen oplegt met betrekking tot bewaar- en archieftermijnen worden die gevolgd.
9. **Ketenpartijen voorkomen ongewenste traceerbaarheid en vindbaarheid van personen**
   In ontwerpen van processen en informatiesystemen wordt uitgegaan van het principe van 'privacy by design', en er is aandacht voor privacybevorderende voorzieningen zoals een nummervoorziening die het gebruik van pseudoniemen in de onderwijsketen mogelijk maakt. Persoonsgegevens worden slechts gebruikt indien dat strikt noodzakelijk is.

Ketenbrede waarborging van beschikbaarheid in ketenprocessen

In de uitvoering van ketenprocessen zijn we afhankelijk van andere partijen in de keten. De volgende kaders helpen ons om een tijdige en juiste uitvoering van een ketenproces te bewerkstelligen:

10. **Ketenpartijen zorgen ervoor dat de juiste gegevens op het juiste moment op de juiste plaats beschikbaar**
    De verschillende schakels in de keten zorgen ervoor dat de juiste gegevens op het juiste moment op de juiste plaats beschikbaar zijn.
11. **Ketenpartijen waarborgen de continuïteit van dienstverlening (ook bij calamiteiten)**
    Voor gegevens waarvoor onderling een kritieke tijdsafhankelijke relatie bestaat, worden maatregelen genomen die de continuïteit van de dienstverlening waarborgen.

Ketenbrede waarborging van controleerbaarheid

Als we in het onderwijs als een veilige en privacybewuste keten willen opereren, moeten we vast kunnen stellen of de maatregelen door de keten heen genomen zijn, afdoende zijn. De volgende kaders helpen ons om de benodigde controleerbaarheid te bewerkstelligen en bij het elkaar kunnen aanspreken op het naleven van de in het basisniveau opgenomen kaders:

12. **Ketenpartijen maken duidelijk welke eisen en verwachtingen ze van elkaar hebben**
    Ketenpartijen zijn open en transparant over onderlinge afhankelijkheden. Zij maken aan elkaar duidelijk:
    - de eisen en verwachtingen die zij hebben ten aanzien van procesuitvoering en informatievoorziening door andere ketenpartijen, en
    - de mate waarin zij zelf aan de verwachtingen en eisen van andere ketenpartijen kunnen voldoen

    Op basis hiervan worden afspraken gemaakt over ieders rol en taak. Ieder komt de bij zijn rol en taak behorende verplichtingen na, en is daarop aan te spreken.
    Dit maakt de betrouwbaarheid van de informatievoorziening in de onderwijsketen testbaar.
13. **Ketenpartijen zorgen voor voldoende meet- en controlepunten**
    Ketenpartijen monitoren, waar mogelijk geautomatiseerd, in welke mate voldaan wordt aan de privacy- en beveiligingskaders en de daaruit voortvloeiende afspraken. Zij delen de resultaten met andere partijen in de onderwijsketen.
    Dit maakt de betrouwbaarheid van de informatievoorziening in de onderwijsketen meetbaar;
14. **Ketenpartijen zijn transparant over de genomen privacy- en beveiligingsmaatregelen**
    Ketenpartijen bieden inzage in de normenkaders en beheersmaatregelen die zij toepassen, en bieden de mogelijkheid die toepassing te (laten) controleren.
    Dit maakt de betrouwbaarheid van de informatievoorziening in de onderwijsketen verifieerbaar.
15. **Ketenpartijen maken afspraken over de te realiseren ambitieniveaus en spreken elkaar daarop aan**
    De ambities met betrekking tot het te realiseren niveau van informatiebeveiliging kunnen in de tijd per onderwijssector of toepassingsgebied verschillen. Het afstemmen van de ambitie vindt binnen de verschillende onderwijssectoren plaats. Om betrouwbaar gegevens te kunnen uitwisselen en in ketens te kunnen samenwerken moeten partijen een vergelijkbaar ambitieniveau hebben.
    Waar mogelijk wordt met het realiseren van de ambities vaart gemaakt, zonder organisaties te overvragen. Er wordt nadrukkelijk rekening gehouden met de huidige stand van zaken, de mogelijke verbeterpunten en een groeipad naar een steeds hoger daadwerkelijk gerealiseerd niveau ten opzichte van de ambitie. Dit gerealiseerde ´volwassenheidsniveau´ kan worden vastgesteld middels toetsingskaders (zie ook Hoofdstuk 3).
    Die maakt de betrouwbaarheid van de informatievoorziening in de onderwijsketen valideerbaar.

Ketenbrede governance van privacy- en beveiligingsmaatregelen

Een ketenbrede aanpak van privacy- en beveiligingsvraagstukken vraagt om een ketenbrede sturing op de te nemen maatregelen. De volgende kaders helpen ons om, vanuit de verschillende onderwijssectoren, de te nemen maatregelen ter voorkoming van en in reactie op incidenten te harmoniseren:

16. **Ketenpartijen werken aan het opstellen en gebruik maken van sectorbrede frameworks en baselines**
    Er bestaan vooral sectorspecifiek nuances in dreigingsbeelden, risico's en realiseerbaarheid van beheersmaatregelen. Om een zekere harmonisatie van te nemen maatregelen te realiseren, wordt in ieder geval sectorbreed afstemming georganiseerd over de te gebruiken beveiligings- en privacyframeworks en -baselines.

17. **Ketenpartijen zorgen voor een goede incident response**
    Voorkomen is beter dan genezen. De privacy- en beveiligingskaders in dit katern richten zich daarom met name op het tegengaan van privacy- en beveiligingsincidenten. Toch kan zich altijd de situatie voordoen dat een plotseling incident leidt tot de noodzaak om snel in te grijpen, door de hele onderwijsketen heen. Zo'n situatie ontstaat bijvoorbeeld wanneer een serieus lek wordt gevonden in veelgebruikte (systeem)software. In zo'n geval moeten - afhankelijk van de schaal en reikwijdte van het incident - individuele partijen in het onderwijsdomein, volledige onderwijssectoren of het hele onderwijsdomein voorbereid zijn om op de juiste manier te kunnen reageren[1].

2.2 Additionele kaders

In aanvulling op het basisniveau gelden voor specifieke werkingsgebieden additionele kaders. Voor het ketenproces toetsen en examineren zijn deze kaders in de volgende paragraaf opgenomen. Voor andere ketenprocessen, op het vlak van bekostiging en online leren, zullen op basis van risicoanalyses in de toekomst soortgelijke aanvullingen worden opgesteld.

Toetsen en examineren

Naast de kaders uit het basisniveau, gelden op het gebied van privacy en beveiliging bij toetsen en examineren de volgende kaders:

1. Gegevens die gebruikt zijn bij de totstandkoming van het toetsresultaat kunnen in ieder geval niet eerder worden verwijderd dan na het verstrijken van de inzage- en beroepstermijn
2. De afnamerespons wordt onmiddellijk verwijderd na het verstrijken van de inzage- en beroepstermijn
3. De totstandkoming van het toetsresultaat is transparant en valideerbaar.
4. De identiteit van een kandidaat wordt voor de toetsafname vastgesteld
5. De toetslocatie is zo ingericht dat fraude wordt voorkomen

[1] Een best practice is om voor dit soort grootschalige, acute incidenten een zogenaamd 'emergency response team' in te richten. Zo'n CERT kan partijen in de keten actief benaderen wanneer zich een relevant incident voordoet dat om onmiddellijke reactie vraagt. Ook kan het individuele ketenpartijen ondersteunen bij het reageren op een lokaal incident. Met goede respons processen kan de impact van een incident, een digitale inbraak, een datalek of een digitale blokkade, zo veel mogelijk beperkt worden.

Het hoger onderwijs heeft, ter ondersteuning van de ho-instellingen, zo'n emergence response team in de vorm van SURFcert. In 2013 zijn door SURFcert meer dan 10.000 security incidenten voor de ho-sector behandeld. Wat het NCSC is voor de Rijksoverheid is SURFcert voor de gebruikers van SURFnet. SURFcert werkt in verschillende “netwerken” nauw samen met NCSC.

3. Toetsingskaders

Er zijn vele manieren waarop instellingen, leveranciers en andere onderwijsketenpartijen kunnen voldoen aan de kaders uit Hoofdstuk 2. Zij kunnen daarbij gebruik maken van diverse normenkaders, waarin samenhangende sets van beheersmaatregelen - vaak gericht op een specifiek werkings- en/of toepassingsgebied - zijn verzameld. In de Bijlage: Normenkaders is een overzicht opgenomen van normenkaders opgenomen. Instellingen en andere ketenpartijen die willen voldoen aan kaders uit het basisniveau en/of aanvullende kaders kunnen daaruit putten.

De keuze voor de toe te passen beheersmaatregelen ligt in beginsel bij de individuele ketenpartijen. Tegelijkertijd betekent het werken in ketens dat er onderlinge verwachtingen en afhankelijkheden zijn; ook - of *juist* - als het gaat om privacybescherming en informatiebeveiliging. De keten is met name op deze aspecten immers zo sterk als de zwakste schakel. Die verwachtingen komen tot uitdrukking in Hoofdstuk 2 in de paragraaf *Informatiebeveiliging en privacybescherming door ketenpartijen*. Daarin staat, kort samengevat, dat we als ketenpartijen in het onderwijs:

1. van andere partijen in de onderwijsketen verwachten dat zij zich - net als wij - conformeren aan de internationale ISO informatiebeveiligingsstandaard (ISO 27001/27002:2013, ook wel bekend als de 'code voor informatiebeveiliging), en
2. dat we gezamenlijk afspraken maken over de te realiseren volwassenheidsniveaus, en de manier waarop we die niveaus objectief meten

Voor het meten van volwassenheidsniveaus maken we gebruik van *toetsingskaders*. Dit zijn normenkaders, zoals de normenkaders uit de bijlage, waarvoor is vastgelegd op welke wijze *bewijsvoering* wordt verkregen voor het al dan niet voldoen aan de desbetreffende beheersmaatregelen.

Bewijsvoering kan op verschillende manieren verkregen worden:

- Via een zelfverklaring, waarbij een organisatie op eigen gezag een toetsingskader toepast en daarover een verklaring opstelt in welke mate aan de norm wordt voldaan;
- Via peer-assessment, waarbij ketenpartijen onderling een toetsingskader toepassen en over hun *peer* een verklaring opstellen in welke mate aan de norm wordt voldaan;
- Via een zogenaamd 'third party memorandum' of 'derdenverklaring', waarbij een onafhankelijke auditor een toetsingskader toepast en een verklaring opstelt in welke mate aan de norm wordt voldaan.

Op basis van die bewijsvoering kan vervolgend worden bepaald welk volwassenheidsniveau is bereikt.

Binnen het onderwijsdomein bestaan reeds verschillende toetsingskaders. Er kan onderscheid gemaakt worden tussen toetsingskaders gericht op verantwoordelijken (partijen die het doel en de middelen voor de verwerking van gegevens vaststellen) en bewerkers (partijen die ten behoeve van verantwoordelijken gegevens verwerken). Dit onderscheid wordt, waar het gaat om de verwerking van *persoons*gegevens, ook door de Wbp gehanteerd. Het onderscheid is relevant voor het onderwijsdomein, omdat steeds meer software 'uit de cloud' wordt betrokken. In de regel zullen instellingen als verantwoordelijke optreden, en leveranciers als bewerkers.

3.1 Toetsingskaders voor Verantwoordelijken

Normenkader informatiebeveiliging Hoger Onderwijs

Werkingsgebied: hoger onderwijs
Toepassingsgebied: (interne) organisatie

Het normenkader van SURF omvat een selectie van maatregelen uit ISO 27002. Het zijn zaken rond bescherming van veiligheid en continuïteit van bedrijfsgegevens en de privacy van studenten en medewerkers die een onderwijsinstelling ten minste geregeld moet hebben. De maatregelen zijn geclusterd; bij een assessment of audit wordt per cluster het volwassenheidsniveau van de instelling bepaald.

Website: https://www.surf.nl/diensten-en-producten/surfaudit/normenkader-surfaudit/index.html

Toetsingskaders informatiebeveiliging en privacy

Werkingsgebied: middelbaar beroepsonderwijs
Toepassingsgebied: (interne) organisatie

Deze gerichte doorvertaling van het Normenkader informatiebeveiliging Hoger Onderwijs door de MBO Taskforce informatiebeveiligingsbeleid (IBB) omvat een selectie van maatregelen uit ISO 27002. Het zijn zaken rond bescherming van veiligheid en continuïteit van bedrijfsgegevens en de privacy van studenten en medewerkers die een onderwijsinstelling ten minste geregeld moet hebben. De maatregelen zijn geclusterd; bij een assessment of audit wordt per cluster het volwassenheidsniveau van de instelling bepaald.

Website: http://www.kennisnet.nl/themas/informatiemanagement/informatiebeveiliging/

Voorwaarden voor aansluiting van een instelling op Studielink

Werkingsgebied: hoger onderwijs
Toepassingsgebied: aansluiten van een instelling op Studielink

Dit document is bedoeld voor een instelling van Hoger Onderwijs die wil aansluiten op Studielink. Het beoogt duidelijk te maken welke verantwoordelijkheden een aansluiting met zich meebrengt. Daarbij worden de voorwaarden van de aansluiting benoemd.

3.2 Toetsingskaders voor Bewerkers

Certificeringsschema ROSA

Werkingsgebied: gehele onderwijsdomein
Toepassingsgebied: aanbieden van clouddiensten via Edukoppeling

Het Certificeringsschema ROSA is bedoeld voor leveranciers van clouddiensten. Een cloudleverancier moet aan de normen in dit schema voldoen, vóórdat de betreffende clouddienst binnen de context van Edukoppeling mag worden ingezet.

Website: http://www.edustandaard.nl/standaarden/afspraken/afspraak/certificeringsschema-rosa/

SURF Juridisch normenkader cloudservices hoger onderwijs

Werkingsgebied: hoger onderwijs
Toepassingsgebied: afnemen van clouddiensten

Dit normenkader geeft een overzicht van de best practice clausules voor overeenkomsten met leveranciers van clouddiensten in het hoger onderwijs. Het juridisch normenkader omvat clausules die in lijn zijn met actuele nationale en Europese regelgeving op het gebied van o.a. gegevensbescherming en privacy.

Website: https://www.surf.nl/kennis-en-innovatie/kennisbank/2013/juridisch-normenkader-cloud-services-hoger-onderwijs.html

Studielink SIS-Adapter certificatie criteria

Werkingsgebied: hoger onderwijs
Toepassingsgebied: aansluiten van leveranciers op Studielink

Omdat veel ho-instellingen hetzelfde Student Informatie Systeem (SIS), (inclusief adapter naar Studielink) gebruiken heeft het zin om op SIS niveau een belangrijk deel van de testen (voor alle gebruikende instellingen) uit te voeren. Certificatie toont aan dat het SIS met Studielink-adapter de inschrijfverzoeken en andere activiteiten ter ondersteuning van het inschrijfproces juist, tijdig, volledig en veilig via berichten met Studielink kan uitwisselen. Certificatie vindt niet alleen plaats bij aansluiting, maar ook bij majeure wijzigingen in Studielink.

Kwalificatie Overstap Service Onderwijs

Werkingsgebied: po en vo
Toepassingsgebied: aansluiten van leveranciers op de voorziening OSO

De meeste softwareleveranciers in het primair en voortgezet onderwijs hebben hun systemen inmiddels voorzien van een aansluiting op de Overstap Service Onderwijs. Deze leveranciers hebben hiervoor een overeenkomst gesloten met OSO en conform afgesproken standaarden en veiligheidseisen hun programma's voorzien van extra OSO functionaliteiten.

Bijlage: Begrippenlijst

De begrippen die in dit document worden gebruikt sluiten zo veel mogelijk aan bij definities uit bestaande begrippenlijsten. Bij elk begrip hieronder is een verwijzing naar de bron van de definitie opgenomen.

Audit
Systematisch, onafhankelijk en gedocumenteerd proces voor het verkrijgen en objectief evalueren van bewijs teneinde vast te stellen in hoeverre aan een toetsingskader is voldaan.
ISO 27001:2013 (audit)

Assessment
Zie ***Audit***

Beheersmaatregel
Maatregel die risico wijzigt
ISO 27000:2013 (control)

Beschikbaarheid
De eigenschap van het toegankelijk en bruikbaar zijn op aanvraag van een geautoriseerde entiteit
ISO 27000:2014 (availability)

Beschikbaarheid betreft het waarborgen dat geautoriseerde gebruikers op de juiste momenten toegang hebben tot informatie en aanverwante bedrijfsmiddelen. Aantasting van beschikbaarheid kan bijvoorbeeld leiden tot aantasting van de continuïteit van bedrijfs- en/of ketenprocessen.

Beveiliging
Behoud van vertrouwelijkheid, integriteit en beschikbaarheid van informatie
ISO 27000:2013 (information security)

Bewerker
Partij die ten behoeven van een verantwoordelijke gegevens verwerkt.
Wbp (NB. Wbp beperkt definitie tot verwerking van persoonsgegevens)
zie ook: ***Verantwoordelijke***

Bewijs
Feitelijke verklaringen of andere informatie die controleerbaar is en relevant voor een toetsingskader.
ISO 19011:2011 (audit evidence)

Integriteit
De eigenschap van juistheid en volledigheid.
ISO 27000:2013 (integrity)

Integriteit betreft het waarborgen van de juistheid, volledigheid en tijdigheid van informatie. Informatie waarvoor de integriteit op orde is, is dus informatie die 'klopt'. Merk op dat een aantasting van vertrouwelijkheid (waardoor onbevoegden bijvoorbeeld mutaties kunnen doorvoeren) kan leiden tot een aantasting van integriteit.

Kader
Verzameling beleid, procedures en/of eisen
zie ook ***Normenkader, Toetsingskader***

Ketenpartij
Een partij die een rol speelt in een ketenproces

Ketenproces	Een samenwerking tussen entiteiten die dient om een (gezamenlijk) doel te realiseren.
Maatregel	Handeling of ingreep met een bepaald doel *Van Dale*
Norm	Beleid, procedure of eis gebruikt als referentie *zie ook **Normenkader, Toetsingskader***
Normenkader	Verzameling beleid, procedures en/of eisen gebruikt als referentie *zie ook **Toetsingskader***
Privacy	Het recht om in de beslotenheid van de persoonlijke levenssfeer met rust te worden gelaten, waaronder het recht op zorgvuldige behandeling van persoonlijke gegevens. *zie Grondwet, artikel 10, lid 2 en 3*
Risico	Effect van onzekerheid op doelstellingen. *ISO 27000:2013 (risk)*
Risicoanalyse	Proces om de aard van risico te begrijpen en het risiconiveau te bepalen *ISO 27000:2013 (risk analysis)*
ROSA	Referentiearchitectuur van het onderwijs
Toetsingskader	Verzameling beleid, procedures en/of eisen gebruikt als referentie waartegen bewijs uit een audit wordt vergeleken. *ISO 19011:2011 (audit criteria)*
Verantwoordelijke	Partij die het doel en de middelen voor de verwerking van gegevens vaststelt. *Wbp (NB. Wbp beperkt definitie tot verwerking van persoonsgegevens)* *zie ook: **Bewerker***
Vertrouwelijkheid	De eigenschap dat informatie niet beschikbaar wordt gesteld of ter kennis komt van onbevoegde personen, entiteiten of processen *ISO 27000:2013 (confidentiality)* Vertrouwelijkheid betreft het waarborgen dat informatie alleen toegankelijk is voor degenen die hiertoe zijn geautoriseerd. Met 'toegang hebben tot' wordt zowel het raadplegen als het muteren, toevoegen en/of vernietigen van informatie bedoeld.

Bijlage: Normenkaders

ISO 27002

Werkingsgebied: gehele onderwijsdomein

Toepassingsgebied: (interne) organisatie

ISO 27002 omvat beheersmaatregelen voor het implementeren van een managementsysteem voor informatiebeveiliging conform ISO27001. Deze maatregelen dienen ook als leidraad voor organisaties die algemeen aanvaarde beheersmaatregelen op het gebied van informatiebeveiliging willen invoeren. Het College voor Standaardisatie heeft ISO27001 en 27002 op de lijst met 'pas toe of leg uit'-standaarden geplaatst. Overheden en semi-overheden zijn daarom verplicht om deze standaard toe te passen.

NORA-katern beveiliging

Werkingsgebied: (semi-)overheid

Toepassingsgebied: massale verwerking van persoons- en financiële gegevens

NORA staat voor Nederlandse Overheid Referentie Architectuur. Het NORA-katern Beveiliging omvat beheersmaatregelen en implementatierichtlijnen (samengenomen onder de noemer 'eisen') voor de beveiliging van massale verwerking van persoons- en financiële gegevens, uitgaande van het basisniveau informatiebeveiliging voor de e-overheid. Het NORA-katern is afgeleid van de werkgebieden informatiebeveiliging en bedrijfscontinuïteit uit ISO 27002. De aspecten fysieke beveiliging en personele integriteit blijven in dit katern buiten beschouwing.

Baseline Informatiebeveiliging Rijksdienst

Werkingsgebied: rijksoverheid

Toepassingsgebied: (interne) organisatie

De BIR (Baseline Informatiebeveiliging Rijksdienst) beschrijft de invulling van ISO27001 en 27002 voor de Rijksoverheid. Het bestaat uit een - binnen de Rijksoverheid verplicht toe te passen - tactisch normenkader (een superset van ISO 27002/maatregelen) en een niet-verplichte operationele baseline die bestaat uit best practices.

Gemeenten en waterschappen hebben een afgeleide variant van de BIR opgesteld: de BIG voor gemeenten en de BIW voor Waterschappen.

Cloud Security Alliance Cloud Controls Matrix

Werkingsgebied: gehele onderwijsdomein

Toepassingsgebied:aanbieden en afnemen van clouddiensten

De Cloud Controls Matrix (CCM) van de Cloud Security Alliance (CSA) legt een relatie tussen de negen grootste risico's van cloud computing en de maatregelen ('controls') die een effectieve bescherming vormen tegen deze risico's. De CCM richt zich enerzijds op het bieden van beveiligingsrichtlijnen aan cloudleveranciers, en anderzijds op het ondersteunen van cloudafnemers bij het beoordelen van de veiligheidsrisico's van een cloudleverancier.

CBP Compliance-instrumenten

Werkingsgebied: gehele onderwijsdomein

Toepassingsgebied: (interne) organisatie

Het CBP heeft een viertal compliance-instrumenten ontwikkeld die gebruikt kunnen worden als handreiking voor het naleven van de geldende wet- en regelgeving:

- Quickscan
- Wbp Zelfevaluatie
- Raamwerk Privacy Audit
- Handreiking bij het Raamwerk Privacy Audit

NCSC Beveiligingsrichtlijnen

Werkingsgebied: gehele onderwijsdomein
Toepassingsgebied: technologie

Het Nationaal Cyber Security Center publiceert beveiligingsrichtlijnen naar aanleiding van trends en (actuele) dreigingen en op basis van best practices :

- ICT-beveiligingsrichtlijnen voor webapplicaties (feb. 2012)
- Beveiligingsrichtlijnen voor mobiele apparaten (nov. 2012)
- ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS) (nov. 2014)

Kennisnet Checklist privacy-afspraken voor scholen

Werkingsgebied: onderwijsinstellingen
Toepassingsgebied: afnemen van clouddiensten

Met deze checklist kan worden vastgesteld of de afspraken tussen scholen en softwareleveranciers voldoen aan de wettelijke eisen.

Afsprakenstelsel IAA (SION)

Werkingsgebied: gehele onderwijsdomein
Toepassingsgebied: persoonsidentiteit

Het afsprakenstelsel leidt tot een *nummervoorziening* die gebruikt wordt om pseudo-identiteiten te genereren. Het gebruik van pseuso-identiteiten c.q. pseudoniemen is een maatregel die voor het hele onderwijsdomein geldt.

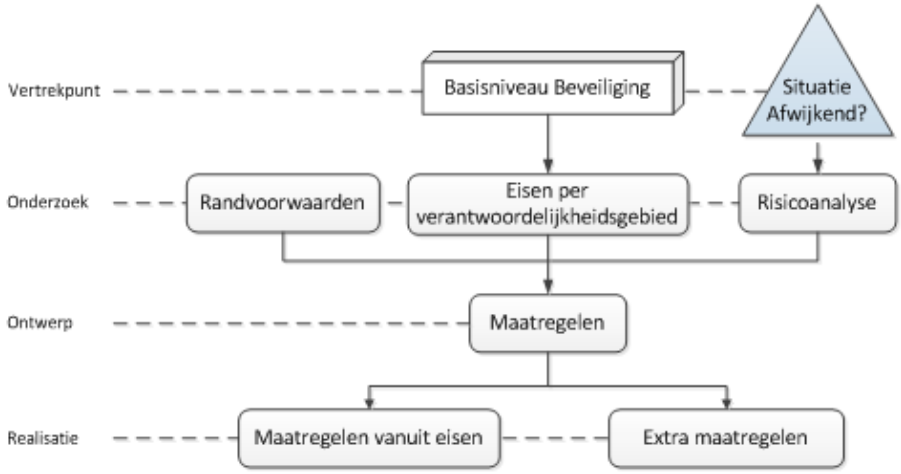
Privacyreglement gebruik van persoonsgegevens van leerlingen binnen leermiddelen PO/VO (GEU)

Werkingsgebied uitgeverijen PO/VO
Toepassingsgebied: gebruik van persoonsgegevens leerlingen

Bijlage: Methodiek voor formuleren kaders

4.1 Aanpak

De kaders uit Hoofdstuk 2 vormen een Basisniveau Beveiliging, voor specifieke contexten aangevuld met additionele kaders. Op basis van deze kaders kunnen beheersmaatregelen worden geselecteerd, bijvoorbeeld uit ISO 27002 of andere raamwerken zoals het NORA Katern Beveiliging[2]. Een voorbeeld van zo'n selectie staat in de **Fout! Verwijzingsbron niet gevonden.**. Deze beheersmaatregelen leiden ot maatregelen in organisaties, processen, applicaties en/of technologie.



Figuur 1: Risicoanalyse (uit NORA Katern Beveiliging)

Doet zich een situatie voor die - vanuit proces, organisatie en/of doelstellingen - afwijkt van het Basisniveau Beveiliging, dan vindt een risicoanalyse plaats die gericht is op die afwijkende situatie. Zo'n risicoanalyse leidt tot nieuwe kaders. Die gelden dan als aanvullend kader voor die specifieke situatie. Als het opgestelde kader breder geldt, dan wordt het opgenomen in het basisniveau zelf. Zodoende breidt het Basisniveau Beveiliging zich met elke risicoanalyse weer een stap verder uit.

4.2 Risicoanalyse

Het Basisniveau Beveiliging wordt gevoed vanuit risicoanalyses. Initieel is (was) het basisniveau nog leeg. Uit een risicoanalyse voor het domein Toetsen en Examineren is de eerste invulling van het basisniveau, zoals dat in Hoofdstuk 3 is beschreven, tot stand gekomen.

Er zijn echter nog meer gebieden, waarvoor op een soortgelijke manier een risicoanalyse kan worden uitgevoerd. De resultaten van die risicoanalyses kunnen ook ondergebracht worden in het Basisniveau Beveiliging. Door steeds meer resultaten samen te brengen in dit katern ontstaat een steeds bredere basisniveau voor privacy en informatiebeveiliging. Ook groeit zo de *body of knowledge* over (de toepassing van) maatregelen om aan dat basisniveau te voldoen.

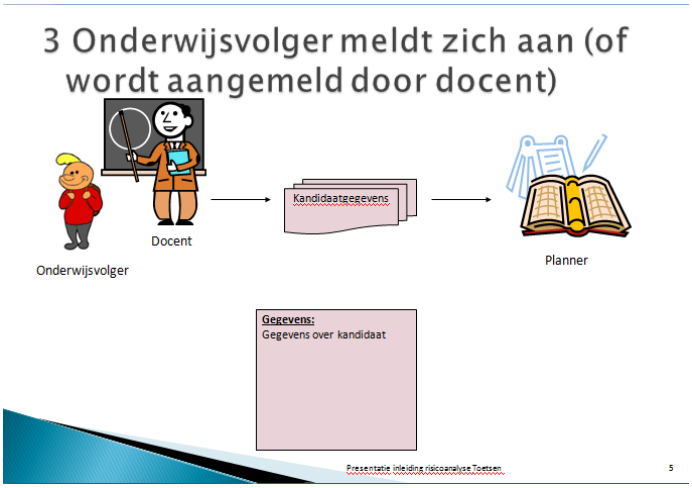
Een risicoanalyse uitvoeren gaat op hoofdlijnen als volgt:

1. Het ketenproces wordt beschreven in opeenvolgende stappen. In elke ketenprocesstap vindt interactie plaats tussen actoren en bepaalde gegevens.
    a. Voorbeeld (uit ketenproces Toetsen en Examineren): *De onderwijsvolger meldt zich aan voor een toets (of wordt aangemeld door de docent)*.

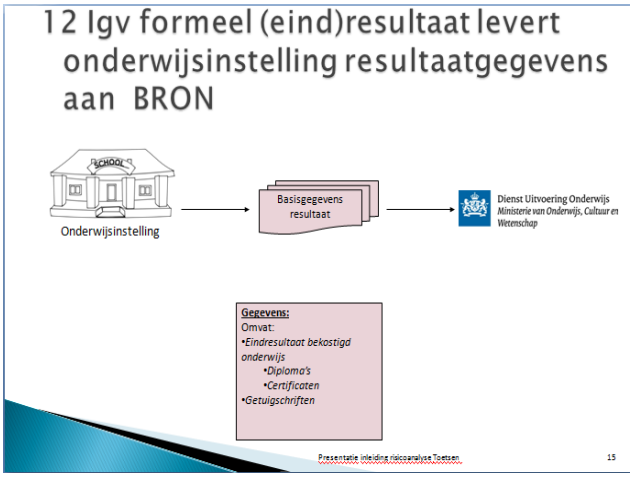
[2] In het NORA Katern Beveiliging zijn beheersmaatregelen en implementatierichtlijnen samengenomen onder de noemer *eisen*. Onder die naam komen ze ook terug in Figuur 1.

b. Voorbeeld (uit ketenproces Toetsen en Examineren): *In geval van een formeel (eind)resultaat levert de onderwijsinstelling de resultaatgegevens aan BRON.*

2. Voor elke ketenprocesstap wordt een dia opgesteld die de betrokken actoren en gegevens toont.
   a. Voorbeeld (uit ketenproces Toetsen en Examineren):



   b. Voorbeeld (uit ketenproces Toetsen en Examineren):



3. De dia's worden afgedrukt en krijgen een plaats aan de muur van de workshopruimte.
4. De aanwezige experts benoemen in hun eigen woorden de risico's die samenhangen met het ketenproces. Ze noteren deze risico's op een post-it en plakken deze op de afdruk van de processtap waarin dat risico optreedt.
5. De geïdentificeerde risico's worden plenair besproken en waar nodig toegelicht door de indiener. Eventueel kunnen risico's na bespreking dan alsnog vervallen.
6. Alle geïdentificeerde risico's worden ter verdere analyse op een risicolijst gezet.

Na deze workshopfase volgt een analysefase. Daarin worden de geïdentificeerde risico's geclusterd. Voor risico's die nog niet door het basisniveau privacy en beveiliging afgedekt zijn, worden kaders geformuleerd om deze (clusters van) risico's af te dekken. De analyseresultaten worden gedeeld en in een vervolgbijeenkomst besproken met de bij de workshop betrokken experts, opdat hierover overeenstemming wordt bereikt. De tabel hieronder toont een cluster van soortgelijke risico's (linkerkolom) dat door hetzelfde kader (rechterkolom) wordt afgedekt.

Neefje maakt de toets	Gegevens met een hoge integriteitsklasse worden zo opgeslagen en getransporteerd dat onrechtmatige aanpassingen onmogelijk worden gemaakt.
Aanlevering onversleuteld (onderschepping + manipulatie)	
Injectie examens	
Toets vastgesteld door verkeerde persoon	
Toetsantwoorden kunnen veranderen	
Wijzigen antwoorden; fraude door afnemer	
Autorisatie afnamesysteem Read/Write – ongeautoriseerde toegang	
Toetsen worden achteraf aangepast	
Score wordt achteraf aangepast	
Norm wordt aangepast door derden	
Scores worden achteraf aangepast	
Toetsresultaat wordt aangepast	
Hacken en cijfers muteren	
Kind van medewerker	

Waar mogelijk worden, zoals hierboven, de gestelde kaders zó veralgemeniseerd, dat ze opgenomen kunnen worden in het basisniveau uit paragraaf 3.1. Anders worden ze, zoals hieronder, geformuleerd als aanvullende kaders op het basisniveau voor een specifiek ketenproces (zie paragraaf 3.2).

Integriteit van locatie kan niet gewaarborgd worden - fraude op toilet	De toetslocatie is zo ingericht dat fraude wordt voorkomen
Toegang tot locatie niet afgeschermd	

Op basis van deze kaders kunnen vervolgens passende maatregelen worden geselecteerd, zoals geïllustreerd in **Fout! Verwijzingsbron niet gevonden.**.

4.3 Risicoclassificatie

De zwaarte van de te nemen maatregelen hangt in de regel af van de zogenaamde BIV-classificatie van de gegevens die bij een ketenprocesstap betrokken zijn. In de toekomst zullen alle gegevens waarop informatiebeveiligingsbeleid van toepassing is, geclassificeerd moeten zijn. Het niveau van de beveiligingsmaatregelen is afhankelijk van de klasse.
De BIV classificatie is afgeleid van de volgende kwaliteitsaspecten:

- **B**eschikbaarheid
- **I**ntegriteit
- **V**ertrouwelijkheid

Ten aanzien van de **beschikbaarheid**seisen worden de volgende klassen onderscheiden:

Klasse	Basisprincipes	Beveiligingsniveau
LAAG (Niet vitaal)	algeheel verlies of niet beschikbaar zijn van deze informatie gedurende langer dan 1 week brengt geen merkbare (meetbare) schade toe aan de belangen van ketenpartijen, hun medewerkers of hun klanten	Basisbescherming (Laag)
MIDDEN (Vitaal)	algeheel verlies of niet beschikbaar zijn van deze informatie gedurende langer dan 1 week brengt merkbare schade toe aan de belangen van ketenpartijen, hun medewerkers of hun klanten	Basisbescherming + (Midden)
HOOG (Zeer vitaal)	algeheel verlies of niet beschikbaar zijn van	Basisbescherming ++

	deze informatie gedurende langer dan 1 etmaal brengt merkbare schade toe aan de belangen van ketenpartijen, hun medewerkers of hun klanten	(Hoog)

Voor **integriteit** en **vertrouwelijkheid** worden de volgende indeling gevolgd.

Klasse	Basisprincipes	Beveiligingsniveau
LAAG (Openbaar)	· Iedereen mag de gegevens inzien, bijvoorbeeld de website van een onderwijsinstelling · Een geselecteerde groep mag deze gegevens wijzigen	Basisbescherming
MIDDEN (Intern)	· Iedereen die aan een instelling is verbonden als medewerker of student mag deze gegevens inzien; toegang kan zowel binnen als buiten de instelling (remote) worden verleend, bijvoorbeeld lesroosters of Elektronische leeromgeving · Een geselecteerde groep mag deze gegevens wijzigen	Basisbescherming
HOOG (Vertrouwelijk)	· Er is expliciet aangegeven wie welke rechten heeft t.a.v. de raadpleging en de verwerking van deze gegevens, bijvoorbeeld Kernregistratie systeem.	Basisbescherming +

Welk beveiligingsniveau geschikt is voor een bepaald informatiesysteem hangt af van de classificatie van de informatie die het systeem verwerkt. De classificatie wordt bepaald door of namens de eigenaar van het betreffende informatiesysteem.

Bijlage: Doelstellingen uit ISO/IEC 27001/27002

1. Ketenpartijen hebben directieaansturing van en -steun voor informatiebeveiliging in overeenstemming met bedrijfseisen en relevante wet- en regelgeving.
2. Ketenpartijen stellen een beheerkader vast om de implementatie en uitvoering van de informatiebeveiliging binnen hun organisatie te initiëren en te beheersen.
   Toelichting: het beheerkader is gericht op het in de organisatie inbedden van de beleidsregels die komen vanuit de directieaansturing.
3. Ketenpartijen waarborgen de veiligheid van telewerken en het gebruik van mobiele apparatuur.
4. Ketenpartijen waarborgen dat medewerkers en contractanten hun verantwoordelijkheden begrijpen en geschikt zijn voor de functies waarvoor zij in aanmerking komen.
5. Ketenpartijen zorgen ervoor dat medewerkers en contractanten zich bewust zijn van hun verantwoordelijkheden op het gebied van informatiebeveiliging en deze nakomen.
6. Ketenpartijen beschermen de belangen van hun organisatie als onderdeel van de wijzigings- of beëindigingsprocedure van het dienstverband.
7. Ketenpartijen identificeren bedrijfsmiddelen die samenhangen met informatie en informatieverwerkende faciliteiten en stellen van deze bedrijfsmiddelen een inventaris op en onderhouden deze.
8. Ketenpartijen bewerkstelligen dat informatie een passend beschermingsniveau krijgt dat in overeenstemming is met het belang ervan voor hun organisatie.
9. Ketenpartijen voorkomen onbevoegde openbaarmaking, wijziging, verwijdering of vernietiging van informatie die op media is opgeslagen.
10. Ketenpartijen beperken toegang tot informatie en informatieverwerkende faciliteiten.
11. Ketenpartijen bewerkstelligen toegang voor bevoegde gebruikers en voorkomen onbevoegde toegang tot systemen en diensten.
12. Ketenpartijen maken gebruikers verantwoordelijk voor het beschermen van hun authenticatie-informatie.
13. Ketenpartijen voorkomen onbevoegde toegang tot systemen en toepassingen.
14. Ketenpartijen zorgen voor correct en doeltreffende gebruik van cryptografie om de vertrouwelijkheid, authenticiteit en/of integriteit van informatie te beschermen.
15. Ketenpartijen voorkomen onbevoegde fysieke toegang tot, schade aan en interferentie met informatie en informatieverwerkende faciliteiten van hun organisatie.
16. Ketenpartijen voorkomen verlies, schade, diefstal of compromittering van bedrijfsmiddelen en onderbreking van de bedrijfsvoering van hun organisatie.
17. Ketenpartijen waarborgen correcte en veilige bediening van informatieverwerkende faciliteiten.
18. Ketenpartijen waarborgen dat informatie en informatieverwerkende faciliteiten beschermd zijn tegen malware.
19. Ketenpartijen beschermen zich tegen het verlies van gegevens.
20. Ketenpartijen leggen gebeurtenissen vast en verzamelen bewijs.
21. Ketenpartijen waarborgen de integriteit van operationele systemen.
22. Ketenpartijen voorkomen de benutting van technische kwetsbaarheden.
23. Ketenpartijen maken de impact van auditactiviteiten op uitvoeringssystemen zo gering mogelijk.
24. Ketenpartijen waarborgen de bescherming van informatie in netwerken en de ondersteunende informatieverwerkende faciliteiten.
25. Ketenpartijen handhaven de beveiliging van informatie die wordt uitgewisseld binnen hun organisatie en met een externe identiteit.
26. Ketenpartijen waarborgen dat informatiebeveiliging integraal deel uitmaakt van informatiesystemen in de gehele levenscyclus. Hiertoe behoren ook de eisen voor informatiesystemen die diensten verlenen via openbare netwerken.
27. Ketenpartijen bewerkstelligen dat informatiebeveiliging wordt ontworpen en geïmplementeerd binnen de ontwikkelingslevenscyclus van informatiesystemen.

28. Ketenpartijen waarborgen bescherming van gegevens die voor het testen zijn gebruikt.
29. Ketenpartijen waarborgen de bescherming van bedrijfsmiddelen van de organisatie die toegankelijk zijn voor leveranciers.
30. Ketenpartijen handhaven een overeengekomen niveau van informatiebeveiliging en dienstverlening in overeenstemming met de leveranciersovereenkomsten.
31. Ketenpartijen bewerkstelligen een consistente en doeltreffende aanpak van het beheer van informatiebeveiligingsincidenten, met inbegrip van communicatie over beveiligingsgebeurtenissen en zwakke plekken in de beveiliging.
32. Ketenpartijen bedden informatiebeveiligingscontinuïteit in de systemen van het bedrijfscontinuïteitsbeheer van hun organisatie.
33. Ketenpartijen bewerkstelligen beschikbaarheid van informatieverwerkende faciliteiten.
34. Ketenpartijen voorkomen schendingen van wettelijke, statutaire, regelgevende of contractuele verplichtingen betreffende informatiebeveiliging en beveiligingseisen.
35. Ketenpartijen verzekeren dat de informatiebeveiliging wordt geïmplementeerd en uitgevoerd in overeenstemming met de beleidsregels en procedures van hun organisatie.
    Toelichting: Dit impliceert dat de genomen maatregelen toetsbaar en controleerbaar zijn, en dat er zowel interne controle is op de naleving van het beveiligingsbeleid als dat er, waar nodig, onafhankelijke (externe) beoordelingen worden uitgevoerd.