Dienst Uitvoering Onderwijs
Ministerie van Onderwijs, Cultuur en Wetenschap

INFORMATIEBEVEILIGINGPLAN

"Baseline Informatiebeveiliging"
(conform de Code voor Informatiebeveiliging, ISO/IEC 27001- 27002)

Ernst R.A. de Widt MBA / Centrale Security Officer DUO

Groningen, juli 2011

Definitief, versie 3.2

Inhoudsopgave

0. Inleiding

Eind 2010 is aan het management van DUO een nieuwe baseline informatiebeveiliging uitgereikt. Velen van u hebben na bestudering verzocht om een nadere uitwerking van de hierin genoemde beveiligingsmaatregelen. Aan dat verzoek wordt door middel van deze notitie voldaan.
Bij deze uitwerking is zo veel mogelijk gebruik gemaakt van formuleringen zoals die staan in de 'Code voor de Informatiebeveiliging, ISO/IEC 27001- en 27002 hierdoor wordt door DUO aangesloten bij de internationale en landelijke standaard.
Nadeel van de gevolgde procedure is echter het forse formaat van dit overzicht. Om een en ander hanteerbaar te houden is er voor gekozen om naast deze notitie ook nog een detail uitwerking te publiceren van alle maatregelen inclusief de toelichtingen. In verband met de omvang zal deze alleen digitaal beschikbaar zijn. (wiki/EA/Beveiligingarchitectuur) Beide documenten zijn strikt bedoeld voor intern gebruik van DUO en zijn geen alternatief voor het uitvoeren van risicoanalyses (A&K) zoals is vastgelegd in het VIR.

1. Samenvatting

Het ministerie van OCW conformeert zich aan het Voorschrift Informatiebeveiliging Rijksdienst (VIR). Het uitvoeren van de risicoanalyses is daarbij één van de verplichte onderdelen van het VIR. Op het gebied van informatiebeveiliging is naast het Rijksbeleid het geformuleerde beleid van OCW voor DUO het uitgangspunt bij de uitvoering en inrichting.

De maatregelen en de samenhang worden ook zichtbaar gemaakt door ze te beschrijven in een Informatiebeveiligingplan, ook wel de Baseline Informatiebeveiliging, of kortheidshalve de 'Baseline' genoemd. Hierin wordt het dan geldende security-niveau van DUO beschreven. Periodiek wordt bekeken welke maatregelen zij moet treffen om risico's aanvaardbaar te houden.

Vanaf 1 januari 2010 is de IB-Groep samen met het CFI, de Centrale Financiën Instellingen, opgegaan in de nieuwe organisatie **Dienst Uitvoering Onderwijs** (DUO). Deze uitvoeringsorganisatie valt rechtstreeks onder de verantwoordelijkheid van het ministerie van Onderwijs, Cultuur en Wetenschappen (min OCW).

Met de fusie is voor DUO de noodzaak ontstaan om de twee informatiebeveiligingsplannen te combineren en te komen tot één document voor de DUO organisatie. Dit plan wijkt af van de Baseline van het Ministerie van OCW. Dit komt door het karakter van onze werkzaamheden en vanwege het feit dat een dergelijk plan dicht moet aansluiten bij onze werkzaamheden en daarmee bij het DUO risicoprofiel. DUO heeft als uitvoeringsorganisatie rechtstreeks te maken met individuele klanten, gegevensuitwisselingen met publieke en private organisaties in het onderwijsveld maar ook daarbuiten.

Informatiebeveiliging ontwikkelt zich steeds meer tot een normale managementtaak richting risicobeheersing en vraagt daarom ook om een actieve en betrokken opstelling van het lijnmanagement bij het opstellen c.q. beheer van procedures en bij het opstellen van continuïteitsplannen.

Onder informatiebeveiliging wordt verstaan: ”Het treffen en onderhouden van een samenhangend pakket van maatregelen om de beoogde betrouwbaarheid (beschikbaarheid, exclusiviteit en integriteit) van de informatievoorziening te waarborgen”.

Het informatiebeveiligingbeleid heeft tot doel het garanderen van:

- de **beschikbaarheid** van middelen en informatie om de werkzaamheden te kunnen uitoefenen;
- de **exclusiviteit** van bepaalde ruimten en informatie;
- de **integriteit** van informatiesystemen en daarmee vastgelegde informatie te waarborgen;
- de **persoonlijke veiligheid** van DUO medewerkers;
- de **fysieke veiligheid** van de gebouwen waarin de activiteiten worden uitgeoefend;
- de **onweerlegbaarheid** van (elektronische) transacties aan te tonen.

Risicobeheersing wordt verkregen door per relevante bedreiging te onderzoeken welke maatregelen, bezien vanuit de bovengenoemde terreinen, uitkomst bieden.
Dit onderzoek gebeurt door het periodiek uitvoeren van risicoanalyses op onze bedrijfsprocessen. Bij DUO wordt hiervoor gebruik gemaakt van de tool CRAMM.

De baseline van DUO is opgesteld volgens de indeling van de Code voor Informatiebeveiliging[1] en op basis van de resultaten uit de uitgevoerde risicoanalyse (inclusief A&K-analyses). Daarnaast is nog een aantal algemene maatregelen vastgesteld. De baseline Informatiebeveiliging is, conform de indeling in de Code voor de Informatiebeveiliging, onderverdeeld in de volgende elf hoofdstukken.

A. 5	Beveiligingsbeleid
A. 6	Organisatie van informatiebeveiliging
A. 7	Beheer van bedrijfsmiddelen
A. 8	Beveiliging van personeel
A. 9	Fysieke beveiliging en beveiliging van de omgeving
A.10	Beheer van communicatie- en bedieningsprocessen
A.11	Toegangsbeveiliging
A.12	Verwerving, ontwikkeling en onderhoud van informatiesystemen
A.13	Beheer van informatiebeveiligingsincidenten

1 De Code voor Informatiebeveiliging is de Nederlandse versie van de British Standards 7799, ofwel BS 7799, die later als internationale standaard (ISO/IEC 17799) voor informatiebeveiliging is gepubliceerd. De Code voor Informatiebeveiliging bestaat uit twee delen: een norm ISO/IEC 27001 en een 'code of practice' (ISO/IEC 27002). Certificering gebeurt tegen de norm, de 'code of practice' deze geeft handreikingen voor de implementatie van maatregelen in de organisatie. De Code voor Informatiebeveiliging beschrijft in 11 hoofdstukken normen en maatregelen, die van belang zijn voor het realiseren van een afdoende niveau van informatiebeveiliging.

A.14	Bedrijfscontinuïteitsbeheer
A.15	Naleving

Vanuit de verantwoordelijkheid van de lijnmanager geeft de Baseline een overzicht van de relevante eisen op het gebied van de Informatiebeveiliging. De grote diversiteit en impact van de individuele systemen zal altijd specifieke te treffen (aanvullende) maatregelen met zich meebrengen. Dit houdt dus in dat per systeem[2] altijd een A&K-analyse uitgevoerd moet worden. De baseline kan dan ook nooit beschouwd worden als vervanging van de risicoanalyse.

Een baseline is nimmer statisch, doch altijd onderhevig aan onderhoud en wijzigingen afhankelijk van (nieuwe) wet- en regelgeving en veranderingen in bijvoorbeeld de technische of fysieke omgeving.

Verder is een verbetering van de kwaliteit van de baseline afhankelijk van:

I. hoeveelheid input (meer uitgevoerde analyses);
II. een verbreding en verdieping van de risico- en maatregel-gebieden;
III. het gewenst beveiligingsniveau en het risicoprofiel.

Het vaststellen en onderhouden van de baseline is onderdeel van het takenpakket van de Centrale Security Officer (CSO) en Decentrale Security Officers (DSO).

2. Verantwoordelijkheden binnen de informatiebeveiliging

OCW Secretaris-generaal (SG)

- is eindverantwoordelijk voor de zorg voor organisatie en bedrijfsvoering en met dit laatste voor de kwaliteit van de werkprocessen, de werkprocessen ondersteunende informatiesystemen en de informatiebeveiliging;
- heeft de PSG in dit kader gemandateerd de taken op het terrein van de informatiebeveiliging namens hem uit te voeren;
- wijst een organisatieonderdeel overstijgend proces en het procesondersteunende informatiesysteem toe aan één lijnmanager;
- is verantwoordelijk voor de uitvoering van de informatiebeveiliging door de lijnmanagers binnen zijn portefeuille;
- ziet toe op de naleving van de kaders van het beheer en onderhoud van de informatiebeveiliging bij de organisatieonderdelen binnen zijn portefeuille.

[2] Onder 'systeem' wordt in dit kader verstaan: Samenhangende gegevensverwerkende functionaliteit die kan worden ingezet om een of meerdere bedrijfsprocessen te kennen, te ondersteunen of te besturen. Omvat apparatuur, programmatuur, gegevens, procedures, werkomgeving en mensen.

OCW Plv. Secretaris-generaal (PSG)

- is namens de SG belast met de algemene zorg voor de beveiliging van de informatie zoals die in het VIR, het VIR-bi en het Beveiligingsvoorschrift 2005 is geregeld;
- is verantwoordelijk voor het vaststellen en het uitdragen van het informatiebeveiligingsbeleid;
- laat concernbreed toezicht uitoefenen op de implementatie van het beleid;
- geeft opdracht tot onderzoek bij (vermoeden van) overtreding gedragscode e-mail- en internetgebruik, of schending van integriteit of vertrouwelijkheid van informatie aan de BVA dan wel de CSO;
- rapporteert in het MT-OCW over de informatiebeveiliging binnen het ministerie;
- heeft de BVA gemandateerd taken voortvloeiende uit de (informatie)beveiliging namens hem uit te voeren;
- is verantwoordelijk voor de uitvoering van de informatiebeveiliging bij organisatieonderdelen binnen zijn portefeuille;
- ziet toe op de naleving van de kaders van het beheer en onderhoud van de informatiebeveiliging door de lijnmanagers binnen zijn portefeuille;
- stelt (onverwijld) na compromittering1 van een staatsgeheim een commissie van onderzoek in.

OCW Beveiligingsambtenaar BVA

De BVA functie is ondergebracht binnen OCW-BOA, bureau Veiligheid Integriteit en Crisismanagement.

- is namens de (P)SG belast met de integrale beveiliging, waaronder de informatiebeveiliging;
- coördineert de integrale beveiliging en zorgt dat de informatiebeveiliging aansluit (blijft aansluiten) bij de integrale beveiliging;
- licht de (P)SG in ingeval incidenten en bij het compromitteren van een staatsgeheim;
- aansturing van DUO CSO beleidsmatig en functioneel;
- toetst of het niveau van de informatiebeveiliging bij OCW voldoet aan de kaders, die gesteld zijn in de betreffende Organisatieregeling c.q. het betreffende Managementcontract.

DUO Directeur-generaal (DG)

- is verantwoordelijk voor de uitvoering van de informatiebeveiliging door de lijnmanagers binnen DUO;
- ziet toe op de naleving van de kaders van het beheer en onderhoud van de informatiebeveiliging bij de organisatieonderdelen binnen DUO, alsmede op het bedrijfscontinuïteitsplan;
- ziet toe op het jaarlijks auditten van informatiebeveiligingstelsels van organisatieonderdelen en informatiesystemen (op basis van opzet, bestaan en werking).

DUO Centrale Security Officer (CSO)

- ontwikkelt binnen DUO visie en beleid op het terrein van de informatiebeveiliging op basis van het VIR, VIR-bi, Beveiligingsvoorschrift 2005, andere wet- en regelgeving en richtlijnen van de BVA en adviseert in dit kader de leiding van DUO en de lijnmanagers;

- werkt de informatiebeveiliging binnen DUO uit op basis van het Integraal Beveiligingsbeleid en wet- en regelgeving;
- ontwikkelt binnen DUO standaards, normen en beleidsinstrumenten;
- is voorzitter van het DUO platform informatiebeveiliging en bescherming persoonsgegevens;
- draagt het beleid en de normen uit (d.m.v. presentaties, voorlichting, communicatiecampagnes en workshops);
- coördineert de informatiebeveiliging binnen DUO, fungeert in dit kader voor de medewerkers van ICT/I&E/Beveiliging als aanspreekpunt indien sprake is van potentiële bedreigingen;
- stuurt de Decentrale Security Officers en de Privacy Officers aan;
- adviseert over (on)mogelijkheden voor de informatiebeveiliging van informatie en informatie-systemen binnen DUO; formuleert in dit kader (wijzigings)-voorstellen;
- ziet toe op en evalueert de uitvoering van het informatiebeveiligingsbeleid;
- toetst de toereikendheid van de informatiebeveiliging;
- voert relatiebeheer en volgt de ontwikkelingen in het beleid van de organisatie en de daaruit voortvloeiende wensen; beziet de consequenties die wensen hebben voor informatiebeveiliging;
- is proceseigenaar voor het incidentenbeheer op het terrein van de informatiebeveiliging, stelt een incidentenprocedure op en onderzoekt inbreuken op de informatiebeveiliging;
- voert intra- en interdepartementaal overleg;
- verzamelt managementinformatie m.b.t. de informatiebeveiliging en rapporteert hierover;
- identificeert en analyseert (nieuwe) bedreigingen in het terrein van informatiebeveiliging;
- signaleert trends en ontwikkelingen rond methoden en technieken, tools, wetten en richtlijnen op het terrein van informatiebeveiliging;
- initieert kwaliteitsverbeteringtrajecten op het terrein van informatiebeveiliging;
- evalueert periodiek de beveiliging van bijzondere informatie;
- rapporteert over de bevindingen ten aanzien van de informatiebeveiliging aan de lijnmanager die verantwoordelijk is voor het organisatieonderdeel en/of informatiesysteem;
- ontwikkelt de informatiebeveiligingsfunctie (verder);
- stelt het bedrijfscontinuïteitsplan op en ziet toe op de consistentie van de deelplannen op product- cq aandachtsgebieden;
- met betrekking tot bijzondere informatie:
  - maakt melding aan de BVA bij incidenten en bij het compromitteren van bijzonder informatie.
  - is aanspreekpunt voor Commissie van Onderzoek ingeval van onderzoek;
  - voert jaarlijks een onderzoek uit naar de deugdelijkheid van de beveiliging van bijzondere informatie;
  - rapporteert zijn bevindingen samen met een samenvatting van de jaarlijkse rapportage van het lijnmanagement met betrekking tot bijzondere informatie via de BVA aan de PSG.
- ziet toe op de fysieke beveiliging, treedt in dat kader ondermeer op als aanspreekpunt m.b.t. de rijkspas.

De CSO is tevens aanspreekpunt op het gebied van integriteit. In de Gedragscode Integriteit OCW, de gedragscode van DUO en andere

regelingen (zoals gebruik internet en e-mail) zijn basisafspraken vastgelegd over wat wel en wat niet mag.
De CSO fungeert in dit kader als:

- onafhankelijk vertrouwenspersoon;
- meldpunt voor medewerkers die een vermoeden van een misstand willen melden. Hij kan hen op verzoek een eerste opvang bieden, van advies dienen en eventueel verdere hulp bieden.

DUO Decentrale Security Officer (DSO)
Voert onder verantwoordelijkheid en in opdracht van de CSO activiteiten op het terrein van de informatiebeveiliging uit:

- levert een bijdrage aan de ontwikkeling, de formulering en de actualisering van beleid en richtlijnen op het gebied van fysieke beveiliging en informatiebeveiliging ten behoeve DUO en is zich hierbij bewust van de weerstand die overwonnen moet worden om dit beleid te laten naleven;
- ontwikkelt richtlijnen voor het toepassen en uitvoeren van het informatiebeveiligingsbeleid, zowel interdepartementaal als binnen OCW-DUO;
- toetst opzet en bestaan van informatiebeveiligingsmaatregelen en rapporteert hierover;
- beoordeelt voorgestelde beveiligingsmaatregelen op opzet, bestaan en werking;
- adviseert het tactisch en operationeel management gevraagd en ongevraagd bij het uitvoeren van het informatiebeveiligingsbeleid, onder meer bij het onderhoud van bestaande systemen en het ontwikkelen van nieuwe informatiesystemen;
- voert risicoanalyses (A&K) uit van operationele processen en bedrijfssystemen, zowel intern als bij ketenpartners, met het oog op informatiebeveiliging in de ruimste zin van het woord en zo nodig met gebruik van een tool zoals CRAMM;
- formuleert en initieert verbetervoorstellen conform het vastgestelde beveiligingsprofiel en voortkomend uit risicoanalyses en ziet toe op de realisatie, houdt hierbij rekening met eventuele politieke gevoeligheden;
- levert een bijdrage aan de ontwikkeling, het formuleren en het actualiseren van beleid en richtlijnen op het gebied van bedrijfsrisico's en continuïteitsvoorzieningen;
- vertegenwoordigt DUO bij externe instanties op informatiebeveiligingsterrein;
- draagt zorg voor veiligheidsbewustzijn en communicatie onder meer door het verzorgen van trainingen aan (nieuwe) medewerkers op het gebied van informatiebeveiliging.

Functionaris Gegevensbescherming (FG)
De functionaris voor de gegevensbescherming (FG) houdt binnen de organisatie toezicht op de toepassing en naleving van de Wet bescherming persoonsgegevens (WBP) in overeenstemming met de richtlijnen van het College Bescherming Persoonsgegevens (CBP).
De FG heeft onder andere de volgende taken:

- toezicht houden;
- klachtenbehandeling;
- verslaggeving;
- ontwikkelen van interne regelingen.

DUO Privacy Officers (PO)

DUO voert in opdracht van OCW, BZK en van de Europese Commissie taken uit die bijna het hele onderwijsveld raken. Het uitvoeren van de wetten en regelingen waarin deze taken zijn vastgelegd brengt met zich mee dat vele gegevens moeten worden verwerkt, waaronder veel persoonsgegevens. In juridisch en maatschappelijk opzicht is de organisatie verplicht om garanties af te geven ten aanzien van de bescherming van persoonsgegevens.
In het prestatiecontract dat de huidige DUO heeft afgesloten met het ministerie **BZK** staat dat DUO, conform de Wet bescherming persoonsgegevens acteert.
De privacy officer voert in de praktijk taken uit op het taakgebied van de bescherming van persoonsgegevens:

- fungeert als centraal aanspreekpunt op het gebied van de bescherming van persoonsgegevens;
- initieert en werkt mee aan het ontwikkelen en actualiseren van OCW-DUO-breed beleid, richtlijnen, instructies en procedures op het gebied van de bescherming van persoonsgegevens;
- toetst bestaande wet- en regelgeving aan de kaders van de Wet bescherming persoonsgegevens;
- verzorgt mondelinge instructies en presentaties op het gebied van de bescherming van persoonsgegevens;
- adviseert bij verzoeken om inzage van individuele klanten en medewerkers (rechten van betrokkenen);
- werkt mee aan uitvoeringstoetsen i.v.m. privacywetgeving;
- monitort de procedures met betrekking tot privacy-aspecten en initieert voor zover nodig wijzigingen;
- vertegenwoordigt OCW-DUO bij externe instanties op het gebied van de bescherming van persoonsgegevens en onderhoudt contacten met in- en externe overlegorganen op het vakgebied;
- adviseert het tactisch en operationeel management gevraagd en ongevraagd over de bescherming van persoonsgegevens;
- werkt mee aan het optimaliseren van ketenprocessen;
- adviseert bij afhandeling van klachten op het gebied van de bescherming van persoonsgegevens tevens gericht op vermindering of preventie van de klachten in de toekomst.

DUO Lijnmanager/proceseigenaar

- neemt de DUO-brede gestelde eisen en randvoorwaarden voor informatiebeveiliging in acht;
- is verantwoordelijk voor de uitvoering van het informatiebeveiligingsbeleid binnen zijn onderdeel, alsmede van het informatiebeveiligingsbeleid voor de ketens waar zijn onderdeel deel van uit maakt;
- stelt aan de hand van de richtlijnen de betrouwbaarheidseisen voor elk informatiesysteem dat behoort tot zijn organisatieonderdeel vast. Kiest en beschrijft op grond daarvan een samenhangend pakket van bijbehorende maatregelen;
- stelt vast dat getroffen maatregelen aantoonbaar overeenstemmen met de betrouwbaarheidseisen en dat de maatregelen worden nageleefd; de vaststelling heeft de aard van een controle op de werking van de informatiebeveiliging;
- is verantwoordelijk voor het onderhoud en beheer van de vastgestelde betrouwbaarheidseisen en maatregelen;
- draagt zorg voor de implementatie van de beveiligingsmaatregelen en evalueert deze periodiek;

- betrekt de CSO bij de informatiebeveiliging van (de te implementeren) interdepartementale systemen;
- stelt bedrijfscontinuïteitsdeelplannen op voor de processen die onder zijn verantwoordelijkheid vallen, conform het door de CSO aangeleverde format;
- zorgt dat de tot zijn organisatieonderdeel behorende medewerkers zorgvuldig met informatie omgaan en zich bewust zijn van de risico's die op dit terrein aanwezig zijn;
- vraagt aan de leiding van het departement om een onderzoek uit te voeren bij vermoeden van overtreding van de gedragscode e-mail- en internetgebruik, of schending van integriteit of vertrouwelijkheid van informatie en meldt dit aan de CSO;
- meldt (het voornemen tot) werken met bijzondere informatie (stg. en dept. vertrouwelijk) bij de CSO;
- rapporteert ieder jaar over de beveiliging van bijzondere informatie aan de CSO;
- rapporteert aan de CSO over wijzigingen in de persoonlijke omstandigheden van medewerkers die voor de beveiliging van bijzondere informatie van belang kunnen zijn.

DUO ICT-algemeen

- legt de standaard dienstverlening vast in een Service Level Agreement (SLA);
- richt de beheerprocessen van de ICT-dienstverlening in volgens ITIL3 of vergelijkbare procesinrichting;
- Maakt bij uitbesteding van de ICT:
  - afspraken met en stuurt externe dienstverleners aan op het terrein van informatiebeveiliging;
  - test (laat testen) de effectiviteit van de genomen beveiligingsmaatregelen genomen door de (externe) dienstverleners (audit);
- meldt informatiebeveiligingsincidenten bij de CSO en werkt mee aan onderzoeken bij voorgevallen incidenten;
- signaleert, bij het voornemen van het in productie nemen van een informatiesysteem het ontbreken van een risicoafweging (en indien van toepassing beveiligingsplan) aan de verantwoordelijke lijnmanager;
- signaleert aan een lijnmanager systeemwijzigingen (functioneel en technisch) die invloed op de informatiebeveiliging kunnen hebben;
- vraagt advies aan de CSO bij onderwerpen op het terrein van de informatiebeveiliging die interdepartementaal aan de orde zijn;
- ziet toe op het door leveranciers naleven van de beveiliging van de technische infrastructuur en van de ICT-voorzieningen, conform normen.

DUO ICT-specifiek

Het in productie nemen van een nieuwe dan wel vernieuwde applicatie is pas toegestaan, nadat dICT en de CSO hier beiden toestemming voor hebben verleend.
ICT/I&E/Beveiliging controleert daarom nieuwe dan wel vernieuwde applicaties op risico's uit het deelgebied informatiebeveiliging. Hierbij worden de risico's ten aanzien van beschikbaarheid, exclusiviteit en integriteit in kaart gebracht. Daarbij maakt de specialist informatiebeveiliging een risicoafweging ten aanzien van zijn bevindingen. Hij doet dit actief door het uitvoeren van hacktesten op nieuwe dan wel

vernieuwde applicaties als pro-actief door samen met ICT/Softwarehuis geautomatiseerde Source Code Review te introduceren. Dit zal een inhoudelijke kwaliteitsverbetering van de sourcecode betekenen, waardoor het aantal bevindingen bij hacktesten en eventuele niet ontdekte zwakheden vermindert.
Bij ernstige risico's is goedkeuring nodig van het management. In bijzondere gevallen, zoals bij het achterwege laten van een hacktest of het niet kunnen garanderen van adequate beveiliging, is goedkeuring nodig van de DG.
dICT belegt bij ICT/I&E/Beveiliging:

- het uitvoeren van de daadwerkelijke hacktest;
- het opstellen de richtlijnen voor dergelijke testen.

DUO Medewerker

- is verantwoordelijk voor het zorgvuldig omgaan met de toevertrouwde informatie, ICT-middelen en de daarop van toepassingzijnde informatiebeveiligingsmaatregelen;
- volgt de aanwijzingen/maatregelen op van zijn leidinggevende en coördinator informatie-beveiliging;
- de uitvoering van het clean-deskbeleid voor wat betreft de directe werkomgeving;
- meldt incidenten, overtredingen of zwakke plekken op het terrein van de informatiebeveiliging aan zijn leidinggevende of aan de Centrale Security Officer.

DUO FD (DUO2-Receptie/Bewaking)

De eigenaar van het kantoorgebouw Kempkensberg 12 is verantwoordelijk voor de uitvoering van de fysieke beveiliging. De FD fungeert als opdrachtgever-contactpersoon, de bewaking en de receptie zijn met de daadwerkelijke uitvoering belast.

OCW Commissie van onderzoek

- wordt ingeval van compromittering van een staatsgeheim, ad hoc en tijdelijk samengesteld door de DG;
- bestaat voor wat betreft DUO uit de CSO en/of de DSO en ambtenaren die niet betrokken zijn bij de compromittering en niet ondergeschikt zijn aan de bij de compromittering betrokken ambtenaar eventueel aangevuld met externe deskundigen;
- doet onderzoek naar mogelijkheid tot de zich voorgedane compromittering, omvang en schade van het incident, en mogelijke maatregelen om schade te beperken en/of herhaling te voorkomen.

3. Informatiebeveiliging

3.1 Wat is informatiebeveiliging?

Informatie is een bedrijfsmiddel dat, net als andere belangrijke bedrijfsmiddelen, waarde heeft voor DUO en voortdurend op een passende manier beveiligd moet zijn. Informatiebeveiliging beschermt informatie tegen een breed scala aan bedreigingen, om de continuïteit van de bedrijfsvoering te waarborgen, de schade voor DUO te minimaliseren en het rendement op investeringen en de kansen van DUO te optimaliseren.

Informatie komt in veel vormen voor. Het kan afgedrukt of geschreven zijn op papier, elektronisch opgeslagen zijn, per post of via elektronische media worden verzonden, getoond worden in films of in gesproken vorm gebracht. Welke vorm de informatie ook heeft, of op welke manier ze ook wordt gedeeld of verzonden, ze moet altijd passend beveiligd zijn.

Informatiebeveiliging wordt gekarakteriseerd als het waarborgen van:

- **Vertrouwelijkheid**: informatie is alleen toegankelijk voor degenen, die hiertoe geautoriseerd zijn[3];
- **Integriteit**: informatie verwerking zijn correctheid en volledig;
- **Beschikbaarheid**: geautoriseerde gebruikers hebben op de juiste momenten tijdig toegang tot informatie en aanverwante bedrijfs-middelen.

Informatie wordt beveiligd door een passende verzameling beveiligings-maatregelen in te zetten, bijvoorbeeld beleid, gedragsregels, procedures, organisatiestructuren en softwarefuncties. Deze beveiligingsmaatregelen stellen we vast om te waarborgen dat de specifieke beveiligings-doelstellingen van de DUO worden bereikt.

3.2 Waarom informatiebeveiliging nodig is

Informatie en de ondersteunende processen, systemen en netwerken zijn belangrijke bedrijfsmiddelen voor de DUO. De beschikbaarheid, integriteit en vertrouwelijkheid ervan kunnen van essentieel belang zijn voor het behoud van de (financiële) relatie met de klanten, de naleving van de wet en het imago van de DUO.

In toenemende mate worden de DUO, haar informatiesystemen en netwerken geconfronteerd met beveiligingsrisico's, zoals computerfraude en vandalisme. Nieuwe oorzaken van schade, zoals computervirussen, computerhacking en het (ver)hinderen van dienstverlening komen steeds vaker voor, worden steeds ambitieuzer en steeds meer verfijnd.

Afhankelijk van informatiesystemen en -diensten zijnde, betekent dat, dat DUO steeds kwetsbaarder wordt voor bedreigingen van de beveiliging. De onderlinge verbondenheid van openbare en private netwerken en het delen van informatiemiddelen maken het steeds moeilijker en noodzakelijker om

[3] Dit impliceert dat het afleggen van de Eed of Belofte geen reden is om alle systemen intern 'open' te zetten. Toegang tot informatie dient relevant te zijn voor de functie uitvoering.

de toegang in brede zin te beveiligen. De trend van gedistribueerde gegevensverwerking heeft de doeltreffendheid van centrale, specialistische sturing verzwakt.

Veel informatiesystemen zijn niet ontworpen met het oog op veiligheid. De beveiliging die met technische middelen kan worden bereikt is begrensd en moet worden ondersteund door passend beheer en procedures. Om te bepalen welke beveiligingsmaatregelen gebruikt moeten worden is, een zorgvuldige planning nodig en aandacht voor het detail. Management van informatiebeveiliging verlangt tenminste de inzet van alle medewerkers van de DUO. Bovendien kan deelname van leveranciers en klanten vereist zijn. Ook kan er specialistisch advies van externe organisaties nodig zijn.

De DUO heeft in toenemende mate te maken met ketenpartners. Dit brengt extra risico's met zich mee. Om de eigen standaard in stand te kunnen houden stelt de DUO ook hoge eisen aan de ketenpartners. Dit is vastgelegd in de (standaard-) overeenkomsten die Inkoop opstelt in overleg met de toeleverende en afnemende partners in het veld.
In principe is de baseline van toepassing op alle kanalen waarmee de toegang tot de DUO wordt gerealiseerd. Een notitie hierover is in ontwikkeling. Voor nadere informatie kunt u zich wenden tot één van de DSO's.

Beveiligingsmaatregelen zijn aanzienlijk goedkoper en doeltreffender wanneer deze meegenomen kunnen worden tijdens het opstellen van de specificatie van eisen in de ontwerpfase van informatiesystemen.

Incidenteel worden beveiligingseisen ingevoerd die het gevolg zijn van recente beveiligingsincidenten elders.

3.3 Het opstellen van beveiligingseisen

Het is van essentieel belang dat DUO haar beveiligingsbehoeften bepaalt. Er zijn drie hoofdbronnen.

De **eerste** bron wordt ontleend aan de beoordeling van de informatiebeveiligingsrisico's voor de DUO. Via risicoanalyses worden de bedreigingen ten aanzien van bedrijfsmiddelen vastgesteld, de kwetsbaarheid voor en waarschijnlijkheid van het optreden hiervan beoordeeld en de potentiële effecten geschat.

De **tweede** bron wordt gevormd door de wettelijke, statutaire, regulerende en contractuele eisen waaraan de organisatie, haar ketenpartners, leveranciers en dienstverlenende bedrijven dienen te voldoen.

De **derde** bron van eisen wordt gevormd door het eigen stelsel van principes, doelstellingen en eisen voor het verwerken van informatie, die DUO heeft ontwikkeld ter ondersteuning van haar eigen bedrijfsvoering en de bedrijfsvoering in de keten van de dienstverlening.

3.4 Inschatting van beveiligingsrisico's

Beveiligingsbehoeften worden bepaald aan de hand van een methodische beoordeling van beveiligingsrisico's. De kosten van beveiligingsmaatregelen

moeten worden afgewogen tegen de bedrijfsschade die zou kunnen ontstaan door beveiligingsincidenten.
Technieken voor risicoanalyse kunnen worden toegepast op de DUO als geheel, of op delen ervan, evenals op afzonderlijke informatiesystemen, specifieke systeemcomponenten of -diensten wanneer dit praktisch, realistisch en nuttig is.
Risicoanalyse is het systematisch beoordelen van:

I. de schade voor de DUO die waarschijnlijk zal ontstaan door een beveiligingsincident, rekening houdend met de mogelijke gevolgen indien de vertrouwelijkheid (exclusiviteit), integriteit en beschikbaarheid van de informatie en andere bedrijfsmiddelen worden geschonden;
II. de waarschijnlijkheid dat een dergelijk beveiligingsincident optreedt in het licht van de aanwezige bedreigingen, kwetsbaarheden en de getroffen maatregelen.

De resultaten van de analyse worden gebruikt om te bepalen welke activiteiten het management moet ondernemen en welke prioriteiten het moet stellen ten aanzien van het beheer van beveiligingsrisico's en het implementeren van de gekozen maatregelen ter bescherming tegen deze risico's. Soms kan het nodig zijn om het proces van risicoanalyse en van maatregelen kiezen te herhalen, voor verschillende delen van de organisatie of voor individuele informatiesystemen.

Het is belangrijk om de beveiligingsrisico's en geïmplementeerde maatregelen periodiek te evalueren, om:

I. in te kunnen spelen op wijzigingen in bedrijfsbehoeften en prioriteiten;
II. nieuwe bedreigingen en kwetsbaarheden te bepalen;
III. te bevestigen dat maatregelen nog steeds effectief en geschikt zijn.

4. Maatregelen bepalen

Wanneer de beveiligingsbehoeften eenmaal zijn vastgesteld, worden maatregelen bepaald en geïmplementeerd om te waarborgen dat de risico's tot een aanvaardbaar niveau worden gereduceerd. Maatregelen kunnen worden geselecteerd uit dit document of uit andere bronnen, of er kunnen geheel nieuwe maatregelen worden ontworpen om aan specifieke behoeften te voldoen. Er zijn veel verschillende manieren om met risico's om te gaan en dit document bevat voorbeelden van gangbare benaderingen.

Het is echter van belang om te onderkennen dat sommige maatregelen niet van toepassing zijn op elk informatiesysteem of elke omgeving en niet voor elk onderdeel van de organisatie bruikbaar zijn. Paragraaf 10.1.3 beschrijft bijvoorbeeld hoe functiescheiding kan worden toegepast, om fraude en fouten te voorkomen. In kleinere onderdelen van een organisatie zal het wellicht niet mogelijk zijn om alle functies te scheiden, zodat het daar noodzakelijk is om op een alternatieve wijze dezelfde beveiligings-doelstellingen te realiseren.

Maatregelen moeten worden gekozen op basis van hoe de kosten van implementatie zich verhouden tot de risico's die ermee worden bestreden en de potentiële schade wanneer de beveiliging wordt geschonden. Ook immateriële factoren, zoals aantasting van de goede naam van de DUO, moeten in overweging worden genomen.

5. Hoe begint informatiebeveiliging?

Een aantal maatregelen kan worden beschouwd als basisprincipe, dat een goed vertrekpunt biedt voor het implementeren van informatiebeveiliging. Ze zijn gebaseerd op essentiële wettelijke eisen of ze worden algemeen beschouwd als “best practice” voor informatiebeveiliging.

Tot de maatregelen die vanuit wettelijk oogpunt van essentieel belang zijn voor een organisatie behoren:

I. intellectuele eigendomsrechten (zie 15.1.2);
II. beveiliging van specifieke bedrijfsdocumenten (zie 15.1.3);
III. bescherming van persoonlijke informatie (zie 15.1.4).

Tot de maatregelen die worden beschouwd als “best practice” voor informatiebeveiliging behoren:

I. het maken van een gedegen beleidsdocument voor informatiebeveiliging (zie 5.1.1);
II. toewijzing van verantwoordelijkheden voor informatie-beveiliging (zie 6.1.3);
III. opleiding en training voor informatiebeveiliging (zie 8.2.2);
IV. het rapporteren van beveiligingsincidenten (zie hoofdstuk 13);
V. continuïteitsmanagement (zie hoofdstuk 14).

Deze maatregelen gelden voor geheel DUO. Hoewel alle maatregelen in dit document belangrijk zijn, moet de relevantie van een maatregel altijd worden vastgesteld in het licht van de specifieke risico’s voor het organisatieonderdeel. Hoewel de bovengenoemde benadering dus een goed vertrekpunt is, komt zij niet in de plaats van het selecteren van maatregelen op basis van risicoanalyse. (A&K)

5.1 Leeswijzer

Zoals eerder aangegeven bestaat het Informatiebeveiligingplan uit twee delen. De verkorte versie met daarin aangegeven welke maatregelen uit de Code van toepassing zijn en de uitgebreide versie waarin per maatregel de toelichting en een uitgebreide beschrijving staat opgenomen zoals verwoord in de Code zelf.

De opbouw van hoofdstukken met de maatregelen in beide documenten is als volgt:

A. 6	Organisatie van informatiebeveiliging

= hoofdstukken
Dit zijn de hoofdstukken onderverdeeld in de elf aandachtsgebieden van de Code.

A. 6.1	Interne organisatie

= paragraaf

A. 6.1.1	Betrokkenheid van de directie bij informatiebeveiliging

= subparagraaf
De onderverdeling van de hoofdstukken.

A. 6.1.1.a	Het beveiligingsforum dient op basis van een overeengekomen agenda te functioneren, zodanig dat alle relevante onderwerpen aandacht krijgen.

= de feitelijke maatregel

Zo is de opbouw van de codering van de maatregel
A . hoofdstuk . paragraaf . sub-paragraaf . maategel

De tekst is de letterlijke tekst uit de code.

6. Beveiligingsbeleid

Code	Maatregel
A. 5	Beveiligingsbeleid
A. 5.1	Informatiebeveiligingsbeleid
A. 5.1.1	Beleidsdocument voor informatiebeveiliging
A. 5.1.1.a	De organisatie dient over een gedocumenteerd en goedgekeurd (ICT-)beveiligingsbeleid te beschikken.
A. 5.1.2	Beoordeling van het informatiebeveiligingbeleid
A. 5.1.2.a	Het beveiligingsbeleid moet actueel gehouden worden.

7. Organisatie van informatiebeveiliging

Code	Maatregel
A. 6	Organisatie van informatiebeveiliging
A. 6.1	Interne organisatie
A. 6.1.1	Betrokkenheid van de directie bij informatiebeveiliging
A. 6.1.1.a	Het beveiligingsforum dient op basis van een overeengekomen agenda te functioneren, zodanig dat alle relevante onderwerpen aandacht krijgen.
A. 6.1.2	Coördinatie van informatiebeveiliging
A. 6.1.2.a	Zorg voor mechanismen om een tijdelijk verhoogd dreigingniveau te herkennen en implementeer procedures om de staat van paraatheid te verhogen.
A. 6.1.2.b	Al het betrokken personeel moet worden geïnformeerd omtrent de te verzamelen gegevens bij een bommelding.
A. 6.1.3	Toewijzing van verantwoordelijkheden voor informatiebeveiliging
A. 6.1.3.a	Alle informatiebeveiliging verantwoordelijkheden dienen helder te zijn gedefinieerd.
A. 6.1.4	Goedkeuringsproces voor IT-voorzieningen
A. 6.1.4.a	De installatie van ICT-voorzieningen moet technisch goedgekeurd en geautoriseerd zijn.
A. 6.1.5	Geheimhoudingsovereenkomst
A. 6.1.5.a	Personeel en contractanten moeten een geheimhoudingsverklaring tekenen.
A. 6.1.6	Contact met overheidsinstanties
A. 6.1.6.a	Houdt contact met autoriteiten.
A. 6.1.7	Contact met speciale belangengroepen
A. 6.1.7.a	Win het advies van een specialist in over het uitvoeren van een onderzoek op de locatie om alle kwetsbare plekken op te sporen en documenteer deze kwetsbare plekken.
A. 6.1.7.b	Win advies in van beveiligingsspecialisten.
A. 6.1.7.c	Beveiligingsspecialisten dienen samen te werken met andere specialisten.
A. 6.1.8	Onafhankelijke beoordeling van informatiebeveiliging
A. 6.1.8.a	Implementatie van informatiebeveiliging dient onafhankelijk te worden gecontroleerd.
A. 6.2	Externe partijen
A. 6.2.1	Identificatie van risico's die betrekking hebben op externe partijen
A. 6.2.1.a	De beveiliging van ICT-voorzieningen en informatiecomponenten waartoe derden toegang hebben moet in stand worden gehouden.
A. 6.2.2	Beveiliging behandelen in de omgang met klanten
A. 6.2.2.a	De hoeveelheid informatie toegankelijk voor klanten dient te zijn gedefinieerd.
A. 6.2.3	Beveiliging behandelen in overeenkomsten met een derde partij
A. 6.2.3.a	Derde partij overeenkomsten dienen beveiligingsrichtlijnen te bevatten.

8. Beheer van bedrijfsmiddelen

Code	Maatregel
A. 7	Beheer van bedrijfsmiddelen
A. 7.1	Verantwoordelijkheid voor bedrijfsmiddelen
A. 7.1.1	Inventarisatie van bedrijfsmiddelen
A. 7.1.1.a	Alle belangrijke informatiecomponenten dienen in een registratie te worden opgenomen.
A. 7.1.1.b	Er moet een nauwkeurige inventaris van het netwerk en zijn onderdelen worden bijgehouden.
A. 7.1.1.c	Inventariseer regelmatig meet- en regelapparatuur.
A. 7.1.1.d	De organisatie moet het merken als een diefstal wordt of is gepleegd.
A. 7.1.2	Eigendom van bedrijfsmiddelen
A. 7.1.2.a	Toegang tot gegevens moet door aangewezen "gegevenseigenaren" worden geregeld.
A. 7.1.3	Aanvaardbaar gebruik van bedrijfsmiddelen
A. 7.1.3.a	Aan alle gebruikers moet worden meegedeeld dat ze geen misbruik van elektronische post mogen maken.
A. 7.1.3.b	Alle gebruikers moet worden meegedeeld dat faciliteiten om op het internet te bladeren uitsluitend voor toegestane doeleinden bedoeld zijn.
A. 7.2	Classificatie van informatie
A. 7.2.1	Richtlijnen voor het classificeren
A. 7.2.2	Labeling en verwerking van informatie
A. 7.2.2.a	Alle ICT-hulpbronnen bevatten labels waarop het niveau van vertrouwelijkheid dat de ICT-hulpbron mag behandelen vermeld staat.
A. 7.2.2.d	Het moet mogelijk zijn om de volledigheid van de printuitvoer te controleren.

9. Beveiliging van personeel

Code	Maatregel
A. 8	Beveiliging van personeel
A. 8.1	Voorafgaand aan het dienstverband
A. 8.1.1	Rollen en verantwoordelijkheden
A. 8.1.2	Screening
A. 8.1.2.c	Zorg ervoor dat personeeldossiers die screeningsgegevens bevatten veilig worden bewaard.
A. 8.1.3	Arbeidsvoorwaarden
A. 8.1.3.a	Arbeidsovereenkomsten moeten volledige functiebeschrijvingen bevatten.
A. 8.2	Tijdens het dienstverband
A. 8.2.1	Directieverantwoordelijkheid
A. 8.2.1.a	Informatiebeveiliging dient een gestuurd (gemanaged) proces binnen een organisatie te zijn.
A. 8.2.2	Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging
A. 8.2.2.a	Het personeel moet weten wat het moet doen bij een bomalarm.
A. 8.2.2.c	Definieer een scholings- en trainingsstrategie op het gebied van beveiliging.
A. 8.2.2.d	Het personeel moet zich bewust zijn van beveiligingskwesties rondom ICT-systemen.
A. 8.2.3	Disciplinaire maatregelen
A. 8.2.3.a	Er moet een disciplinair proces zijn om beveiligingsincidenten af te handelen.
A. 8.3	Beëindiging of wijziging van dienstverband
A. 8.3.1	Beëindiging van verantwoordelijkheden
A. 8.3.1.a	De opzegtermijn dient te zijn opgenomen in het arbeidscontract.
A. 8.3.2	Retournering van bedrijfsmiddelen
A. 8.3.2.a	Alle organisatie eigendom dient te worden geretourneerd als de medewerker de organisatie verlaat.
A. 8.3.3	Blokkering van toegangsrechten
A. 8.3.3.a	Toegangsrechten dienen te worden aangepast indien een gebruiker vertrekt of van rol veranderd.

10. Fysieke beveiliging en beveiliging van de omgeving

Code	Maatregel
A. 9	Fysieke beveiliging en beveiliging van de omgeving
A. 9.1	Beveiligde ruimten
A. 9.1.1	Fysieke beveiliging van de omgeving
A. 9.1.1.a	Het gebouw moet enige weerstand bieden bij een gewelddadige aanval.
A. 9.1.1.d	De toegangsdeuren tot het gebouw moeten enige weerstand bieden aan een gewelddadige aanval.
A. 9.1.1.e	Houd het aantal ingangen naar het gebouw zo klein mogelijk.
A. 9.1.1.h	Reguleer de toegang tot het gebouw.
A. 9.1.1.i	Men moet het gebouw binnengaan via een bemande ontvangstruimte.
A. 9.1.2	Fysieke toegangsbeveiliging
A. 9.1.2.a	Toegang tot het gebouw mag alleen worden verleend aan mensen met een geldige pas of badge.
A. 9.1.2.b	De uitgifte van personeelspasjes moet goed geregeld zijn.
A. 9.1.2.d	Het pasje moet moeilijk na te maken zijn.
A. 9.1.2.f	Een persoonsgebonden pas moet de foto bevatten van de persoon aan wie de pas is uitgereikt.
A. 9.1.2.g	Toegang tot het gebouw moet worden gecontroleerd door een geautomatiseerd toegangscontrolesysteem.
A. 9.1.2.h	Toegang tot het gebouw moet worden gecontroleerd door een elektronisch toegangscontrolesysteem dat een passend beveiligingsniveau biedt.
A. 9.1.3	Beveiliging van kantoren, ruimten en faciliteiten
A. 9.1.3.b	De ramen van het gebouw moeten enige weerstand bieden aan een inbraakpoging.
A. 9.1.3.c	De ramen van het gebouw moeten weerstand bieden aan een inbraakpoging.
A. 9.1.3.e	Installeer een alarmsysteem waarmee een extern alarmsignaal wordt gegeven.
A. 9.1.3.f	Het alarmsysteem moet blijven werken, zelfs als de indringer enige kennis van alarmsystemen heeft.
A. 9.1.3.g	Het alarmsysteem moet blijven werken, zelfs als de indringer vertrouwd is met indringerdetectiesystemen en verschillende gereedschappen tot zijn beschikking heeft.
A. 9.1.3.h	Het alarmsysteem moet blijven werken, zelfs als de indringer een volledige set apparatuur tot zijn beschikking heeft waarmee hij kritieke systeemcomponenten kan vervangen.
A. 9.1.3.j	Reik schriftelijke beveiligingsinstructies uit aan de bewakers.
A. 9.1.3.t	Sleutels moeten alleen beschikbaar zijn voor geautoriseerde personen.
A. 9.1.3.u	Er moeten maatregelen zijn om diefstal van bedrijfsmiddelen te voorkomen.
A. 9.1.3.v	ICT-apparatuur moet fysiek worden beveiligd indien niet gebruikt.
A. 9.1.3.w	Brand moet in een vroeg stadium ontdekt en gemeld worden.
A. 9.1.3.x	Neem fysieke maatregelen om uitbreiding van brand zoveel mogelijk tegen te gaan.
A. 9.1.4	Bescherming tegen bedreigingen van buitenaf
A. 9.1.4.a	Eigendommen dienen tegen verlies en schade verzekerd te worden.
A. 9.1.4.b	Bij brand moet al het personeel veilig worden geëvacueerd.
A. 9.1.4.c	Er moet een brandpreventieprogramma zijn.
A. 9.1.4.d	Wanneer ongewenst water het gebouw binnenkomt, moet verspreiding ervan zoveel mogelijk worden tegengegaan.
A. 9.1.4.e	Het binnendringen van water moet worden voorkomen.
A. 9.1.4.g	Het gebouw moet worden beveiligd tegen blikseminslag.
A. 9.1.5	Werken in beveiligde ruimten
A. 9.1.5.a	Toegang van onderhoudspersoneel moet gecontroleerd worden.
A. 9.1.5.b	Bij het werken in een beveiligd gebied dient men zich aan de maatregelen en richtlijnen te houden die bedoeld zijn om de beveiliging zoals die door fysieke middelen wordt geboden, te verbeteren.
A. 9.1.6	Openbare toegang en gebieden voor laden en lossen
A. 9.1.6.a	Goederen moeten in een aparte ruimte worden afgeleverd.
A. 9.1.6.c	Onderwerp bezorgingen buiten kantooruren aan strikte procedures en houd ze weg van kritieke ruimtes.
A. 9.1.6.d	Goederen moeten in een aparte ruimte worden afgeleverd.
A. 9.2	Beveiliging van apparatuur
A. 9.2.1	Plaatsing en bescherming van apparatuur
A. 9.2.1.a	Houd fysieke toegang tot netwerkapparaten in de hand.
A. 9.2.1.b	Alle ongebruikte meet- en regelapparatuur moet veilig opgeborgen worden.
A. 9.2.1.c	Alleen geautoriseerde gebruikers mogen meet- en regelapparatuur gebruiken.
A. 9.2.1.d	Controleer het gebruik van meet- en regelapparatuur om na te gaan of er geen misbruik van wordt gemaakt.
A. 9.2.1.e	Verleen alleen aan geautoriseerd personeel toegang tot apparatuur voor netwerkbeheer.
A. 9.2.1.f	De specificaties van de fabrikant voor operationele ruimtes moeten worden nageleefd.
A. 9.2.1.g	Plaatsing van apparatuur dient risico's ten gevolge van omgevingsbedreigingen en ongeautoriseerde toegang te verminderen.
A. 9.2.1.j	De ICT-apparatuur moet op een ononderbroken voeding (UPS) worden aangesloten.

Code	Maatregel
A. 9.2.2	Nutsvoorzieningen
A. 9.2.2.a	Voorzie ICT-apparatuur van een adequate, geconditioneerde stroomvoorziening.
A. 9.2.2.b	De voeding moet in noodgevallen onder controle zijn.
A. 9.2.2.e	Bewaak de werking van het klimaatbeheersingssysteem.
A. 9.2.3	Beveiliging van kabels
A. 9.2.3.a	De infrastructuur van de netwerkbekabeling moet actief worden beheerd.
A. 9.2.3.b	Leg de kabels op zo'n manier uit dat ze bestand zijn tegen storingen.
A. 9.2.3.c	Elektrische apparatuur moet volgens de geldende regels worden geïnstalleerd.
A. 9.2.4	Onderhoud van apparatuur
A. 9.2.4.a	Sluit voor alle onmisbare apparatuur een onderhoudscontract af.
A. 9.2.4.c	Monitor het gebruik van apparatuur om de kans op storingen zo klein mogelijk te houden.
A. 9.2.4.d	Verzorg het onderhoud van apparatuur.
A. 9.2.4.e	Bij uitval van apparatuur moeten de hinderlijke gevolgen zo klein mogelijk zijn.
A. 9.2.4.f	Storingen aan apparatuur moeten gedetecteerd worden.
A. 9.2.4.g	Er moet onderhoud aan voorzieningen die de werkomgeving ondersteunen plaatsvinden.
A. 9.2.5	Beveiliging van apparatuur buiten het terrein
A. 9.2.5.a	Voor elk middel dat voor het verwerken van informatie wordt gebruikt moet goedkeuring door leidinggevenden worden verleend, ongeacht wie de eigenaar is.
A. 9.2.6	Veilig verwijderen en hergebruiken van apparatuur
A. 9.2.6.a	Verwijder of overschrijf alle gegevens en vertrouwelijke toepassingsprogrammatuur als ze niet langer nodig zijn, met name voor reparatie of het afstoten van de gegevensdragers.
A. 9.2.6.b	Overschrijf of verwijder alle gegevens en vertrouwelijke toepassingsprogrammatuur op de juiste manier als ze niet langer nodig zijn, en voor reparatie of het afstoten van de betreffende gegevensdragers.
A. 9.2.7	Verwijdering van bedrijfseigendommen
A. 9.2.7.a	Apparatuur dient alleen na schriftelijke toestemming van de locatie te kunnen worden afgevoerd.

11. Beheer van communicatie- en bedienings-processen

Code	Maatregel
A.10	Beheer van communicatie- en bedieningsprocessen
A.10.1	Bedieningsprocedures en verantwoordelijkheden
A.10.1.1	Gedocumenteerde bedieningsprocedures
A.10.1.1.a	Stel operatorprocedures op waarin alle handelingen van de operators zijn beschreven.
A.10.1.1.b	Werkzaamheden aan het netwerk moeten op gecontroleerde wijze plaatsvinden.
A.10.1.2	Wijzigingsbeheer
A.10.1.2.a	Voor alle modems moet toestemming zijn verleend.
A.10.1.2.b	Wijzigingen in de ICT-voorzieningen moeten gecontroleerd worden doorgevoerd.
A.10.1.3	Functiescheiding
A.10.1.3.a	Zorg ervoor dat de kans dat het bedieningspersoneel het systeem misbruikt zo klein mogelijk is.
A.10.1.4	Scheiding van faciliteiten voor ontwikkeling, testen en productie
A.10.1.4.a	Alle betrokken partijen moeten alle wijzigingen aan toepassingen goedkeuren.
A.10.1.4.b	Personeelsprocedures moeten een adequate ontwikkelomgeving ondersteunen c.q. erop aansluiten.
A.10.1.4.c	Er dienen aparte test- en productieomgevingen te zijn.
A.10.1.4.d	Tref maatregelen om gebruikersfouten te voorkomen.
A.10.2	Beheer van de dienstverlening door een derde partij
A.10.2.1	Dienstverlening
A.10.2.1.a	Men dient de risico's die het inschakelen van een externe partij voor het beheren van gegevens verwerkende voorzieningen met zich meebrengt, te onderkennen en dienovereenkomstig te handelen.
A.10.2.1.b	Ook indien de informatieverwerking uitbesteed is, dient de informatiebeveiliging zeker gesteld te zijn.
A.10.2.2	Controle en beoordeling van dienstverlening door een derde partij
A.10.2.2.a	Er dienen acceptatiecriteria voor nieuwe informatiesystemen, upgrades en nieuwe versies te worden opgesteld.
A.10.2.3	Beheer van wijzigingen in dienstverlening door een derde partij
A.10.2.3.a	Veranderingen in de voorwaarden van dienstverlening dienen het kritische gehalte van de te leveren dienst in beschouwing te nemen en de risico's daaraan verbonden.
A.10.3	Systeemplanning en -acceptatie
A.10.3.1	Capaciteitsbeheer
A.10.3.1.a	Beoordeel regelmatig de capaciteit van het systeem ter voorkoming van systeemstoringen.
A.10.3.1.c	Er dient programmatuur geïnstalleerd te zijn om het systeem te monitoren en te verzekeren dat er voldoende capaciteit is ter voorkoming van storingen.
A.10.3.2	Systeemacceptatie
A.10.3.2.a	Specificeer acceptatiecriteria voor het testen van de beveiliging.
A.10.4	Bescherming tegen virussen en 'mobile code'
A.10.4.1	Maatregelen tegen virussen
A.10.4.1.a	De kans dat kwaadaardige programmatuur op het ICT-systeem terecht komt, moet zo klein mogelijk worden gehouden.
A.10.4.1.b	Monitor het systeem op mogelijke activiteit van kwaadaardige programmatuur.
A.10.4.1.c	Identificeer, isoleer en verwijder kwaadaardige programmatuur.
A.10.4.1.d	Een beleidsbesluit moet aangeven of het toegestaan is mobiele code op een bepaald systeem te draaien.
A.10.4.2	Maatregelen tegen 'mobile code'
A.10.4.2.a	Mobiele code mag alleen van betrouwbare bronnen worden geaccepteerd.
A.10.4.2.b	Zorg ervoor dat mobiele code niet geactiveerd kan worden.
A.10.4.2.c	Er moet duidelijk aangegeven worden wie er informatie mag downloaden en welk soort informatie mag worden gedownload.
A.10.4.2.d	Alle bestanden moeten eerst naar een "geïsoleerde" omgeving worden gedownload.
A.10.5	Back-up
A.10.5.1	Reservekopieën maken (back-ups)
A.10.5.1.a	Maak reservekopieën van alle kritieke bedrijfsgegevens.
A.10.5.1.b	Van alle applicaties dienen reservekopieën te worden gemaakt.
A.10.5.1.c	Maak reservekopieën van alle gegevens met behulp van een geschikte technologie.
A.10.5.1.d	Het moet mogelijk zijn om gegevens die na de laatste back-up verloren zijn gegaan opnieuw te maken.
A.10.6	Beheer van netwerkbeveiliging
A.10.6.1	Maatregelen voor netwerken
A.10.6.1.a	De configuratie van het netwerk moet actief worden beheerd.
A.10.6.1.b	De actuele status van het netwerk moet actief worden beheerd.
A.10.6.1.c	Houd het netwerkbeheerverkeer dat ontstaat bij het beheren en in de gaten houden van

Code	Maatregel
	netwerkapparaten onder controle.
A.10.6.1.d	De grenzen van een netwerk moeten vastgesteld zijn, evenals de samenstelling en de diensten ervan.
A.10.6.1.e	Het netwerk moet in staat zijn de uitval van afzonderlijke netwerkcomponenten op te vangen.
A.10.6.1.f	Het aantal "single points of failure" in een netwerkontwerp dient zo klein mogelijk te zijn.
A.10.6.1.g	De actuele status van het netwerk moet in de gaten worden gehouden.
A.10.6.1.i	Het vereiste kwaliteitsniveau van de netwerkdienst moet worden vastgesteld.
A.10.6.1.j	De kwaliteit van het netwerk als dienst voor de eindgebruikers moet bewaakt worden.
A.10.6.1.k	Verbindingen met openbare netwerken dienen zo te zijn ingericht dat ze tegen beschikbaarheidaanvallen bestand zijn.
A.10.6.1.l	Er dient een procedure te zijn om met beschikbaarheidaanvallen om te gaan.
A.10.6.1.m	De integriteitscontrole-, foutcorrectie- en rapportagemechanismen die inherent zijn aan het gebruikte communicatieprotocol moeten de integriteit van de informatie beschermen.
A.10.6.1.s	Netwerken dienen tegen niet-geautoriseerde toegang te worden beschermd.
A.10.6.2	Beveiliging van netwerkdiensten
A.10.6.2.a	Houd toezicht op de netwerkdienst.
A.10.6.2.b	Het contract met de dienstverlener moet formeel de beveiligingsaspecten voor de netwerkdienst definiëren.
A.10.6.2.c	Laat regelmatig onafhankelijke audits en beoordelingen uitvoeren.
A.10.7	Behandeling van media
A.10.7.1	Beheer van verwijderbare media
A.10.7.2	Verwijdering van media
A.10.7.3	Procedures voor de behandeling van informatie
A.10.7.4	Beveiliging van systeemdocumentatie
A.10.8	Uitwisseling van informatie
A.10.8.1	Beleid en procedures voor informatie-uitwisseling
A.10.8.1.f	Informatie die wordt verstuurd of ontvangen via de fax dient te worden beschermd.
A.10.8.2	Uitwisselingsovereenkomsten
A.10.8.2.d	Er moet tussen twee organisaties die informatie uitwisselen een formele overeenkomst opgesteld worden.
A.10.8.2.e	Onweerlegbaarheid in het elektronische verkeer dient te zijn geïmplementeerd.
A.10.8.3	Fysieke media die worden getransporteerd
A.10.8.3.a	Sla gegevensdragers tijdens transport veilig op.
A.10.8.4	Elektronische berichtuitwisseling
A.10.8.4.b	Gebruikers moeten op de hoogte van de gevaren die elektronische berichten en hun bijlagen kunnen bevatten worden gesteld.
A.10.8.4.d	Gebruikers moet verteld worden welke acties ze moeten ondernemen wanneer ze ongewenste elektronische berichten of spam ontvangen.
A.10.8.4.e	Ongewenste elektronische berichten moeten eruit worden gefilterd.
A.10.8.5	Systemen voor bedrijfsinformatie
A.10.8.5.a	Er moeten richtlijnen worden opgesteld met betrekking tot de risico's voor het bedrijf en beveiliging die het gebruik van elektronische kantoorapplicaties met zich meebrengt.
A.10.8.5.b	Er moet een persoon zijn aangewezen die verantwoordelijk voor de beveiliging van de bedrijfscentrale is.
A.10.8.5.c	Fysiek toegangsbeheer tot de bedrijfscentrale en bijbehorende voorzieningen dient ingesteld te zijn.
A.10.8.5.d	Alleen geautoriseerd personeel heeft logische toegang ten behoeve van beheer en onderhoud van de bedrijfscentrale.
A.10.8.5.f	Er moet voor calamiteiten of incidenten een reserve-host beschikbaar zijn om de verwerking over te nemen.
A.10.8.5.g	Implementeer een fout-tolerante host-architectuur.
A.10.8.5.h	Val waar mogelijk terug op een handmatig proces.
A.10.8.5.i	Er moeten voor noodgevallen reserveonderdelen beschikbaar zijn.
A.10.8.5.j	Er moeten stand-by-netwerkinterfaces beschikbaar zijn.
A.10.8.5.k	Leveranciers moeten contractueel verplicht zijn om een vooraf vastgesteld minimumniveau aan service te verlenen.
A.10.8.5.l	Er moeten stand-by-netwerkdiensten beschikbaar zijn.
A.10.8.5.q	Zorg voor reservegegevensdragers.
A.10.8.5.v	Het systeem moet robuust genoeg zijn om storingen aan afzonderlijke opslagschijven op te vangen.
A.10.8.5.w	Het personeel dient op de risico's te worden gewezen die alle vormen van informatie-uitwisseling met zich meebrengen, of het nu door middel van stemgeluid, fax of videocommunicatie is.
A.10.9	Diensten voor e-commerce
A.10.9.1	E-commerce
A.10.9.1.a	Zorg ervoor dat de gebruikersregistratie toegangsniveaus ondersteunt die consistent zijn met het opgegeven niveau van gebruikersidentificatie.
A.10.9.1.b	Het vaststellen van de identiteit van gebruikers moet op een geldig identiteitscertificaat

Code	Maatregel
	gebaseerd zijn dat door een erkende instantie uitgegeven is.
A.10.9.1.c	Gegevens van een gebruiker moeten van tijd tot tijd nagekeken worden om ervoor te zorgen dat ze volledig, juist en nog steeds nodig zijn.
A.10.9.1.d	Het netwerk moet een bevestiging van verzending geven.
A.10.9.2	Online transacties
A.10.9.2.a	De integriteit van online transacties dient te worden beschermd.
A.10.9.3	Openbaar beschikbare informatie
A.10.9.3.a	De integriteit van informatie die elektronisch gepubliceerd wordt moet worden beschermd.
A.10.9.3.b	De webbrowser moet zo ingesteld worden dat andere organisaties niet kunnen achterhalen welke sites de gebruikers hebben bezocht.
A.10.10	Controle
A.10.10.1	Aanmaken auditlogbestanden
A.10.10.1.a	Het moet mogelijk zijn de hoeveelheid log-gegevens die geregistreerd moet worden in te stellen.
A.10.10.2	Controle van systeemgebruik
A.10.10.2.a	Er moet kunnen worden opgegeven welke gebeurtenissen worden vastgelegd.
A.10.10.2.b	Het vastleggen van beheer- en gebruikersactiviteiten dient te geschieden op basis van betrouwbare voorzieningen.
A.10.10.2.c	Het loggen van gebruikersactiviteiten dient altijd actief te zijn.
A.10.10.2.d	Specificeer de soorten gebeurtenissen die onderzocht moeten worden.
A.10.10.2.e	Specificeer hoe vaak de account log moet worden beoordeeld.
A.10.10.2.f	Maak gebruik van netwerkmonitoring.
A.10.10.2.g	Alle fouten op het netwerk moeten worden gemeld.
A.10.10.2.h	Controleer netwerkverkeer op tekenen van ongeoorloofde activiteiten.
A.10.10.2.i	Het berichtensysteem moet een lokaal logbestand bijhouden van de verzendingen.
A.10.10.2.j	Bedieningsactiviteiten dienen bewaakt te worden.
A.10.10.3	Bescherming van informatie in logbestanden
A.10.10.3.a	Logboekinformatie en logboek faciliteiten dienen tegen wijzigingen en onbevoegde toegang te worden beschermd.
A.10.10.4	Logbestanden van administrators en operators
A.10.10.4.a	Bedieningspersoneel (operators) dient een activiteitenlogboek bij te houden.
A.10.10.5	Registratie van storingen
A.10.10.5.a	Storingen moeten gemeld en verholpen worden.
A.10.10.5.b	Gebreken aan programmatuur dienen te worden gemeld.
A.10.10.6	Synchronisatie van systeemklokken
A.10.10.6.a	Systeemklokken moeten gelijk lopen.

12. Toegangsbeveiliging

Code	Maatregel
A.11	Toegangsbeveiliging
A.11.1	Bedrijfseisen ten aanzien van toegangsbeheersing
A.11.1.1	Toegangsbeleid
A.11.1.1.a	Er moeten bedrijfscriteria voor toegangscontrole worden opgesteld.
A.11.1.1.b	Beperk de logische toegang tot bedieningsapparaten voor het netwerk.
A.11.2	Beheer van toegangsrechten van gebruikers
A.11.2.1	Registratie van gebruikers
A.11.2.1.a	Toegang tot een informatiesysteem voor meerdere gebruikers moet door een inschrijvings- en uitschrijvingsproces bepaald worden.
A.11.2.2	Beheer van speciale bevoegdheden
A.11.2.2.a	Het systeem moet het screeningsniveau en autorisaties bijhouden die aan gebruikers toegekend zijn.
A.11.2.2.b	Er moet een regeling zijn voor het gebruik van functies waarvoor bijzondere rechten nodig zijn.
A.11.2.2.c	Toegang tot de systeembeheerderaccounts moet strikt worden beperkt.
A.11.2.3	Beheer van gebruikerswachtwoorden
A.11.2.3.a	Zorg bij afgifte voor de vertrouwelijkheid van wachtwoorden.
A.11.2.3.b	Beperk het aantal wachtwoorden dat gebruikers nodig hebben.
A.11.2.4	Beoordeling van toegangsrechten van gebruikers
A.11.2.4.a	De toegangsrechten van gebruikers moeten met regelmatige tussenpozen worden geëvalueerd.
A.11.3	Verantwoordelijkheden van gebruikers
A.11.3.1	Gebruik van wachtwoorden
A.11.3.1.a	Wachtwoorden moeten zo lang zijn dat het moeilijk is om ze te ontcijferen.
A.11.3.1.b	Gebruikers dienen hun wachtwoorden te kiezen en te gebruiken op basis van adequate veiligheidsgebruiken.
A.11.3.1.c	Wachtwoorden moeten worden gewijzigd wanneer ze bekend raken.
A.11.3.1.d	Wachtwoorden moeten regelmatig worden gewijzigd.
A.11.3.2	Onbeheerde gebruikersapparatuur
A.11.3.2.a	Apparatuur die in een kantooromgeving opgesteld staat moet tegen ongeoorloofde toegang beschermd worden.
A.11.3.3	'Clear desk'- en 'clear screen'-beleid
A.11.3.3.a	Er dient een clear desk policy te worden ingesteld.
A.11.4	Toegangsbeheersing voor netwerken
A.11.4.1	Beleid ten aanzien van het gebruik van netwerkdiensten
A.11.4.1.a	Houd de hoeveelheid van het netwerkverkeer in de gaten.
A.11.4.1.b	Er moet beleid worden opgesteld met betrekking tot het gebruik van netwerken en netwerkdiensten.
A.11.4.1.c	Beperk de toegang op afstand tot netwerkapparaten.
A.11.4.1.d	Domain Name Servers moeten tegen aanvallen beschermd worden.
A.11.4.2	Authenticatie van gebruikers bij externe verbindingen.
A.11.4.2.a	Gebruikers op afstand moeten strenger dan plaatselijke gebruikers worden gecontroleerd om toegang te krijgen.
A.11.4.3	Identificatie van netwerkapparatuur
A.11.4.3.a	Alle werkstations die zijn gekoppeld aan een host-systeem moeten herkenbaar zijn.
A.11.4.3.b	De verbindingen tussen knooppunten moeten geïdentificeerd worden.
A.11.4.3.c	Knooppunten moeten worden geïdentificeerd.
A.11.4.3.d	Gebruik extra knooppuntauthenticatie.
A.11.4.4	Bescherming op afstand van poorten voor diagnose en configuratie
A.11.4.4.a	Voorkom ongeautoriseerde remote toegang tot toegangspoorten.
A.11.4.4.b	De vertrouwelijkheid van informatie die over verbindingen voor externe toegang wordt verstuurd, moet worden gewaarborgd.
A.11.4.4.c	Verbied remote diagnostiek.
A.11.4.5	Scheiding van netwerken
A.11.4.5.a	Voorzie in "gebruikersdomeinen" om gebruikers te scheiden.
A.11.4.5.b	Verkeersstromen tussen netwerken dienen beheerst te worden.
A.11.4.5.c	Isoleer bepaalde segmenten van het interne netwerk.
A.11.4.5.d	Netwerkgebruikers moeten een eigen account met beperkte functionaliteit hebben.
A.11.4.5.e	Isoleer specifieke hosts en regel de communicatie tussen hosts en netwerken.
A.11.4.5.f	Scheid het netwerk van andere netwerken.
A.11.4.5.g	Isoleer internetverbindingen.
A.11.4.6	Beheersmaatregelen voor netwerkverbindingen
A.11.4.6.a	Netwerkvoorzieningen voor gebruikers dienen alleen voor degenen beschikbaar te zijn voor wie kan worden aangetoond dat het zakelijk gezien noodzakelijk is.

Code	Maatregel
A.11.4.6.b	Er moet een vastomlijnd beleid voor het toegangsbeheer van gateways en firewalls zijn.
A.11.4.6.c	Van routeertabellen dienen regelmatig reservekopieën gemaakt te worden.
A.11.4.7	Beheersmaatregelen voor netwerkroutering
A.11.4.7.a	Het pad van het werkstation van de gebruiker tot de computerdienst dient via een bepaald pad te verlopen.
A.11.4.7.b	Er moeten in een gedeeld netwerk routeringsmechanismen worden ingesteld om ervoor te zorgen dat gegevensverkeer geen inbreuk op het toegangscontrolebeleid maakt.
A.11.4.7.c	Voorkom algemene toegang van en naar externe netwerken.
A.11.4.7.d	Toegang tot internet moet op gecontroleerde wijze plaatsvinden.
A.11.5	Toegangsbeveiliging voor besturingssystemen
A.11.5.1	Beveiligde inlogprocedures
A.11.5.1.a	Regel de toegang tot identificatievoorzieningen.
A.11.5.1.b	De toepassing moet bij het systeem bekend gemaakt worden.
A.11.5.2	Gebruikersidentificatie en -authenticatie
A.11.5.2.a	Iedere gebruiker moet een gebruikersnaam (user-ID) toegewezen krijgen.
A.11.5.3	Systemen voor wachtwoordbeheer
A.11.5.3.a	Wachtwoorden moeten worden opgeslagen in een eenzijdig versleutelde vorm.
A.11.5.4	Gebruik van systeemhulpmiddelen
A.11.5.4.a	Het gebruik van hulpmiddelen met de mogelijkheid om systeem en applicatie beperkingen te omzeilen dient beperkt en streng gereguleerd te worden.
A.11.5.5	Time-out van sessies
A.11.5.5.a	Onbeheerde werkstations moeten worden beveiligd tegen mogelijk gebruik door een ongeautoriseerd persoon.
A.11.5.6	Beperking van verbindingstijd
A.11.5.6.a	Gebruikers moeten worden beperkt tot gebruik van het systeem op specifieke tijden.
A.11.6	Toegangsbeheersing voor toepassingen en informatie
A.11.6.1	Beperking van toegang tot informatie
A.11.6.1.a	De eigenaar van een bestand is verantwoordelijk voor het bepalen wie toegang tot het bestand krijgt.
A.11.6.1.b	Toegangrechten voor individuen dienen afhankelijk te zijn van de rollen waar de persoon voor is geautoriseerd.
A.11.6.1.c	Toegang tot bestanden moet op basis van centraal beleid worden gegeven.
A.11.6.1.d	Toegang tot gegevens moet worden verleend in overeenstemming met het toegangsbeleid van de organisatie.
A.11.6.1.e	De toegang tot systeembestanden van applicaties moet geregeld worden.
A.11.6.1.f	Toegang tot audit trails moet geregeld worden.
A.11.6.1.g	Alle in-/uitvoereenheden moeten een unieke identificatie krijgen.
A.11.6.2	Isolatie van gevoelige systemen
A.11.6.2.a	Zeer gevoelige applicaties moeten op een aparte computer draaien.
A.11.7	Draagbare computers en telewerken
A.11.7.1	Draagbare computers en communicatievoorzieningen
A.11.7.1.a	Er moeten richtlijnen worden opgesteld met betrekking tot de risico's en de voorzorgsmaatregelen die genomen moeten worden bij het gebruik van mobiele computervoorzieningen.
A.11.7.1.b	Informatie op Personal Digital Assistants (PDA's) dient te worden beschermd tegen diefstal, virussen en communicatie interceptie.
A.11.7.2	Telewerken
A.11.7.2.a	Telewerken mag alleen toegestaan worden wanneer passende beveiligingsmaatregelen aanwezig zijn.

13. Beheer (Verwerving, ontwikkeling en onderhoud van informatiesystemen)

Code	Maatregel
A.12	Verwerving, ontwikkeling en onderhoud van informatiesystemen
A.12.1	Beveiligingseisen voor informatiesystemen
A.12.1.1	Analyse en specificatie van beveiligingseisen
A.12.1.1.a	Applicatieontwikkeling moet zodanig worden uitgevoerd dat de kans op onopzettelijke dan wel opzettelijke fouten in de programmatuur zo klein mogelijk is.
A.12.2	Correcte verwerking in toepassingen
A.12.2.1	Validatie van invoergegevens
A.12.2.2	Beheersing van interne gegevensverwerking
A.12.2.3	Integriteit van berichten
A.12.2.3.a	Alle communicerende entiteiten moeten worden geauthenticeerd.
A.12.2.4	Validatie van uitvoergegevens
A.12.3	Cryptografische beveiliging
A.12.3.1	Beleid voor het gebruik van cryptografische beheersmaatregelen
A.12.3.2	Sleutelbeheer
A.12.3.2.c	Cryptosleutels dienen door middel van een beproefd algoritme tot stand te komen.
A.12.3.2.j	Het tijdstip waarop een transactie plaatsvindt dient van een tijdstempel te worden voorzien.
A.12.4	Beveiliging van systeembestanden
A.12.4.1	Beheersing van operationele software
A.12.4.1.a	Signaleer en voorkom inbreuken op de integriteit van de programmatuur.
A.12.4.1.b	Er moet een lijst worden bijgehouden met alle wijzigingen die in de programmatuur worden aangebracht.
A.12.4.1.c	Beheersmiddelen dienen beschikbaar te zijn om programmatuur op bedrijfssystemen te implementeren.
A.12.4.2	Bescherming van testdata
A.12.4.2.a	Testgegevens dienen te worden beschermd en beheerd.
A.12.4.3	Toegangsbeheersing voor broncode van programmatuur
A.12.4.3.a	Er dienen regels te zijn voor het gebruik van programmeerfaciliteiten van elektronische kantoorsystemen.
A.12.4.3.b	Er moet een gecontroleerde ontwikkelomgeving zijn.
A.12.4.3.c	Er dient strikt toezicht op toegang tot bibliotheken met programmacode uitgeoefend te worden.
A.12.4.3.d	Zorg ervoor dat de kans dat het systeem wordt misbruikt door ontwikkelaars zo klein mogelijk is.
A.12.4.3.e	Alleen geautoriseerd onderhoudspersoneel voor software mag onderhoudstaken uitvoeren.
A.12.5	Beveiliging bij ontwikkel- en ondersteuningsprocessen
A.12.5.1	Procedures voor wijzigingsbeheer
A.12.5.1.a	Alle wijzigingen in de programmatuur moeten worden geautoriseerd voordat de wijziging wordt doorgevoerd.
A.12.5.1.b	Er moet een regeling zijn voor noodzakelijke programmatuurwijzigingen die aangebracht moeten worden vóórdat autorisatie kan worden toegekend.
A.12.5.1.c	Wijzigingen in het besturingssysteem moeten geautoriseerd worden.
A.12.5.1.d	Voer wijzigingen in toepassingen gecontroleerd door.
A.12.5.1.e	Het systeem moet herstel vergemakkelijken bij het ontstaan van problemen.
A.12.5.2	Technische beoordeling van toepassingen na wijzigingen in het besturingssysteem
A.12.5.2.a	Beoordeel het effect van een wijziging van het besturingssysteem op de beveiliging.
A.12.5.3	Restricties op wijzigingen in programmatuurpakketten
A.12.5.3.a	Aanpassingen in standaard programmatuur moeten zo worden uitgevoerd dat geen nieuwe problemen ontstaan.
A.12.5.4	Uitlekken van informatie
A.12.5.4.a	Gelegenheid tot het lekken van informatie dient te worden verhinderd.
A.12.5.5	Uitbestede ontwikkeling van programmatuur
A.12.5.5.a	Er dient voor maatwerk dat door derden gemaakt is een formeel contract te bestaan.
A.12.5.5.b	De kwaliteit van al het onderhoudswerk aan software moet worden gecontroleerd.
A.12.6	Beheer van technische kwetsbaarheden
A.12.6.1	Beheersing van technische kwetsbaarheden
A.12.6.1.a	Informatie over technische kwetsbaarheden van informatiesystemen dient te worden geëvalueerd.

14. Beheer van informatiebeveiliging incidenten

Code	Maatregel
A.13	Beheer van informatiebeveiligingsincidenten
A.13.1	Rapportage van informatiebeveiligingsgebeurtenissen en zwakke plekken
A.13.1.1	Rapportage van informatiebeveiligingsgebeurtenissen
A.13.1.1.b	Alle incidenten/schendingen moeten worden doorgegeven aan de centrale incidentregistratie.
A.13.1.1.c	Beveiligingsincidenten moeten snel en via de juiste kanalen worden gemeld.
A.13.1.2	Rapportage van zwakke plekken in de beveiliging
A.13.1.2.a	Alle zwakke plekken in de beveiliging moeten snel worden gemeld.
A.13.2	Beheer van informatiebeveiligingsincidenten en -verbeteringen
A.13.2.1	Verantwoordelijkheden en procedures
A.13.2.1.a	Onderzoek alle vermoedelijke of gesignaleerde pogingen om door de beveiliging heen te komen.
A.13.2.2	Leren van informatiebeveiligingsincidenten
A.13.2.2.a	De organisatie dient stappen te nemen om ervoor te zorgen dat ze van incidenten leert.
A.13.2.3	Verzamelen van bewijsmateriaal

15. Bedrijfscontinuïteitsbeheer

Code	Maatregel
A.14	Bedrijfscontinuïteitsbeheer
A.14.1	Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer
A.14.1.1	Informatiebeveiliging opnemen in het proces van bedrijfscontinuïteitsbeheer
A.14.1.2	Bedrijfscontinuïteit en risicobeoordeling
A.14.1.2.a	De continuïteitsstrategie dient op een risicoanalyse gebaseerd te zijn.
A.14.1.2.b	Continuïteitsplannen dienen na een onderbreking van het bedrijfsproces herstel van bedrijfsactiviteiten binnen de vereiste tijdsduur mogelijk te maken.
A.14.1.3	Continuïteitsplannen ontwikkelen en implementeren waaronder informatiebeveiliging
A.14.1.3.a	Er moet een calamiteitenplan worden opgesteld.
A.14.1.4	Kader voor de bedrijfscontinuïteitsplanning
A.14.1.4.a	Stel continuïteitsplannen op.
A.14.1.5	Testen, onderhoud en herbeoordelen van continuïteitsplannen
A.14.1.5.a	Continuïteitsplannen dienen regelmatig testen te ondergaan.
A.14.1.5.b	De continuïteitsplannen dienen onderhouden te worden.

16. Naleving

Code	Maatregel
A.15	Naleving
A.15.1	Naleving van wettelijke voorschriften
A.15.1.1	Identificatie van toepasselijke wetgeving
A.15.1.1.b	Voer controles uit om na te gaan of er wordt voldaan aan de wettelijk voorgeschreven en contractueel vastgelegde beveiligingseisen.
A.15.1.2	Intellectuele eigendomsrechten (Intellectual Property Rights, IPR)
A.15.1.2.a	De organisatie dient ervoor te zorgen dat ze software rechtmatig gebruikt.
A.15.1.2.b	Intellectuele eigendomsrechten dienen gerespecteerd te worden.
A.15.1.2.c	Proprietary software dient overeenkomstig de licentieovereenkomst gebruikt te worden.
A.15.1.3	Bescherming van bedrijfsdocumenten
A.15.1.3.a	Het logbestand met gebruikersactiviteiten moet bewaard worden om het uitvoeren van een onderzoek mogelijk te maken.
A.15.1.4	Bescherming van gegevens en geheimhouding van persoonsgegevens
A.15.1.4.a	Er dient formeel een Verantwoordelijke te worden vastgesteld. Dit kan een natuurlijke- of een rechtspersoon zijn.
A.15.1.4.b	Er dient een Functionaris voor de gegevensbescherming (FG) aangesteld te worden. Dit kan geschieden door de Verantwoordelijke of door een brancheorganisatie.
A.15.1.4.c	Er moet worden vastgesteld wie de Gegevensverwerkers zijn.
A.15.1.4.f	Informatiesystemen die persoonsgegevens gebruiken dienen conform de principes van de Wet bescherming persoonsgegevens te werken.
A.15.1.4.i	Binnen de organisatie dienen regelmatig trainingen te worden gegeven om het besef, dat gegevens beschermd moeten worden, te verhogen.
A.15.1.4.j	De gegevens in het registratiesysteem dienen regelmatig gecontroleerd te worden.
A.15.1.5	Voorkoming van misbruik van IT-voorzieningen
A.15.1.5.a	Gebruikers moet worden meegedeeld dat in de gaten kan worden gehouden welke internetsites ze bezoeken.
A.15.1.6	Voorschriften voor het gebruik van cryptografische beheersmaatregelen
A.15.2	Naleving van beveiligingsbeleid en -normen en technische naleving
A.15.2.1	Naleving van beveiligingsbeleid en -normen
A.15.2.1.a	Voer beveiligingsreviews uit om ervoor te zorgen dat wordt voldaan aan fysieke, procedurele en technische maatregelen.
A.15.2.2	Controle op technische naleving
A.15.2.2.a	Beveiligingstesten moeten worden uitgevoerd volgens de beveiligingseisen, waarbij gebruik wordt gemaakt van de overeengekomen acceptatiecriteria.
A.15.2.2.b	Netwerkapparaten moeten worden nagekeken om zeker te stellen dat alle bekende kwetsbaarheden geëlimineerd zijn.
A.15.3	Overwegingen bij audits van informatiesystemen
A.15.3.1	Beheersmaatregelen voor audits van informatiesystemen
A.15.3.1.a	Er moeten voorzieningen voor het analyseren van logbestanden met gebruikersactiviteiten beschikbaar zijn.
A.15.3.1.b	Het opstellen en uitvoeren van audits moet zorgvuldig gepland worden om de kans op verstoringen in het bedrijfsproces zo klein mogelijk te maken.
A.15.3.2	Bescherming van hulpmiddelen voor audits van informatiesystemen
A.15.3.2.a	Toegang tot hulpmiddelen voor systeemaudits moet worden beveiligd om misbruik en aanpassing te voorkomen.