Gemeenschappelijk normenkader informatiebeveiliging

Afsprakenstelsel			Document	
Versie	1.13 14 juli 2022		Auteur	Beheerorganisatie
Datum vaststelling	14 Jul 2022		Classificatie	Openbaar
Datum publicatie	07 Sep 2022		Status	Definitief

Legenda

Afkorting	Betekenis
v	Vanuit het afsprakenstelsel is er geen nadere specificatie van de norm gegeven. Deelnemers, BSNk en de Beheerorganisatie baseren de keuze van maatregelen op hun uitgevoerde risicoanalyse. In deze risicoanalyse moeten de gegeven risico's op stelselniveau wel worden meegewogen. De norm c.q. beheersmaatregel maakt geen verplicht onderdeel uit van de VvT van de deelnemers en Beheerorganisatie.
S	Vanuit het afsprakenstelsel zijn er nadere specificaties voor de norm gegeven. Er wordt verwezen naar een document of er wordt om speciale aandacht gevraagd. De norm c.q. beheersmaatregel maakt onderdeel uit van de VvT van de Deelnemers, BSNk en Beheerorganisatie.
Sv	De norm is vanuit stelseloptiek relevant, maar er is geen nadere specificatie van de norm gegeven. Dit betekent dat de norm onderdeel uit maakt van de VvT van het ISMS van de Deelnemers, BSNk en Beheerorganisatie of dat er argumenten zijn waarom deze norm vanuit de rol of dienstverlening in het kader van het stelsel niet van toepassing is voor de Deelnemers, BSNk of de Beheerorganisatie. Deze argumenten dienen in relatie tot de VvT controleerbaar te worden vastgelegd en onderdeel gemaakt van het auditdossier.

ISO 27001:2013 beheersdoelstellingen en beheersmaatregelen binnen de scope van eToegangsdiensten, - activiteiten, -objecten en -informatie

Norm	Titel	Doelstellingen en beheersmaatregelen	Deelnemer	BSNk	BO	Opmerkingen	Toelichting en referenties
A.5	**Informatiebeveiligingsbeleid**						
A.5.1	Aansturing door de directie van de informatiebeveiliging	Het verschaffen van directieaansturing van en -steun voor informatiebeveiliging in overeenstemming met bedrijfseisen en relevante wet- en regelgeving.					
A.5.1.1	Beleidsregels voor informatiebeveiliging	Ten behoeve van informatiebeveiliging moet een reeks beleidsregels worden gedefinieerd, goedgekeurd door de directie, gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen.	Sv	Sv	Sv	Iedere deelnemer, BSNk en de BO stelt een eigen beleidsdocument voor informatiebeveiliging op waarin rekening wordt gehouden met het beleidsdocument voor informatiebeveiliging dat voor het Netwerk c.q. het stelsel van Elektronische Toegangsdiensten is opgesteld.	De beheerorganisatie beheert het Beleid voor informatiebeveiliging namens het Stelsel.
A.5.1.2	Beoordelen van het informatiebeveiligingsbeleid	Het beleid voor informatiebeveiliging moet met geplande tussenpozen of als zich significante veranderingen voordoen, worden beoordeeld om te waarborgen dat het voortdurend passend, adequaat en doeltreffend is.	Sv	Sv	Sv	Deelnemers, BSNk en de BO beoordelen regelmatig de werking van het informatiebeveiligingsbeleid en leveren hierover input t.b.v. de beoordeling op stelselniveau.	Beleid voor informatiebeveiliging wordt periodiek beoordeeld met input van de Toezichthouder, de deelnemers, BSNk en de BO.
A.6	**Organiseren van informatiebeveiliging**						
A.6.1	Interne organisatie	Een beheerkader vaststellen om de implementatie en uitvoering van de informatiebeveiliging binnen de organisatie te initiëren en te beheersen.					-
A.6.1.1	Rollen en verantwoordelijkheden bij informatiebeveiliging	Alle verantwoordelijkheden bij informatiebeveiliging moeten worden gedefinieerd en toegewezen.	Sv	Sv	S		Beheerorganisatie coördineert t.b.v. het stelsel. Concreet door toewijzing van de rollen van security officer, riskmanager en incidentmanager.
A.6.1.2	Scheiding van taken	Conflicterende taken en verantwoordelijkheidsgebieden moeten worden gescheiden om de kans op onbevoegd of onbedoeld wijzigen of misbruik van de bedrijfsmiddelen van de organisatie te verminderen.	Sv	v	v	Voor MU al standaard bij PKI. Zo mogelijk moet functiescheiding worden toegepast. Waar dit voor kleine organisaties niet mogelijk is moeten compenserende maatregelen worden genomen (bijv. audit trails).	Zwaarte van de maatregelen moet in relatie staan tot de geleverde betrouwbaarheidsniveaus van de dienst. Deelnemers, BSNk en BO richten dit naar eigen inzicht in.
A.6.1.3	Contact met overheidsinstanties	Er moeten passende contacten met relevante overheidsinstanties worden onderhouden.	v	v	S	Stelseltaak voor BO	De BO onderhoudt op stelselniveau contact met relevante overheidsinstanties.
A.6.1.4	Contact met speciale belangengroepen	Er moeten passende contacten met speciale belangengroepen of andere gespecialiseerde beveiligingsfora en professionele organisaties worden onderhouden.	v	v	S	Stelseltaak voor BO	De BO onderhoudt contact met speciale groepen of fora zoals bij Europese ontwikkelingen (eIDAS) en het NCSC specifiek voor informatiebeveiliging.

A.6.1.5	Informatiebeveiliging in projectbeheer	Informatiebeveiliging moet aan de orde komen in projectbeheer, ongeacht het soort project.	v	v	v		Deelnemers, BSNk en BO vullen dit naar eigen inzicht in.
A.6.2	Mobiele apparatuur en telewerken	Het waarborgen van de veiligheid van telewerken en het gebruik van mobiele apparatuur.				Mogelijk ontstaat vanuit bestaande normenkaders (hogere betrouwbaarheidsniveaus) een beperking op de mogelijkheid om werkzaamheden via mobiele apparatuur uit te voeren.	Indien draagbare computers en communicatievoorzieningen ten behoeve van het verlenen van stelseldiensten of stelselbeheer worden toegestaan MOETEN passende maatregelen te worden genomen.
A.6.2.1	Beleid voor mobiele apparatuur	Beleid en ondersteunende beveiligingsmaatregelen moeten worden vastgesteld om de risico's die het gebruik van mobiele apparatuur met zich meebrengt te beheren.	v	v	v		Deelnemers, BSNk en BO vullen dit naar eigen inzicht in.
A.6.2.2	Telewerken	Beleid en ondersteunende beveiligingsmaatregelen moeten worden geïmplementeerd ter beveiliging van informatie die vanaf telewerklocaties wordt bereikt, verwerkt of opgeslagen.	v	v	v		Deelnemers, BSNk en BO vullen dit naar eigen inzicht in.
A.7	**Veilig personeel**						
A.7.1	Voorafgaand aan het dienstverband	Waarborgen dat medewerkers en contractanten hun verantwoordelijkheden begrijpen en geschikt zijn voor de functies waarvoor zij in aanmerking komen.					
A.7.1.1	Screening	Verificatie van de achtergrond van alle kandidaten voor een dienstverband moet worden uitgevoerd in overeenstemming met relevante wet- en regelgeving en ethische overwegingen en moet in verhouding staan tot de bedrijfseisen, de classificatie van de informatie waartoe toegang wordt verleend en de vastgestelde risico's.	S	S	S	Uit de risicoanalyse (bijv. via "misbruik-scenario's") kan blijken dat per rol en evt. per betrouwbaarheidsniveau onderscheid moet worden gemaakt in het niveau van screening.	1. De wijze en diepgang van de screening moet zijn gerelateerd aan de bevoegdheden en taakstelling van de betreffende medewerker. Zo mag worden verwacht dat de screening voor een systeembeheerder met speciale bevoegdheden ten aanzien van systeemprogrammatuur strenger zal zijn dan voor een ondersteunende stafmedewerker. 2. Basis niveau van screening: Het basisniveau van screening voor alle personeel, moet bestaan uit: a. Het controleren van de juistheid van de identiteit (WID-document); b. Controleren van de juistheid van gegevens in het curriculum vitae en met name van opleidingsgegevens; c. Controleren van relevante referenties.

3. Screening van vast personeel t.b.v. het Stelsel:
    a. Medewerkers die met activiteiten voor EID zijn belast moeten een Verklaring Omtrent Gedrag (VOG) aanvragen c.q. overleggen in relatie tot de omgang van gegevens waarbij integriteit en vertrouwelijkheid van belang zijn.
    b. De (originele of digitale kopie) VOG moet worden opgenomen in het personeelsdossier of digitale registratie.
    c. In het geval een zwaardere screening aantoonbaar al reeds heeft plaatsgevonden mag de deelnemer of beheerorganisatie besluiten om de VOG achterwege te laten. Zwaarder dan een VOG zijn bijvoorbeeld: veiligheidsonderzoek door de AIVD (A, B of C onderzoek) of de MIVD, antecedentenonderzoek door een erkend onderzoeksbureau.

4. Screening van tijdelijk personeel:
    a. Deze screeningprocedure voor intern personeel is ook van toepassing op van externe leveranciers ingehuurd personeel.
    b. De eisen die aan ingehuurd personeel worden gesteld worden moeten van het zelfde niveau zijn als de eisen aan het vaste personeel;
    In het contract met de leverancier moet zijn opgenomen:
        i. welke verantwoordelijkheden deze heeft ten aanzien van het screeningproces en;
        ii. de verplichting daarover om direct de opdrachtgever te informeren als de screening van een in te zetten of ingezette medewerker niet (volledig) heeft plaatsgevonden of tot een negatief resultaat heeft geleid.
5. De organisatie (deelnemer, BSNk, BO) moet een functionaris aanwijzen die verantwoordelijk is voor het laten uitvoeren van het screeningproces. In veel gevallen ligt deze verantwoordelijkheid bij een securityofficer of een risk manager.
6. De werkgever moet de medewerker verzoeken om een VOG aan te vragen.
    a. In de aanvraag moet de werkgever aangeven wat de aard van het werk is dat de medewerker gaat uitvoeren.
    b. De werkgever heeft expliciet beleid geformuleerd dat er zorg voor moet dragen dat gedurende het dienstverband van de medewerker de integriteit en betrouwbaarheid aantoonbaar geborgd is.

							7. Het screeningsproces moet worden doorlopen voor elk personeelslid (vast of ingehuurd): a. Bij indiensttreding. b. Ingeval van een bestaand dienstverband als de screening nog niet heeft plaatsgevonden of is verlopen. c. Bij verandering van functie of werkgebied van een medewerker als de nieuwe werkzaamheden meer omvatten of in hoge mate afwijken van de vroegere werkzaamheden.
A.7.1.2	Arbeidsvoorwaarden	De contractuele overeenkomst met medewerkers en contractanten moet hun verantwoordelijkheden voor informatiebeveiliging en die van de organisatie vermelden.	Sv	Sv	Sv	Bijv. in de vorm van een ondertekend arbeidscontract of vergelijkbaar alternatief.	Deelnemers, BSNk en BO vullen dit naar eigen inzicht in.
A.7.2	Tijdens het dienstverband	Ervoor zorgen dat medewerkers en contractanten zich bewust zijn van hun verantwoordelijkheden op het gebied van informatiebeveiliging en deze nakomen.					
A.7.2.1	Directieverantwoordelijkheden	De directie moet van alle medewerkers en contractanten eisen dat ze informatiebeveiliging toepassen in overeenstemming met de vastgestelde beleidsregels en procedures van de organisatie.	Sv	Sv	Sv	Management dient personeel dat een taak /activiteit verricht ten behoeve van een rol in het stelsel, o.m. op de hoogte te stellen van de relevante eisen uit het afsprakenstelsel en bijbehorende procedures	
A.7.2.2	Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	Alle medewerkers van de organisatie en, voor zover relevant, contractanten moeten een passende bewustzijnsopleiding en -training krijgen en regelmatige bijscholing van beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie.	Sv	Sv	Sv		Deelnemers, BSNk en BO vullen dit naar eigen inzicht in.
A.7.2.3	Disciplinaire procedure	Er moet een formele en gecommuniceerde disciplinaire procedure zijn om actie te ondernemen tegen medewerkers die een inbreuk hebben gepleegd op de informatiebeveiliging.	Sv	Sv	Sv	Voor deelnemers, BSNk en Beheerorganisatie is de maatregel bedoeld voor werknemers die inbreuk op de beveiliging hebben gepleegd. Iedere organisatie binnen het stelsel bepaalt zelf of daartoe een formeel disciplinair proces moet worden vastgesteld.	Deelnemers, BSNk en BO vullen dit naar eigen inzicht in.
A.7.3	Beëindiging en wijziging van dienstverband	Het beschermen van de belangen van de organisatie als onderdeel van de wijzigings- of beëindigingsprocedure van het dienstverband.					Deelnemers, BSNk en BO vullen dit naar eigen inzicht in.
A.7.3.1	Beëindiging of wijziging van verantwoordelijkheden van het dienstverband	Verantwoordelijkheden en taken met betrekking tot informatiebeveiliging die van kracht blijven na beëindiging of wijziging van het dienstverband moeten worden gedefinieerd, gecommuniceerd aan de medewerker of contractant, en ten uitvoer worden gebracht.	v	v	v		Deelnemers, BSNk en BO vullen dit naar eigen inzicht in.
A.8	**Beheer van bedrijfsmiddelen**						
A.8.1	Verantwoordelijkheid voor bedrijfsmiddelen	Bedrijfsmiddelen van de organisatie identificeren en passende verantwoordelijkheden ter bescherming definiëren.					
A.8.1.1	Inventariseren van bedrijfsmiddelen	Bedrijfsmiddelen die samenhangen met informatie en informatieverwerkende faciliteiten moeten worden geïdentificeerd, en van deze bedrijfsmiddelen moet een inventaris worden opgesteld en onderhouden.	Sv	Sv	Sv	Het stelsel beschikt niet over gemeenschappelijke bedrijfsmiddelen.	Vooralsnog zijn er geen gemeenschappelijke bedrijfsmiddelen onderkend. Indien dit wel het geval zou worden, is de Beheerorganisatie verantwoordelijk voor het bijhouden van de inventarisatie.
A.8.1.2	Eigendom van bedrijfsmiddelen	Bedrijfsmiddelen die in het inventarisoverzicht worden bijgehouden moeten een eigenaar hebben.	v	v	v		idem
A.8.1.3	Aanvaardbaar gebruik van bedrijfsmiddelen	Voor het aanvaardbaar gebruik van informatie en van bedrijfsmiddelen die samenhangen met informatie en informatieverwerkende faciliteiten moeten regels worden geïdentificeerd, gedocumenteerd en geïmplementeerd.	v	v	v		idem
A.8.1.4	Teruggeven van bedrijfsmiddelen	Alle medewerkers en externe gebruikers moeten alle bedrijfsmiddelen van de organisatie die ze in hun bezit hebben bij beëindiging van hun dienstverband, contract of overeenkomst teruggeven.	v	v	v		idem

A.8.2	Informatieclassificatie	Bewerkstelligen dat informatie een passend beschermingsniveau krijgt dat in overeenstemming is met het belang ervan voor de organisatie.					
A.8.2.1	Classificatie van informatie	Informatie moet worden geclassificeerd met betrekking tot wettelijke eisen, waarde, belang en gevoeligheid voor onbevoegde bekendmaking of wijziging.	S	S	S	Deelnemers, BSNk en BO moeten een eigen classificatie van hun informatie hebben gebaseerd op de richtlijnen voor classificatie van informatie uit het Informatiebeveiligingsbeleid, de stelselrisicoanalyse en hun eigen risicoanalyse.	Zie Afspraken Gemeenschappelijke Classificatie van Stelselinformatie
A.8.2.2	Informatie labelen	Om informatie te labelen moet een passende reeks procedures worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.	Sv	Sv	S		idem
A.8.2.3	Behandelen van bedrijfsmiddelen	Procedures voor het behandelen van bedrijfsmiddelen moeten worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.	v	v	v	Het stelsel Elektronische Toegangsdiensten beschikt niet over gemeenschappelijke bedrijfsmiddelen.	Deelnemers, BSNk en BO vullen dit naar eigen inzicht in.
A.8.3	Behandelen van media	Onbevoegde openbaarmaking, wijziging, verwijdering of vernietiging van informatie die op media is opgeslagen voorkomen.					
A.8.3.1	Beheer van verwijderbare media	Voor het beheren van verwijderbare media moeten procedures worden geïmplementeerd in overeenstemming met het classificatieschema dat door de organisatie is vastgesteld.	Sv	Sv	Sv	-	Alleen specifiek: Deelnemers, BSNk en BO moeten ten minste een procedure inrichten voor voor zorgvuldig beheer van verwijderbare media die drager zijn van persoonsgegevens en metagegevens.
A.8.3.2	Verwijderen van media	Media moeten op een veilige en beveiligde manier worden verwijderd als ze niet langer nodig zijn, overeenkomstig formele procedures.	Sv	Sv	Sv	Media waar archiveringsgegevens zijn opgeslagen. Media waar persoonsgegevens zijn opgeslagen. Media waar metadata is opgeslagen.	De BO is verantwoordelijk voor het verwijderen van media binnen de eigen organisatiecontext en op het niveau van het stelsel. Deelnemers en BSNk zijn verantwoordelijk voor het verwijderen media binnen de eigen organisatie context.
A.8.3.3	Media fysiek overdragen	Media moeten op een veilige en beveiligde manier worden verwijderd als ze niet langer nodig zijn, overeenkomstig formele procedures.	Sv	Sv	Sv	idem	idem
A.9	**Toegangsbeveiliging**						
A.9.1	Bedrijfseisen voor toegangsbeveiliging	Toegang tot informatie en informatieverwerkende faciliteiten beperken.					
A.9.1.1	Beleid voor toegangsbeveiliging	Een beleid voor toegangsbeveiliging moet worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfs- en informatiebeveiligingseisen.	S Sv	S Sv	S Sv	Specificatie (S) bedoeld voor de registratie van externe gebruikers i.c. bedrijven /klanten van deelnemers. Voor interne gebruikers (medewerkers van deelnemers) bepaalt de deelnemers zelf de invulling (Sv).	Toegangsbeveiligingsbeleid moet in overeenstemming overeenstemming met: 1. de classificatie van informatie voor stelselinformatie en 2. de betrouwbaarheidsniveaus van stelseldiensten t.b.v. gebruikers van stelseldiensten. Zie voor 1) Beleid voor informatiebeveiliging Zie voor 2) Normenkader betrouwbaarheidsniveaus
A.9.1.2	Toegang tot netwerken en netwerkdiensten	Gebruikers moeten alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn.	S Sv	S Sv	S Sv	idem	Zie Normenkader betrouwbaarheidsniveaus
A.9.2	Beheer van toegangsrechten van gebruikers	Toegang voor bevoegde gebruikers bewerkstelligen en onbevoegde toegang tot systemen en diensten voorkomen.				Op stelselniveau gaat het om de registratie van gebruikers van stelselsystemen: Confluence, Mantis, Metadata, Dienstencatalogus, Managementinformatie, Simulator.	
A.9.2.1	Registratie en uitschrijving van gebruikers	Een formele registratie- en uitschrijvingsprocedure moet worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.	S Sv	S Sv	S Sv	Specificatie (S) bedoeld voor de registratie van externe gebruikers i.c. bedrijven /klanten van deelnemers. Voor interne gebruikers (medewerkers van deelnemers) bepaalt de deelnemers zelf de invulling (Sv).	Met name voor MU, MR: Procesbeschrijvingen en registratie moeten voldoen aan de beschrijving van de betrouwbaarheidsniveaus voor het verkrijgen van authenticatiemiddelen en registraties van machtigingen.
A.9.2.2	Gebruikers toegang verlenen	Een formele gebruiker-toegangsverleningsprocedure moet worden geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken	Sv		Sv		
A.9.2.3	Beheren van speciale toegangsrechten	Het toewijzen en gebruik van bevoorrechte toegangsrechten moeten worden beperkt en gecontroleerd.	Sv	Sv	Sv		
A.9.2.4	Beheer van geheime authenticatie-informatie van gebruikers	Het toewijzen van geheime authenticatie-informatie moet worden beheerst via een formeel beheersproces.	Sv	Sv	Sv		

A.9.2.5	Beoordeling van toegangsrechten van gebruikers	Eigenaren van bedrijfsmiddelen moeten toegangsrechten van gebruikers regelmatig beoordelen.	Sv	Sv	Sv		
A.9.2.6	Toegangsrechten intrekken of aanpassen	De toegangsrechten van alle medewerkers en externe gebruikers voor informatie en informatieverwerkende faciliteiten moeten bij beëindiging van hun dienstverband, contract of overeenkomst worden verwijderd, en bij wijzigingen moeten ze worden aangepast.	Sv	Sv	Sv		
A.9.3	Gebruikersverantwoordelijkheden	Gebruikers verantwoordelijk maken voor het beschermen van hun authenticatie-informatie.					
A.9.3.1	Geheime authenticatie-informatie gebruiken	Van gebruikers moet worden verlangd dat zij zich bij het gebruiken van geheime authenticatie-informatie houden aan de praktijk van de organisatie.	Sv	Sv	Sv		Gebruikers worden geacht een goede beveiligingspraktijk te hanteren bij het selecteren en gebruik van wachtwoorden. Zie Gebruiksvoorwaarden Elektronische Toegangsdiensten
A.9.4	Toegangsbeveiliging van systeem en toepassing	Onbevoegde toegang tot systemen en toepassingen voorkomen.					
A.9.4.1	Beperking toegang tot informatie	Toegang tot informatie en systeemfuncties van applicaties moet worden beperkt in overeenstemming met het beleid voor toegangscontrole.	Sv	Sv	Sv		
A.9.4.2	Beveiligde inlogprocedures	Indien het beleid voor toegangsbeveiliging dit vereist, moet toegang tot systemen en toepassingen worden beheerst door een beveiligde inlogprocedure.	Sv	Sv	Sv		
A.9.4.3	Systeem voor wachtwoordbeheer	Systemen voor wachtwoordbeheer moeten interactief zijn en sterke wachtwoorden waarborgen.	Sv	Sv	Sv		Specifiek voor MU: Voor authenticatiemiddelen in het stelsel Zie Normenkader betrouwbaarheidsniveaus
A.9.4.4	Speciale systeemhulpmiddelen gebruiken	Het gebruik van systeemhulpmiddelen die in staat zijn om beheersmaatregelen voor systemen en toepassingen te omzeilen moet worden beperkt en nauwkeurig worden gecontroleerd.	v	v	v		Deelnemers, BSNk en BO vullen dit naar eigen inzicht in.
A.9.4.5	Toegangsbeveiliging op programmabroncode	Toegang tot de programmabroncode moet worden beperkt.	v	v	v		Deelnemers, BSNk en BO vullen dit naar eigen inzicht in.
A.10	**Cryptografie**						
A.10.1	Cryptografische beheersmaatregelen	Zorgen voor correct en doeltreffend gebruik van cryptografie om de vertrouwelijkheid, authenticiteit en/of integriteit van informatie te beschermen.					
A.10.1.1	Beleid inzake het gebruik van cryptografische beheersmaatregelen	Ter bescherming van informatie moet een beleid voor het gebruik van cryptografische beheersmaatregelen worden ontwikkeld en geïmplementeerd.	S	S	S		Conform Information security requirements
A.10.1.2	Sleutelbeheer	Met betrekking tot het gebruik, de bescherming en de levensduur van cryptografische sleutels moet tijdens hun gehele levenscyclus een beleid worden ontwikkeld en geïmplementeerd.	Sv	Sv	Sv		Conform Information security requirements
A.11	**Fysieke beveiliging en beveiliging van de omgeving**						**Deelnemers en BO vullen dit naar eigen inzicht in.**
A.11.1	Beveiligde gebieden	Onbevoegde fysieke toegang tot, schade aan en interferentie met informatie en informatieverwerkende faciliteiten van de organisatie voorkomen.					
A.11.1.1	Fysieke beveiligingszone	Beveiligingszones moeten worden gedefinieerd en gebruikt om gebieden te beschermen die gevoelige of essentiële informatie en informatieverwerkende faciliteiten bevatten.	v	v	v		
A.11.1.2	Fysieke toegangsbeveiliging	Beveiligde gebieden moeten worden beschermd door passende toegangsbeveiliging om ervoor te zorgen dat alleen bevoegd personeel toegang krijgt.	v	v	v		
A.11.1.3	Kantoren, ruimten en faciliteiten beveiligen	Voor kantoren, ruimten en faciliteiten moet fysieke beveiliging worden ontworpen en toegepast.	v	v	v		
A.11.1.4	Beschermen tegen bedreigingen van buitenaf	Tegen natuurrampen, kwaadwillige aanvallen of ongelukken moet fysieke bescherming worden ontworpen en toegepast.	v	v	v		
A.11.1.5	Werken in beveiligde gebieden	Voor het werken in beveiligde gebieden moeten procedures worden ontwikkeld en toegepast.	v	v	v		
A.11.1.6	Laad- en loslocatie	Toegangspunten zoals laad- en loslocaties en andere punten waar onbevoegde personen het terrein kunnen betreden, moeten worden beheerst, en zo mogelijk worden afgeschermd van informatieverwerkende faciliteiten om onbevoegde toegang te vermijden.	v	v	v		

A.11.2	Apparatuur	Verlies, schade, diefstal of compromittering van bedrijfsmiddelen en onderbreking van de bedrijfsvoering van de organisatie voorkomen.					
A.11.2.1	Plaatsing en bescherming van apparatuur	Apparatuur moet zo worden geplaatst en beschermd dat risico's van bedreigingen en gevaren van buitenaf, alsook de kans op onbevoegde toegang worden verkleind.	v	v	v		
A.11.2.2	Nutsvoorzieningen	Apparatuur moet worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door ontregelingen in nutsvoorzieningen.	v	v	v		
A.11.2.3	Beveiliging van bekabeling	Voedings- en telecommunicatiekabels voor het versturen van gegevens of die informatiediensten ondersteunen, moeten worden beschermd tegen interceptie, verstoring of schade.	v	v	v		
A.11.2.4	Onderhoud van apparatuur	Apparatuur moet correct worden onderhouden om de continue beschikbaarheid en integriteit ervan te waarborgen.	v	v	v		
A.11.2.5	Verwijdering van bedrijfsmiddelen	Apparatuur, informatie en software mogen niet van de locatie worden meegenomen zonder voorafgaande goedkeuring.	v	v	v		
A.11.2.6	Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein	Bedrijfsmiddelen die zich buiten het terrein bevinden, moeten worden beveiligd, waarbij rekening moet worden gehouden met de verschillende risico's van werken buiten het terrein van de organisatie.	v	v	v		
A.11.2.7	Veilig verwijderen of hergebruiken van apparatuur	Alle onderdelen van de apparatuur die opslagmedia bevatten, moeten worden geverifieerd om te waarborgen dat gevoelige gegevens en in licentie gegeven software voorafgaand aan verwijdering of hergebruik zijn verwijderd of veilig zijn overschreven.	Sv	Sv	Sv	Belangrijk hierbij is dat wanneer apparatuur wordt verwijderd/hergebruikt of anderszins er gecontroleerd moet worden dat gevoelige gegevens (bijv. persoonsgegevens, metagegevens, routeringstabellen, etc.) onleesbaar worden gemaakt.	
A.11.2.8	Onbeheerde gebruikersapparatuur	Gebruikers moeten ervoor zorgen dat onbeheerde apparatuur voldoende beschermd is.	Sv	Sv	Sv		
A.11.2.9	'Clear desk'- en 'clear screen'-beleid	Er moet een 'clear desk'-beleid voor papieren documenten en verwijderbare opslagmedia en een 'clear screen'-beleid voor informatieverwerkende faciliteiten worden ingesteld.	Sv	Sv	Sv		
A.12	**Beveiliging bedrijfsvoering**						
A.12.1	Bedieningsprocedures en verantwoordelijkheden	Correcte en veilige bediening van informatieverwerkende faciliteiten waarborgen.					
A.12.1.1	Gedocumenteerde bedieningsprocedures	Bedieningsprocedures moeten worden gedocumenteerd en beschikbaar gesteld aan alle gebruikers die ze nodig hebben.	Sv	Sv	S		Specifiek voor BO: De BO beheert de procedures, instructies, e.d. die betrekking hebben op het Stelsel.
A.12.1.2	Wijzigingsbeheer	Veranderingen in de organisatie, bedrijfsprocessen, informatieverwerkende faciliteiten en systemen die van invloed zijn op de informatiebeveiliging moeten worden beheerst.	S	S	S		Specifiek voor BO: Alle wijzigingen op het Stelsel worden behandeld conform Proces change en release
A.12.1.3	Capaciteitsbeheer	Het gebruik van middelen moet worden gemonitord en afgestemd, en er moeten verwachtingen worden opgesteld voor toekomstige capaciteitseisen om de vereiste systeemprestaties te waarborgen.	S	S	S	Maatregel moet gezien worden in het kader van de Service Level afspraken.	Conform Service level
A.12.1.4	Scheiding van ontwikkel-, test- en productieomgevingen	Ontwikkel-, test- en productieomgevingen moeten worden gescheiden om het risico van onbevoegde toegang tot of veranderingen aan de productieomgeving te verlagen.	S	S	S	BO is verantwoordelijk voor de coördinatie van de (keten)testen bij wijzigingen en van nieuwe toetreders in het netwerk met behulp van de simulatie-/testtool.	Conform Operationeel handboek en Service level. Het Stelsel hanteert een O, TA en P omgeving en een pre-productie omgeving. Voor de beschikbaarheid en inrichting van het testnetwerk zijn eisen gesteld.
A.12.2	Bescherming tegen malware	Waarborgen dat informatie en informatieverwerkende faciliteiten beschermd zijn tegen malware.					
A.12.2.1	Beheersmaatregelen tegen malware	Ter bescherming tegen malware moeten beheersmaatregelen voor detectie, preventie en herstel worden geïmplementeerd, in combinatie met een passend bewustzijn van gebruikers.	Sv	Sv	Sv	Iedere organisatie neemt adequate maatregelen tegen virussen en malware. Bij 'doorbraken' dient onderzocht te worden wat de impact op het netwerk c.q. stelsel is.	
A.12.3	Back-up	Beschermen tegen het verlies van gegevens.					
A.12.3.1	Back-up van informatie	Regelmatig moeten back-upkopieën van informatie, software en systeemafbeeldingen worden gemaakt en getest in overeenstemming met een overeengekomen back-upbeleid.	Sv	Sv	Sv	Back-up strategie moet minimaal de SLA ondersteunen. Additioneel afspraken over: • "dienst" zoals benoemd in SLA: inclusief gegevens die met de dienst beheerd worden, • maximaal dataverlies • afspraken m.b.t. classificatie van gegevens hebben tevens betrekking op de back-up	
A.12.4	Verslaglegging en monitoren	Gebeurtenissen vastleggen en bewijs verzamelen.					

A.12.4.1	Gebeurtenissen registreren	Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, moeten worden gemaakt, bewaard en regelmatig worden beoordeeld.	S	S	S	Deze maatregel omvat het loggen van transacties, incidenten, foutmeldingen e.d.	Conform Beleid voor informatiebeveiliging en 1. Elke Deelnemer en BSNk moet het volledige HTTP bericht van binnenkomende communicatie als gevolg van Elektronische Toegangsdiensten loggen. Elke Deelnemer en BSNk moet alle uitgaande SAML berichten loggen. 2. Een Deelnemer en BSNk moet op basis van logging inzicht kunnen geven in het totaal aantal geslaagde transacties (succesvolle responses op verstuurde requests) en het totaal aantal foutieve transacties (requests zonder response of met een foutmelding als response) in een periode. 3. Elke Deelnemer en BSNk moet alle door haar ondertekende en alle door haar ontvangen ondertekende berichten minimaal 7 jaar archiveren. Na deze periode moeten ten minste de in deze berichten voorkomende persoonsgegevens vernietigd worden tenzij noodzaak kan worden aangetoond om deze langer te bewaren 4. Authenticatiediensten moeten bij de gearchiveerde berichten een referentie naar het gebruikte middel opslaan, zodat de audit trail naar de gebruiker sluitend wordt. 5. Machtigingenregisters moeten bij de gearchiveerde berichten een referentie naar de geregistreerde bevoegdheid waarop de verklaring van bevoegdheid berust opslaan, zodat de audit trail naar de machtigingsverlener sluitend wordt. 6. Authenticatiediensten en Machtigingenregisters moeten bewijsstukken die zijn gebruikt bij uitgifte/registratie van middelen of machtigingen 7 jaar archiveren zodat de audittrail naar gebruiker of machtingsverlener sluitend wordt, tenzij beargumenteerd wordt waarom dit niet wordt gearchiveerd
A.12.4.2	Beschermen van informatie in logbestanden	Logfaciliteiten en informatie in logbestanden moeten worden beschermd tegen vervalsing en onbevoegde toegang.	Sv	Sv	Sv	Dient aan te sluiten op de vereiste historie voor b.v. fraudeonderzoek (geen relatie met archivering), b.v. passend bij 6 maanden periode voor terugzoeken transacties en handelingen op kritieke systemen	Elke deelnemer en BSNk moet logging beveiligd opslaan en moet deze alleen toegankelijk maken voor bevoegde personen. Een deelnemer mag logging niet verwijderen binnen de verplichte bewaartermijn.
A.12.4.3	Logbestanden van beheerders en operators	Activiteiten van systeembeheerders en -operators moeten worden vastgelegd en de logbestanden moeten worden beschermd en regelmatig worden beoordeeld.	Sv	Sv	Sv		Deelnemers, BSNk en BO vullen dit naar eigen inzicht in, maar moet wel in VvT.
A.12.4.4	Kloksynchronisatie	De klokken van alle relevante informatieverwerkende systemen binnen een organisatie of beveiligingsdomein moeten worden gesynchroniseerd met één referentietijdbron.	S	S	v	Noodzakelijk voor goede berichtenafhandeling, er dient een eenduidige tijdsbron te worden gedefinieerd en gebruikt	Conform Interface specifications. Afspraken omtrent tijdsynchronisatie zijn opgenomen in Synchronize system clocks.

A.12.5	Beheersing van operationele software	De integriteit van operationele systemen waarborgen.	v	v	v		Deelnemers, BSNk en BO vullen dit naar eigen inzicht in
A.12.5.1	Software installeren op operationele systemen	Om het op operationele systemen installeren van software en moeten procedures worden geïmplementeerd.	v	v	v		Deelnemers, BSNk en BO vullen dit naar eigen inzicht in.
A.12.6	Beheer van technische kwetsbaarheden	Benutting van technische kwetsbaarheden voorkomen.					
A.12.6.1	Beheer van technische kwetsbaarheden	Informatie over technische kwetsbaarheden van informatiesystemen die worden gebruikt moet tijdig worden verkregen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden moet worden geëvalueerd en passende maatregelen moeten worden genomen om het risico dat ermee samenhangt aan te pakken.	Sv	Sv	S	Er wordt een hoog niveau van beveiliging verwacht. Specifiek wordt van de deelnemer verwacht dat deze zelf de ontwikkelde informatiesystemen test op alle bekende technische kwetsbaarheden in de broncode (test/audittools) en werking van het informatiesysteem (penetratietesten). Daarnaast dient conform de afspraken in het afsprakenstelsel periodiek, op initiatief van de beheerorganisatie, een penetratietest te worden uitgevoerd op het netwerk en de specifieke systemen van een deelnemer en het BSNk.	1. De deelnemers, BSNk en de beheerorganisatie moe ten ten minste tweemaal per jaar een penetratietest laten uitvoeren. 2. In het geval dat de beheerorganisatie penetratietesten organiseert ten behoeve van het stelsel dan moeten deelnemers en BSNk hier aan meewerken.
A.12.6.2	Beperkingen voor het installeren van software	Voor het door gebruikers installeren van software moeten regels worden vastgesteld en geïmplementeerd.	v	v	v		Deelnemers, BSNk en BO vullen dit naar eigen inzicht in.
A.12.7	Overwegingen betreffende audits van informatiesystemen	De impact van auditactiviteiten op uitvoeringssystemen zo gering mogelijk maken.					
A.12.7.1	Beheersmaatregelen betreffende audits van informatiesystemen	Auditeisen en -activiteiten die verificatie van uitvoeringssystemen met zich meebrengen, moeten zorgvuldig worden gepland en afgestemd om bedrijfsprocessen zo min mogelijk te verstoren.	Sv	Sv	S		Deelnemers, BSNk en BO vullen dit naar eigen inzicht in, maar moet wel in VvT. BO beheert de auditeisen i.e. normenkaders.
A.13	**Communicatiebeveiliging**						
A.13.1	Beheer van netwerkbeveiliging	De bescherming van informatie in netwerken en de ondersteunende informatieverwerkende faciliteiten waarborgen				Beveiligen van verbindingen en ondertekenen van berichten MOET gebeuren conform de specificaties in de koppelvlakbeschrijvingen	
A.13.1.1	Beheersmaatregelen voor netwerken	Netwerken moeten worden beheerd en beheerst om informatie in systemen en toepassingen te beschermen.	S	S	S	Netwerkverkeer tussen deelnemers onderling, tussen deelnemers en dienstverleners en tussen deelnemers en dienstafnemers.	Conform Interface specifications
A.13.1.2	Beveiliging van netwerkdiensten	Beveiligingsmechanismen, dienstverleningsniveaus en beheerseisen voor alle netwerkdiensten moeten worden geïdentificeerd en opgenomen in overeenkomsten betreffende netwerkdiensten. Dit geldt zowel voor diensten die intern worden geleverd als voor uitbestede diensten.	S	S	S	Beheerorganisatie is verantwoordelijk voor doorvertaling maatregelen naar onderlinge afspraken in het afsprakenstelsel. Let ook op doorvertaling naar onderaannemers van de deelnemers.	Conform Interface specifications en BSNk mag uitsluitend pakketten die van trusted IP-adressen komen (white listing) accepteren.
A.13.1.3	Scheiding in netwerken	Groepen van informatiediensten, -gebruikers en -systemen moeten in netwerken worden gescheiden.	v	v	v		Deelnemers, BSNk en BO vullen dit naar eigen inzicht in.
A.13.2	Informatietransport	Handhaven van de beveiliging van informatie die wordt uitgewisseld binnen een organisatie en met een externe entiteit.					
A.13.2.1	Beleid en procedures voor informatietransport	Ter bescherming van het informatietransport, dat via alle soorten communicatiefaciliteiten verloopt, moeten formele beleidsregels, procedures en beheersmaatregelen voor transport van kracht zijn.	S	S	S		Conform Information security requirements. Beleid, procedures en afspraken met betrekking tot de uitwisseling van informatie en programmatuur tussen Deelnemers, BSNk en BO is vastgelegd in het Afsprakenstelsel.
A.13.2.2	Overeenkomsten over informatietransport	Overeenkomsten moeten betrekking hebben op het beveiligd transporteren van bedrijfsinformatie tussen de organisatie en externe partijen.	S	S	S		Betreft uitwisseling van informatie en programmatuur tussen deelnemers, BSNk en BO.
A.13.2.3	Elektronische berichten	Informatie die is opgenomen in elektronische berichten moet passend beschermd zijn.	S	S	S		Conform Interface specifications

A.13.2.4	Vertrouwelijkheids- of geheimhoudingsovereenkomst	Eisen voor vertrouwelijkheids- of geheimhoudingsovereenkomsten die de behoeften van de organisatie betreffende het beschermen van informatie weerspiegelen moeten worden vastgesteld, regelmatig worden beoordeeld en gedocumenteerd.	Sv	Sv	Sv	Uit risico-analyse zal moeten blijken dat toegang tot bepaalde gegevens extra aandacht voor of eisen ten aanzien van de geheimhoudingsplicht zal vereisen.	Het betreft tenminste die gegevens die persoons- en bedrijfsgevoelige elementen bevatten zoals: • bij MU: registaties van personen en middelen, • bij AD: persistent pseudoniem, authenticatiecredentials • bij MR: registraties van personen, bedrijven en machtigingen • bij BSNk: BSN en persistent pseudoniem • bij BO: commerciële informatie deelnemers, metagegevens. Geheimhoudingsovereenkomsten (non-disclosure agreements) worden geacht de eisen ten aanzien van deze gegevens te reflecteren of te omvatten. Het is niet noodzakelijk om betreffende gegevens expliciet in de geheimhoudingsverklaring op te nemen.
A.14	**Acquisitie, ontwikkeling en onderhoud van informatiesystemen**						
A.14.1	Beveiligingseisen voor informatiesystemen	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.					
A.14.1.1	Analyse en specificatie van informatiebeveiligingseisen	De eisen die verband houden met informatiebeveiliging moeten worden opgenomen in de eisen voor nieuwe informatiesystemen of voor uitbreidingen van bestaande informatiesystemen.	Sv	Sv	Sv		Deelnemers, BSNk en BO vullen dit naar eigen inzicht in, maar moet wel in VvT.
A.14.1.2	Toepassingsdiensten op openbare netwerken beveiligen	Informatie die deel uitmaakt van uitvoerings diensten en die via openbare netwerken wordt uitgewisseld, moet worden beschermd tegen frauduleuze activiteiten, geschillen over contracten en onbevoegde openbaarmaking en wijziging.	Sv	Sv	S		BO is verantwoordelijk voor het beheer van de openbaar beschikbare informatie van het Stelsel. Van belang is bijv dat informatie over het stelsel juist is en consistent is met de informatie die deelnemers openbaar maken.
A.14.1.3	Transacties van toepassingsdiensten beschermen	Informatie die deel uitmaakt van transacties van toepassingsdiensten moet worden beschermd ter voorkoming van onvolledige overdracht, foutieve routering, onbevoegd wijzigen van berichten, onbevoegd openbaar maken, onbevoegd vermenigvuldigen of afspelen.	S	S	S	Implementatie conform de relevante koppelvlakspecificaties.	Conform Interface specifications, waarbij te allen tijde een of meerdere versies geïmplementeerd dienen te zijn die door het afsprakenstelsel zijn toegestaan.
A.14.2	Beveiliging in ontwikkelings- en ondersteunende processen	Bewerkstelligen dat informatiebeveiliging wordt ontworpen en geïmplementeerd binnen de ontwikkelingslevenscyclus van informatiesystemen.					
A.14.2.1	Beleid voor beveiligd ontwikkelen	Voor het ontwikkelen van software en systemen moeten regels worden vastgesteld en op ontwikkelactiviteiten binnen de organisatie worden toegepast.	Sv	Sv	Sv		Deelnemers, BSNk en BO vullen dit naar eigen inzicht in, maar moet wel in VvT.
A.14.2.2	Procedures voor wijzigingsbeheer met betrekking tot systemen	Wijzigingen aan systemen binnen de levenscyclus van de ontwikkeling moeten worden beheerst door het gebruik van formele controleprocedures voor wijzigingsbeheer.	S	S	S		Conform Proces change en release.
A.14.2.3	Technische beoordeling van toepassingen na wijzigingen bedieningsplatform	Als bedieningsplatforms zijn veranderd, moeten bedrijfskritische toepassingen worden beoordeeld en getest om te waarborgen dat er geen nadelige impact is op de activiteiten of de beveiliging van de organisatie.	Sv	Sv	Sv	Van belang voor betrouwbaarheid netwerk. Specifiek wordt van Deelnemers, BSNk en Beheerorganisatie een zorgvuldig proces verwacht ten aanzien van wijzigingen in relatie tot de andere partijen en adequaat patch- en updatebeleid.	Deelnemers, BSNk en BO vullen dit naar eigen inzicht in.
A.14.2.4	Beperkingen op wijzigingen aan softwarepakketten	Wijzigingen aan softwarepakketten moeten worden ontraden, beperkt tot noodzakelijke veranderingen en alle veranderingen moeten strikt worden gecontroleerd.	S	S	S		Conform Proces change en release. Restricties kunnen volgen uit de besluiten van het Tactisch Beraad.
A.14.2.5	Principes voor engineering van beveiligde systemen	Principes voor de engineering van beveiligde systemen moeten worden vastgesteld, gedocumenteerd, onderhouden en toegepast voor alle verrichtingen betreffende het implementeren van informatiesystemen.	v	v	v		Deelnemers, BSNk en BO vullen dit naar eigen inzicht in.
A.14.2.6	Beveiligde ontwikkelomgeving	Organisaties moeten beveiligde ontwikkelomgevingen vaststellen en passend beveiligen voor verrichtingen op het gebied van systeemontwikkeling en integratie die betrekking hebben op de gehele levenscyclus van de systeemontwikkeling.	v	v	v		Deelnemers, BSNk en BO vullen dit naar eigen inzicht in.

A.14.2.7	Uitbestede softwareontwikkeling	Uitbestede systeemontwikkeling moet onder supervisie staan van en worden gemonitord door de organisatie.	Sv	Sv	Sv	Bij uitbesteding van ontwikkelwerkzaamheden aan een onderaannemer, dienen de stelselspecifieke eisen ten aanzien van het te ontwikkelen product doorvertaald te worden naar de onderaannemer.	Deelnemers, BSNk en BO vullen dit naar eigen inzicht in.
A.14.2.8	Testen van systeembeveiliging	Tijdens ontwikkelactiviteiten moet de beveiligingsfunctionaliteit worden getest.	Sv	Sv	Sv	Bij uitbesteding van ontwikkelwerkzaamheden aan een onderaannemer, dienen de stelselspecifieke eisen ten aanzien van het te ontwikkelen product doorvertaald te worden naar de onderaannemer.	Deelnemers, BSNk en BO vullen dit naar eigen inzicht in.
A.14.2.9	Systeemacceptatietests	Voor nieuwe informatiesystemen, upgrades en nieuwe versies moeten programma's voor het uitvoeren van acceptatietests en gerelateerde criteria worden vastgesteld.	S	S	S	Bij wijzigingen, onderhoud en verstoringen dienen stelselspecifieke afspraken gevolgd te worden.	Conform Operationeel handboek
A.14.3	Testgegevens	Bescherming waarborgen van gegevens die voor het testen zijn gebruikt.					
A.14.3.1	Bescherming van testgegevens	Testgegevens moeten zorgvuldig worden gekozen, beschermd en gecontroleerd.	Sv	Sv	S		Conform Testing.
A.15	**Leveranciersrelaties**						
A.15.1	Informatiebeveiliging in leveranciersrelaties	De bescherming waarborgen van bedrijfsmiddelen van de organisatie die toegankelijk zijn voor leveranciers.					
A.15.1.1	Informatiebeveiligingsbeleid voor leveranciersrelaties	Met de leverancier moeten de informatiebeveiligingseisen om risico's te verlagen die verband houden met de toegang van de leverancier tot de bedrijfsmiddelen van de organisatie, worden overeengekomen en gedocumenteerd.	v	v	v		Deelnemers, BSNk en BO vullen dit naar eigen inzicht in.
A.15.1.2	Opnemen van beveiligingsaspecten in leveranciersovereenkomsten	Alle relevante informatiebeveiligingseisen moeten worden vastgesteld en overeengekomen met elke leverancier die toegang heeft tot IT-infrastructuurelementen ten behoeve van de informatie van de organisatie, of deze verwerkt, opslaat, communiceert of biedt.	Sv	Sv	Sv	Bij uitbesteding (deel) van de rol/activiteiten aan een onderaannemer, dienen de stelselspecifieke (beveiligings)eisen doorvertaald te worden, de opdrachtgever (deelnemer, BSNk,BO) blijft verantwoordelijk.	Iedere overeenkomst met een derde moet een paragraaf/onderdeel te bevatten met eisen ten aanzien van informatiebeveiliging. Deze eisen moeten zijn gebaseerd op een risicoanalyse.
A.15.1.3	Toeleveringsketen van informatie- en communicatietechnologie	Overeenkomsten met leveranciers moeten eisen bevatten die betrekking hebben op de informatiebeveiligingsrisico's in verband met de toeleveringsketen van de diensten en producten op het gebied van informatie- en communicatietechnologie.	Sv	Sv	Sv	Bij uitbesteding (deel) van de rol/activiteiten aan een onderaannemer, dienen de stelselspecifieke (beveiligings)eisen doorvertaald te worden, de opdrachtgever (deelnemer, BSNk,BO) blijft verantwoordelijk.	Iedere overeenkomst met een derde moet een paragraaf/onderdeel te bevatten met eisen ten aanzien van informatiebeveiliging m.b.t. de toeleveringsketen. Deze eisen moeten zijn gebaseerd op een risicoanalyse.
A.15.2	Beheer van dienstverlening van leveranciers	Een overeengekomen niveau van informatiebeveiliging en dienstverlening in overeenstemming met de leveranciersovereenkomsten handhaven.					
A.15.2.1	Monitoring en beoordeling van dienstverlening van leveranciers	Organisaties moeten regelmatig de dienstverlening van leveranciers monitoren, beoordelen en auditen.	Sv	Sv	Sv		Deelnemers, BSNk en BO vullen dit naar eigen inzicht in.
A.15.2.2	Beheer van veranderingen in dienstverlening van leveranciers	Veranderingen in de dienstverlening van leveranciers, met inbegrip van handhaving en verbetering van bestaande beleidslijnen, procedures en beheersmaatregelen voor informatiebeveiliging, moeten worden beheerd, rekening houdend met de kritikaliteit van bedrijfsinformatie, betrokken systemen en processen en herbeoordeling van risico's.	Sv	Sv	Sv		Deelnemers, BSNk en BO vullen dit naar eigen inzicht in.
A.16	**Beheer van informatiebeveiligingsincidenten**						
A.16.1	Beheer van informatiebeveiligingsincidenten en -verbeteringen	Een consistente en doeltreffende aanpak bewerkstelligen van het beheer van informatiebeveiligingsincidenten, met inbegrip van communicatie over beveiligingsgebeurtenissen en zwakke plekken in de beveiliging.					
A.16.1.1	Verantwoordelijkheden en procedures	Directieverantwoordelijkheden en -procedures moeten worden vastgesteld om een snelle, doeltreffende en ordelijke respons op informatiebeveiligingsincidenten te bewerkstelligen.	S	S	S	Er dient per deelnemer en voor BSNk een contactpersoon te zijn voor coördinatie van beveiligingsincidenten. De centrale coördinatie wordt gedaan door de beheerorganisatie.	Conform Proces incidentmanagement.
A.16.1.2	Rapportage van informatiebeveiligingsgebeurtenissen	Informatiebeveiligingsgebeurtenissen moeten zo snel mogelijk via de juiste leidinggevende niveaus worden gerapporteerd.	S	S	S	-	Conform Proces incidentmanagement.
A.16.1.3	Rapportage van zwakke plekken in de informatiebeveiliging	Van medewerkers en contractanten die gebruikmaken van de informatiesystemen en -diensten van de organisatie moet worden geëist dat zij de in systemen of diensten waargenomen of vermeende zwakke plekken in de informatiebeveiliging registreren en rapporteren.	S	S	S	-	Conform Proces incidentmanagement.
A.16.1.4	Beoordeling van en besluitvorming over informatiebeveiligingsgebeurtenissen	Informatiebeveiligingsgebeurtenissen moeten worden beoordeeld en er moet worden geoordeeld of zij moeten worden geclassificeerd als informatiebeveiligingsincidenten.	S	S	S	-	Conform Proces incidentmanagement.
A.16.1.5	Respons op informatiebeveiligingsincidenten	Op informatiebeveiligingsincidenten moet worden gereageerd in overeenstemming met de gedocumenteerde procedures.	S	S	S	-	Conform Proces incidentmanagement.

A.16.1.6	Lering uit informatiebeveiligingsincidenten	Kennis die is verkregen door informatiebeveiligingsincidenten te analyseren en op te lossen moet worden gebruikt om de waarschijnlijkheid of impact van toekomstige incidenten te verkleinen.	S	S	S	Iedere organisatie dient de beveiligingsincidentregistraties en -rapportages te evalueren op trends en verbeterpunten	Periodiek moeten trend-analyses van incidenten worden gemaakt en besproken in het security officers overleg bestaande uit de de security officers van deelnemers, BSNk en BO. Indien mogelijk en beschikbaar deelt de BO de analyses van het NCSC met de deelnemers.
A.16.1.7	Verzamelen van bewijsmateriaal	De organisatie moet procedures definiëren en toepassen voor het identificeren, verzamelen, verkrijgen en bewaren van informatie die als bewijs kan dienen.	S	S	S	Bij aanleiding tot onderzoek (intern het stelsel of op verzoek van opsporingsinstanties) dient relevante informatie voor een transactie door de keten van de deelnemers heen verzameld te kunnen worden.	Conform Beleid voor informatiebeveiliging.
A.17	**Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer**						
A.17.1	Informatiebeveiligingscontinuïteit	Informatiebeveiligingscontinuïteit moet worden ingebed in de systemen van het bedrijfscontinuïteitsbeheer van de organisatie.					
A.17.1.1	Informatiebeveiligingscontinuïteit	De organisatie moet haar eisen voor informatiebeveiliging en voor de continuïteit van het informatiebeveiligingsbeheer in ongunstige situaties, bijv. een crisis of een ramp, vaststellen.	Sv	Sv	S	Alle Rollen (inclusief BSNk) en BO: Bedrijfscontinuïteit is van belang voor het imago van het netwerk. In te vullen n.a.v. risicoanalyse voor het halen van de service levels. Ook aandacht besteden aan maatregelen voor herstel van de dienstverlening na een calamiteit.	Deelnemers, BSNk en de BO moeten maatregelen nemen op basis van een risicobeoordeling en de SLA. Hierbij moet rekening worden gehouden met processen die zijn uitbesteed processen. Op stelselniveau moet de bedrijfscontinuïteit worden gemonitord door de BO.
A.17.1.2	Informatiebeveiligingscontinuïteit implementeren	De organisatie moet processen, procedures en beheersmaatregelen vaststellen, documenteren, implementeren en handhaven om het vereiste niveau van continuïteit voor informatiebeveiliging tijdens een ongunstige situatie te waarborgen.	Sv	Sv	S	Stelseltaak voor BO	Conform Service level
A.17.1.3	Informatiebeveiligingscontinuïteit verifiëren, beoordelen en evalueren	De organisatie moet de ten behoeve van informatiebeveiligingscontinuïteit vastgestelde en geïmplementeerde beheersmaatregelen regelmatig verifiëren om te waarborgen dat ze deugdelijk en doeltreffend zijn tijdens ongunstige situaties.	Sv	Sv	S	Stelseltaak voor BO	Conform Service level
A.17.2	Redundante componenten	Beschikbaarheid van informatieverwerkende faciliteiten bewerkstelligen.					
A.17.2.1	Beschikbaarheid van informatieverwerkende faciliteiten	Informatieverwerkende faciliteiten moeten met voldoende redundantie worden geïmplementeerd om aan beschikbaarheidseisen te voldoen.	Sv	Sv	Sv	-	Conform Service level. De BO moet de mate van redundantie van rollen in het Stelsel monitoren.
A.18.	**Naleving**						
A.18.1	Naleving van wettelijke en contractuele eisen	Voorkomen van schendingen van wettelijke, statutaire, regelgevende of contractuele verplichtingen betreffende informatiebeveiliging en beveiligingseisen.					
A.18.1.1	Vaststellen van toepasselijke wetgeving en contractuele eisen	Alle relevante wettelijke statutaire, regelgevende, contractuele eisen en de aanpak van de organisatie om aan deze eisen te voldoen moeten voor elk informatiesysteem en de organisatie expliciet worden vastgesteld, gedocumenteerd en actueel gehouden.	Sv	Sv	Sv	-	Conform Juridisch kader. Deelnemers, BSNk en BO moeten zelf een overzicht vast te stellen van toepasselijke wetgeving en contractuele eisen.
A.18.1.2	Intellectuele eigendomsrechten	Om de naleving van wettelijke, regelgevende en contractuele eisen in verband met intellectuele-eigendomsrechten en het gebruik van eigendomssoftwareproducten te waarborgen moeten passende procedures worden geïmplementeerd.	Sv	Sv	Sv		Deelnemers, BSNk en BO dienen dit zelf in te vullen. De Eigenaar van het stelsel moet de verantwoordelijkheid nemen voor borging van de IPR betreffende stelselbrede rechten zoals het merkenrecht.
A.18.1.3	Beschermen van registraties	Registraties moeten in overeenstemming met wettelijke, regelgevende, contractuele en bedrijfseisen worden beschermd tegen verlies, vernietiging, vervalsing, onbevoegde toegang en onbevoegde vrijgave.	Sv	Sv	Sv	Beschermingsniveau afhankelijk van classificatie.	Conform Juridisch kader en Operationeel handboek
A.18.1.4	Privacy en bescherming van persoonsgegevens	Privacy en bescherming van persoonsgegevens moeten, voor zover van toepassing, worden gewaarborgd in overeenstemming met relevante wet- en regelgeving.	Sv	Sv	Sv	Er behoort door de Deelnemers, BSNk en de BO een beleid voor bescherming van persoonsgegevens te worden ontwikkeld en ingevoerd. Dit beleid behoort te worden gecommuniceerd naar alle personen die betrokken zijn bij het verwerken van persoonsgegevens.	Conform Privacybeleid en Normenkader betrouwbaarheidsniveaus. En specifiek betreft dit het omgaan met persoonsgegevens i.c. het gebruik van pseudoniemen binnen het netwerk.
A.18.1.5	Voorschriften voor het gebruik van cryptografische beheersmaatregelen	Cryptografische beheersmaatregelen moeten worden toegepast in overeenstemming met alle relevante overeenkomsten, wet- en regelgeving.	S	S	S	-	Conform Juridisch kader en Interface specifications.

A.18.2	Informatiebeveiligingsbeoordelingen	Verzekeren dat informatiebeveiliging wordt geïmplementeerd en uitgevoerd in overeenstemming met de beleidsregels en procedures van de organisatie.					
A.18.2.1	Onafhankelijke beoordeling van informatiebeveiliging	De aanpak van de organisatie ten aanzien van het beheer van informatiebeveiliging en de implementatie ervan (bijv. beheersdoelstellingen, beheersmaatregelen, beleidsregels, processen en procedures voor informatiebeveiliging), moeten onafhankelijk en met geplande tussenpozen of zodra zich belangrijke veranderingen voordoen worden beoordeeld.	S	S	S	Voor de deelnemers, het BSNk en de Beheerorganisatie gaat het om het laten uitvoeren van (interne en externe) audits en reviews. Onderdeel van de ISO 27001 certificering is het periodiek/jaarlijks uitvoeren van een controleaudit door de certificerende organisatie.	1. De beheersmaatregelen uit dit document moeten door deelnemers (afhankelijk van hun rol(len) in het stelsel) in hun individuele VvT worden opgenomen. a. Verplichte maatregelen uit het Gemeenschappelijk normenkader informatiebeveiliging mogen niet ontbreken in de VvT. Voor dit type maatregel zijn er op stelselniveau reeds uitwerkingen vastgesteld zoals koppelvlakspecificaties, operationeel handboek en procedure- en procesbeschrijvingen. b. Overige gemeenschappelijke maatregelen zijn maatregelen die de deelnemer of beheerorganisatie vanuit zijn rol zou moeten nemen. De deelnemer mag de beheersmaatregel 'niet van toepassing' verklaren maar in dat geval moet deze uitsluiting met argumenten zijn omkleed in de VvT. 2. Deelnemers moeten binnen 3 maanden na vaststelling van de bijstelling van het Gemeenschappelijk normenkader informatiebeveiliging deze hebben geïmplementeerd tenzij het Tactisch Beraad anders besluit.

							3. Deelnemers die voor het eerst willen toetreden en de genoemde certificaten of TPM's nog niet kunnen overleggen moeten om te worden toegelaten: • zelf verklaren dat zij aan de materiële eisen van ISO 27001 (inclusief het Gemeenschappelijk Normenkader) voldoen, alsmede aan de gestelde eisen voor de dienstverlening van de betrouwbaarheidsniveaus die geleverd gaan worden. • voorbereidingen in gang hebben gezet voor de ISO 27001 certificatie en /of een TPM van het managementsysteem voor informatiebeveiliging, zoals bedoeld in ISO 27001, alsook de specifieke eisen die zijn gesteld aan de betrouwbaarheidsniveaus van de te leveren diensten. • een risicoanalyse overleggen die op de Elektronische Toegangsdiensten betrekking heeft (en de Stelselrisicoanalyse als input heeft) met daarin aangegeven de reeds genomen, nog te nemen maatregelen en de restrisico's. • een GAP-analyse overleggen waarin ten opzichte van het Gemeenschappelijk normenkader informatiebeveiliging is aangegeven welke maatregelen reeds zijn geïmplementeerd en welke maatregelen nog moeten worden geïmplementeerd. 4. De Beheerorganisatie moet per deelnemer bijhouden welke versie van het normenkader van toepassing was bij de audits in het kader van certificering of TPM.
A.18.2.2	Naleving van beveiligingsbeleid en -normen	De directie moet regelmatig de naleving van de informatieverwerking en -procedures binnen haar verantwoordelijkheidsgebied beoordelen aan de hand van de desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging.	Sv	Sv	S	Opstellen en uitvoeren van een controleplan op basis waarvan procedures regelmatig worden gecontroleerd op naleving.	De Deelnemers, BSNk en BO moeten de naleving van informatiebeveiliging kunnen aantonen. De Toezichthouder op het stelsel toetst de naleving van Stelselafspraken door Deelnemers, BSNk en BO.

A.18.2.3	Beoordeling van technische naleving	Informatiesystemen moeten regelmatig worden beoordeeld op naleving van de beleidsregels en normen van de organisatie voor informatiebeveiliging.	Sv	Sv	S	Opstellen en uitvoeren van een controleplan op basis waarvan informatiesystemen regelmatig worden gecontroleerd op de implementatie van beveiligingsstandaards.	Conform Operationeel handboek. De beheersmaatregel op stelselniveau betreft het (laten) uitvoeren van security assessments zoals pentesten en code reviews.