Informatiebeveiliging

In het DD JGZ worden persoonsgebonden en medische informatie geregistreerd. Deze zijn zeer privacy gevoelig voor de cliënt. Het DD JGZ moet daarom – zowel vanuit ethisch als vanuit wettelijk oogpunt - goed beveiligd zijn. Ongewenste toegang tot gegevens moet zowel binnen als buiten de organisatie voorkomen worden. Het is daarom van belang dat er zorgvuldig met vertrouwelijke gegevens wordt omgegaan. JGZ organisaties zijn wettelijk verplicht (Wet Bescherming Persoonsgegevens) om gegevens goed te beveiligen en medewerkers bewust te maken zorgvuldig met gegevens om te gaan. Daarbij is het de uitdaging voor JGZ organisaties om de toegang laagdrempelig te houden voor de medewerkers. De gebruiksvriendelijkheid van het DD JGZ is een voorwaarde voor succesvol gebruik.

Deze factsheet moet samen met de handreiking aanbevelingen informatiebeveiliging duidelijkheid brengen ten aanzien van het informatiebeveiligingsbeleid van JGZ-organisaties. De aanbevelingen zijn gericht op de harde (technische infrastructuur) en de zachte (organisatie en procedure) kant van informatiebeveiliging. De aanbevelingen betreffen het organisatiebrede beveiligingbeleid, waar het DD JGZ onderdeel van uitmaakt.

Twee beveiligingsniveaus

Omdat persoonsgebonden en medische gegevens privacygevoelig zijn, staat veiligheid voorop. Het is daarom van belang dat JGZ organisaties een goed beheerd zorgsysteem gebruiken. Dit betekent onder andere dat de hard- en software geschikt zijn om gegevens veilig uit te wisselen. Een goede beveiliging is hierbij noodzakelijk. Bij de aanschaf van hard- en software is het van belang met betrouwbare leveranciers in zee te gaan. NICTIZ heeft een Xis-kwalificatiesysteem ontwikkelend voor ICT-leveranciers. Een Xis-leverancier werkt met een zogenaamd typegekwalificeerd zorginformatiesysteem. Dit betekent dat de applicatie voldoet aan de eisen die worden gesteld aan een Goed Beheerd Zorgsysteem (GBZ).

Niet alleen is het intern van belang om de informatiebeveiliging goed te organiseren. Van buitenaf worden JGZ instellingen ook verplicht om een goed beheerd zorgsysteem te hebben. Alleen dan krijgen zij de mogelijkheid om op het landelijke schakelpunt aangesloten te worden. Binnen dit informatiebeveiligingsbeleid onderscheiden wij twee niveaus van informatiebeveiliging:

1. Intern: informatiebeveiliging van de JGZ-organisatie voor het gebruik van het DD JGZ
2. Extern: beveiligingseisen voor aansluiting op het Landelijk Schakelpunt (LSP)

Kaders:

- Wet Bescherming Persoonsgegevens: gaat in op de bewaking van privacy en is wettelijk verplicht
- NEN-normen 7510, 7511 en 7512: richtlijnen voor informatiebeveiliging in de zorg en leidend voor een betrouwbare informatiebeveiliging
- Goed beheerd zorgsysteem (GBZ): eisen waaraan een JGZ organisatie moet voldoen (Xis-kwalificatie voor leveranciers)
- NORA-eis: Het gebruik van het burgerservicenummer en uitwisseling van gegevens
- Inspectie Gezondheidszorg (IGZ): inspecteert de kwaliteit van informatiebeveiliging
- College bescherming persoonsgegevens (CBP): inspecteert de kwaliteit van informatiebeveiliging

Informatiebeveiliging binnen de JGZ-organisaties

Het ministerie ziet erop toe dat de toenemende (elektronische) gegevensuitwisseling goed en vooral ook veilig functioneert. Zij heeft hiertoe de normcommissie 'Informatiebeveiliging in de zorg' gevraagd het 'denkwerk' rondom de NEN7510 te verrichten. De NEN7510 zijn richtlijnen en nog niet wettelijk verplicht. Dit zal in de toekomst waarschijnlijk veranderen. De normcommissie geeft aan dat daarbij rekening wordt gehouden met het feit dat zorgorganisaties van elkaar verschillen in complexiteit. De informatievoorziening van een huisarts verschilt van die van zorgorganisaties. Ook de manier waarop zij hun beveiligingsproblemen oplossen is niet één op één hetzelfde. In het geval van DD JGZ moet rekening worden gehouden met de complexiteit van verschillende samenwerkende organisaties. De te treffen maatregelen voor het waarborgen van informatiebeveiliging verschillen per organisatie, maar moeten desalniettemin op elkaar worden afgestemd. Met het oog op aansluiting op het Landelijk Schakelpunt is het op termijn van belang dat informatiebeveiliging ook landelijk uniform geschied. Een van de maatregelen die deze uniformiteit moet garanderen is de Wet gebruik burgerservicenummer (BSN). Per 1 juni is iedere zorginstelling verplicht om het BSN te gebruiken bij het vastleggen en uitwisselen van cliëntgegevens. Hierdoor worden de cliëntgegevens beter inzichtelijk. De aansluiting op het LSP zorgt voor een betere zorgcoördinatie tussen de verschillende JGZ organisaties.

Het organiseren van informatiebeveiliging is onderhevig aan verschillende richtlijnen. Het instituut voor de NEderlandse Norm (NEN) heeft het belangrijkste kader opgesteld voor informatiebeveiliging in de zorg (de NEN 7510). Deze norm is (nog) geen wettelijke verplichting, maar bevat wel componenten die volgens wettelijke bepalingen geregeld moeten zijn. Vanuit vereisten uit de NEN-normen en de andere richtlijnen (GBZ, NORA, etc.) stellen wij in de bijlage een checklist op voor informatiebeveiliging. De checklist vormt samen met de aanbevelingen een handreiking om informatiebeveiliging te organiseren.

Landelijke informatiearchitectuur eisen

Wanneer informatiebeveiliging op organisatieniveau goed geregeld is, kan landelijke aansluiting plaatsvinden via het LSP. Ook voor deze landelijke aansluiting zijn richtlijnen opgesteld. Een goed functionerende en beveiligde informatievoorziening is een belangrijk onderdeel van de bedrijfsvoering van de overheid. Mede hierom is de NORA-eis (Nederlandse Overheid Referentie Architectuur) opgesteld. De NORA bevat inrichtingsprincipes, modellen en standaarden voor het ontwerp en de inrichting van de elektronische overheid.

De NORA is een naslagwerk voor overheidsorganen over samenwerking in ketens en netwerken. De NORA beschrijft onder andere hoe de samenhang tussen onderdelen van de elektronische overheid beveiligd moet worden. Ook organisaties die informatie uitwisselen met de overheid – zoals de JGZ-organisaties middels het BSN - moeten aan deze eisen voldoen. Aangezien gemeenten verantwoordelijk zijn voor het BSN hebben de JGZ-organisaties te maken met de specificeerde NORA-eis van gemeenten: de GEMMA-eis (GEMeentelijke Model Architectuur). GEMMA is speciaal door EGEM i-teams ontwikkeld voor gemeenten.

Vertrekpunt van de NORA voor wat betreft beveiliging en privacy is dat de individuele organisaties hun zaken op orde hebben. De NEN-normen 7510, 7511 en 7512 geven hier voor de JGZ-organisaties invulling aan. Door het volgen van deze NEN-normen zijn de organisaties dus in staat hun informatiebeveiliging en privacy goed te beheersen en slagvaardig te reageren op verstoringen in hun bedrijfsvoering. Wanneer de NEN-normen zijn opgevolgd bestaan er geen obstakels voor aansluiting op het LSP.

Bijlage - Checklist

Onderstaande checklist is gebaseerd op de NEN 7510 eisen en de GBZ-richtlijnen waaraan moeten worden voldaan wil een organisatie haar informatie volledig beveiligd hebben. Voor iedere organisatie is dit een goed streven. Toch vergt het veel inspanning en tijd om tot een volledig beveiligde informatievoorziening te komen. Met deze reden lichten wij de aspecten uit – *schuin gedrukt* - die voor het DD JGZ specifieke aandacht behoeven. Deze moeten ook op korte termijn in de organisatie ingebed worden. De andere aspecten verdienen echter evenzeer de aandacht om goede informatiebeveiliging in te richten.

De NEN 7510 vormt de basis voor informatiebeveiliging in de interne organisatie. De NEN 7511 en NEN 7512 vormen een verdere uitwerking en toelichting van de NEN 7510. Deze normen zijn een interessante toelichting voor de samenwerking binnen en tussen verschillende zorgaanbieders en de aansluiting op het landelijk schakelpunt. De NEN 7512 geeft richtlijnen voor communicatieprocessen en de risico's die deze voor de gezondheidszorg met zich meebrengen. Het gaat hierbij om de bron van de gegevens, het transportkanaal en de ontvanger van de gegevens. Binnenkort lanceert de NEN ook de richtlijn 7513 die voorbeelden geeft voor het goed gebruik van digitale systemen.

Voor het structureren van de checklist voor informatiebeveiliging verdelen wij de aandachtspunten onder in drie thema's:

1. de organisatorische beveiliging (betreft het beveiligingsbewustzijn)
2. de procedurele beveiliging (betreft de vastlegging in werkwijzen en –processen)
3. de technische beveiliging (betreft de infrastructuur en werkplek beveiliging).

Organisatorische beveiliging

- ☐ *De instelling beschikt over een beleidsdocument voor informatiebeveiliging en er wordt periodiek beoordeeld en geëvalueerd.*
- ☐ *De verantwoordelijkheden voor informatiebeveiliging, bescherming van individuele gegevens en het uitvoeren van bepaalde beveiligingsprocedures zijn duidelijk gedefinieerd en toegewezen binnen de organisatie.*
- ☐ De instelling beschikt over een bron voor specialistisch advies op het gebied van informatiebeveiliging.
- ☐ *De implementatie van maatregelen voor informatiebeveiliging wordt gecoördineerd door hiertoe door de leiding aangewezen vertegenwoordigers.*
- ☐ *Er is een goedkeuringsproces voor de installatie en het in gebruik nemen van nieuwe middelen voor de informatievoorziening.*
- ☐ *Er zijn procedures van kracht die de contacten met officiële instanties regelen en de mogelijkheid geven om incidenten te rapporteren wanneer er een vermoeden bestaat dat er wettelijke bepalingen zijn geschonden.*
- ☐ *De juiste contacten worden onderhouden met communicatiepartners (zoals leveranciers van informatiediensten, telecommunicatiebedrijven en andere zorginstellingen) om ervoor te zorgen dat in geval van een incident snel de benodigde actie kan worden ondernomen en advies kan worden ingewonnen.*
- ☐ De implementatie van informatiebeveiliging wordt periodiek, en bij belangrijke wijzigingen, onafhankelijk beoordeeld.
- ☐ *Er zijn maatregelen genomen tegen de risico's die ontstaan doordat externe gebruikers toegang hebben tot informatieverwerkende voorzieningen.*
- ☐ Er zijn beveiligingsvoorwaarden en bijbehorende sancties gespecificeerd in contracten met derden die betrekking hebben op de toegang tot de informatieverwerkende voorzieningen van de instelling.

- ☐ Er is een overzicht van middelen die worden gebruikt voor de informatievoorziening.
- ☐ *De verantwoordelijkheden zijn bepaald en vastgelegd voor alle gegevens en overige middelen.*
- ☐ *De instelling maakt gebruik van classificatie van gegevens, teneinde het vereiste beveiligingsniveau te kunnen aangeven.*
- ☐ *Er zijn passende procedures opgesteld voor het classificeren en verwerken van gegevens, overeenkomstig met het classificatiesysteem.*

Procedurele beveiliging

- ☐ De verantwoordelijkheden voor informatiebeveiliging zijn opgenomen in de functieomschrijving en vastgelegd in het arbeidscontract van de medewerker.
- ☐ Eigen en externe medewerkers die gebruik maken van middelen voor de informatievoorziening ondertekenen bij het begin van hun dienstverband een geheimhoudingsverklaring.
- ☐ *Personen die onder de wettelijke zwijgplicht vallen zijn van dit feit op de hoogte.*
- ☐ *Alle gebruikers van informatieverwerkende voorzieningen worden op passende wijze getraind in het informatiebeveiligingsbeleid en de bijbehorende procedures.*
- ☐ *Alle medewerkers worden opgeleid om voorlichting te geven aan cliënten omtrent gebruik van BSN en landelijke gegevensuitwisseling.*
- ☐ *Alle medewerkers moeten zich (kunnen) verantwoorden voor het opvragen van gegevens en zijn van dit feit op de hoogte.*
- ☐ *Alle medewerkers worden opgeleid hoe ze om moeten gaan met mogelijke foutmeldingen en problemen.*
- ☐ *Alle medewerkers weten hoe ze melding moeten maken van vermoeden of de constatering van zwakke punten of bedreigingen in het systeem.*
- ☐ Sollicitanten worden ‘gescreend’ alvorens zij worden aangenomen en bepaald wordt welk toezicht nodig is voor nieuw personeel dat geautoriseerd is voor toegang tot gevoelige systemen.
- ☐ Werkzaamheden van medewerkers worden periodiek onderworpen aan een beoordelings- en goedkeuringsprocedure.
- ☐ *De leiding stimuleert medewerkers, contractanten en externe gebruikers om de vastgestelde beveiligingsmaatregelen en procedures in acht te nemen.*
- ☐ Inbreuken op de beveiliging worden disciplinair afgehandeld.
- ☐ Met medewerkers die de instelling verlaten wordt een afsluitingsgesprek gehouden. De verantwoordelijkheden om het proces van vertrek te begeleiden zijn duidelijk gedefinieerd en belegd.
- ☐ *Gewaarborgd is dat alle medewerkers en externe partijen bij het beëindigen van hun contract alle nog in hun bezit zijnde eigendommen van de instelling teruggeven en dat toegangsrechten tot informatiesystemen worden ingetrokken.*

Technische beveiliging

Fysieke ruimten:

- ☐ Er zijn beveiligde zones aangewezen waarin personeel, apparatuur en gegevens kunnen worden beschermd. Deze zones worden beschermd door een adequate toegangscontrole, zodat alleen geautoriseerd personeel toegang kan krijgen.
- ☐ Er is een analyse uitgevoerd van activiteiten die in de directe omgeving van de instelling plaatsvinden.
- ☐ *Bij de keuze en het ontwerp van beveiligde zones en ruimten is rekening gehouden met de mogelijkheid van schade door brand, wateroverlast, explosies, ordeverstoringen en andere natuurlijke of door mensen veroorzaakte calamiteiten.*

- ☐ Aanvullende maatregelen en richtlijnen zijn aanwezig om de beveiliging van beveiligde ruimten te kunnen waarborgen.
- ☐ Laad- en losruimten worden bewaakt en zo mogelijk afgezonderd van de IT-voorzieningen om toegang door ongeautoriseerde personen te voorkomen.

Apparatuur en programmatuur:

- ☐ *Apparatuur wordt zodanig geplaatst en beveiligd dat de risico's van schade en storing van buitenaf en de kansen op ongeautoriseerde toegang of gebruik beperkt zijn. Dit geldt ook voor apparatuur die buiten de instelling wordt gebruikt.*
- ☐ Apparatuur is beveiligd tegen stroomstoringen en andere elektrische storingen.
- ☐ De voedings- en telecommunicatiebekabeling voor gegevensverkeer en/of voor ondersteunende informatiediensten wordt beschermd tegen interceptie en beschadiging.
- ☐ *Alle apparatuur wordt op correcte wijze onderhouden volgens de voorschriften van de leverancier.*
- ☐ *Gevoelige gegevens en gelicentieerde programmatuur wordt verwijderd of overschreven voordat de apparatuur wordt afgevoerd.*
- ☐ *Er is een "clear desk" en "clear screen" beleid ingesteld.*
- ☐ Er zijn maatregelen getroffen om te voorkomen dat het personeel zonder toestemming eigendommen van de instelling meeneemt.
- ☐ *Schriftelijke procedures zijn opgesteld voor de bediening van alle computersystemen.*
- ☐ Er zijn procedures met betrekking tot de controle op wijzigingen in ICT-voorzieningen en systemen.
- ☐ Functiescheiding wordt toegepast om ongeautoriseerde wijzigingen of opzettelijk misbruik van gegevens en diensten te verkleinen.
- ☐ De voorzieningen voor het ontwikkelen en testen van systemen en het opleiden van gebruikers zijn gescheiden van operationele systemen.
- ☐ Procedures zijn aanwezig voor het overdragen van programmatuur van het ontwikkel (of test)stadium naar het productiestadium.
- ☐ In het geval van het uitbesteden van het beheer van middelen zijn passende beveiligingsmaatregelen met de contractant overeen gekomen en zijn in het contract maatregelen overeengekomen die de instelling in staat stellen hierop te controleren?
- ☐ Bij wijzigingen in de dienstverlening worden de eisen ten aanzien van informatiebeveiliging opnieuw betrokken.
- ☐ *Computer en netwerkcapaciteitseisen worden in de gaten gehouden teneinde storingen ten gevolge van een gebrek aan capaciteit te voorkomen.*
- ☐ *Acceptatiecriteria worden gedefinieerd, besproken, gedocumenteerd en getest alvorens nieuwe systemen worden geaccepteerd.*
- ☐ *Er zijn maatregelen ingevoerd voor de preventie en detectie van kwaadaardige programmatuur en er zijn adequate procedures om het bewustzijn van gebruikers te vergroten.*
- ☐ *Er worden regelmatig reservekopieën gemaakt van essentiële gegevens en programmatuur.*
- ☐ De instelling beschikt over een duidelijke beschrijving van de beveiligingskenmerken van alle gebruikte netwerkdiensten.
- ☐ *Er zijn procedures voor het beheer van verwijderbare media zoals banden, schijven, diskettes en (medische) dossiers. Deze worden op een veilige en beveiligde manier afgevoerd wanneer zij niet langer nodig zijn.*
- ☐ *Procedures zijn opgesteld voor de behandeling en opslag van media om de erop opgeslagen gegevens te beschermen tegen ongeoorloofde openbaarmaking of misbruik .*
- ☐ *Systeemdocumentatie is beveiligd tegen ongeautoriseerde toegang, beschadiging en verlies.*

Uitwisseling

- ☐ *In het beleid is opgenomen welke gegevens in aanmerking komen voor uitwisseling, zowel intern als extern, inclusief de daarbij geldende voorwaarden.*
- ☐ *In overeenkomsten met andere zorginstellingen en met andere partijen zijn beveiligingsmaatregelen met betrekking tot het uitwisselen van gegevens opgenomen.*
- ☐ *Maatregelen zijn genomen ter beveiliging van media tijdens transport en geautomatiseerde gegevensuitwisseling tegen beschadiging, verlies, ongeautoriseerde toegang, misbruik en manipulatie.*
- ☐ *Er is een duidelijk beleid geformuleerd ten aanzien van het gebruik van elektronische communicatie.*
- ☐ *Gegevens die in online transacties zijn betrokken zijn beschermd tegen onvolledige overdracht, verkeerd terecht komen, ongeautoriseerde wijziging, ongeautoriseerde openbaarmaking en multiplicatie.*
- ☐ *Richtlijnen en procedures zijn opgesteld en geïmplementeerd voor de beheersing van de risico's die elektronische kantoorsystemen met zich meebrengen.*
- ☐ Er is aandacht besteed aan de bescherming van de integriteit van programmatuur, gegevens en andere informatie die beschikbaar wordt gesteld via een publiek toegankelijk systeem.
- ☐ *Gegarandeerd is dat gegevens alleen via elektronische publicatiesystemen worden verkregen in overeenstemming met de wetgeving op het gebied van privacybescherming.*
- ☐ Er wordt een goedkeuringsprocedure gevolgd voordat informatie op publiek toegankelijke systemen wordt gezet.

Toegangsbeveiliging:

- ☐ *Duidelijke regels en rechten zijn opgesteld met betrekking tot toegangsbeveiliging voor elke gebruiker of groep van gebruikers.*
- ☐ *De toegang tot informatiediensten verloopt via een veilige inlogprocedure.*
- ☐ *Procedures zijn opgesteld voor het registreren en afmelden van gebruikers.*
- ☐ *Alle gebruikers hebben een unieke gebruikersidentificatie voor persoonlijk gebruik.* GBZ vereist in dit geval het gebruik van UZI-passen.
- ☐ *Procedures zijn vastgesteld voor het toewijzen van gebruikersidentificaties.*
- ☐ *De instelling beschikt over een wachtwoordsysteem om de identiteit van een gebruiker te verifiëren*
- ☐ *Naast wachtwoorden worden andere technologieën voor gebruikersidentificatie en authenticatie overwogen, zoals biometrie en het gebruik van identificatietekens (hardware tokens).*
- ☐ *Er zijn procedures voor het instellen, wijzigen en intrekken van wachtwoorden.*
- ☐ Er zijn procedures voor het aanvragen, intrekken, vervangen, als verloren opgeven en blokkeren van UZI-passen.
- ☐ De instelling beschikt over systemen en procedures voor het uitgeven van middelen voor sterke authenticatie.
- ☐ *Beeldschermapparatuur waarop gevoelige gegevens worden verwerkt is zodanig opgesteld dat er zo min mogelijk kans op toevallige waarneming is.*
- ☐ *Gebruikers worden verplicht om goede beveiligingsgewoontes in acht te nemen bij het kiezen en gebruiken van wachtwoorden.*
- ☐ Er wordt een automatisch identificatiesysteem voor werkstations gebruikt om de verbindingen met specifieke locaties te verifiëren.
- ☐ Er worden automatische verbindingen met computersystemen op afstand geauthenticeerd.
- ☐ *Gebruikers zijn verplicht te zorgen dat onbeheerde apparatuur voldoende is beveiligd.*

- ☐ *Er is voor inactieve werkstations op locaties met verhoogd risico een time-out voorziening ingesteld.*
- ☐ *De toegang tot gegevens en functies wordt verleend overeenkomstig het toegangsbeleid van de instelling.*
- ☐ Aan bepaalde gebruikers kan voor gebruik in onvoorziene noodsituaties de bevoegdheid worden toegekend de normale afscherming te doorbreken.
- ☐ *De instelling heeft procedures en regels vastgesteld voor de toekenning en intrekking van bevoegdheden.*
- ☐ *Toepassingen, systemen en netwerkvoorzieningen worden zodanig ingericht dat toegang alleen mogelijk is in overeenstemming met geldige bevoegdheden.*
- ☐ *De toewijzing en het gebruik van bijzondere bevoegdheden voor noodprocedures, systeembeheer, onderhoud en dergelijke worden beperkt.*
- ☐ Er is een procedure opgesteld voor de verificatie van de toegangsrechten van gebruikers.
- ☐ Gebruikersautorisaties worden periodiek gecontroleerd.

Netwerk en netwerkdiensten

- ☐ *Er is een beleid geformuleerd ten aanzien van het gebruik van netwerken en netwerkdiensten.*
- ☐ Het netwerk van de instelling zijn opgesplitst in afzonderlijke logische domeinen.
- ☐ De gevoeligheid van systemen is bepaald om vast te stellen of zij een vast toegewezen (geïsoleerde) computeromgeving vereisen.
- ☐ *De route tussen werkstation en netwerkdiensten worden beperkt voor kritische informatievoorzieningen.*
- ☐ Poorten die dienen voor systeemdiagnose ten behoeve van onderhoud worden op afstand door een beveiligingsmechanisme en een beveiligingsprocedure beveiligd.
- ☐ *Er is een beleid opgesteld voor de omgang met mobiele computers die de risico's behandelt van het gebruik van mobiele computervoorzieningen.*
- ☐ *Er is beleid geformuleerd voor telewerken en de risico's daarvan.*
- ☐ *Een analyse van de beveiligingseisen wordt uitgevoerd tijdens het specificeren van het pakket van eisen voor elk te ontwikkelen informatiesysteem.*
- ☐ *Gegevens die worden ingevoerd in toepassingssystemen worden gevalideerd op juistheid, volledigheid en mate van actualiteit.*
- ☐ Gegevens die worden verwerkt door toepassingssystemen worden gevalideerd.
- ☐ *Controles worden uitgevoerd op de uitvoergegevens om te waarborgen dat de verwerking van opgeslagen gegevens op een correcte manier plaatsvindt en passend is gezien de omstandigheden.*
- ☐ Er is een risicoanalyse uitgevoerd om te bepalen of authenticatie voor de verzending van gevoelige gegevens vereist is.
- ☐ Binnen de instelling wordt gebruik gemaakt van cryptografische technieken voor de beveiliging van informatie.
- ☐ De implementatie van programmatuur en aanpassingen daarop worden op operationele systemen beheerst.
- ☐ *Leveranciers van programmatuur krijgen alleen fysieke of logische toegang wanneer dit nodig is en dan alleen na toestemming van de leiding.*
- ☐ *Strenge beveiligingsmaatregelen worden in acht genomen in het geval productiegegevens worden gebruikt bij systeem- en acceptatietesten.*
- ☐ *Het gebruik van originele databases met persoonsgegevens voor systeem- en acceptatietesten worden tot het noodzakelijke minimum beperkt.*

- ☐ *De toegang tot bronbestanden voor programmatuur wordt beperkt en beheerst.*
- ☐ Procedures zijn opgesteld voor het beheer van wijzigingen in informatiesystemen.
- ☐ De gevolgen voor de beveiliging van alle wijzigingen in het besturingssysteem worden nagegaan.
- ☐ Wijzigingen in programmatuurpakketten worden zoveel mogelijk vermeden.
- ☐ *Er zijn maatregelen getroffen om te voorkomen dat gegevens bereikt kunnen worden via verborgen communicatiekanalen*
- ☐ *In geval van uitbesteding van de ontwikkeling van programmatuur worden schriftelijke afspraken gemaakt om de kwaliteit van de programmatuur te waarborgen.*

Incidenten

- ☐ Er is een proces van continuïteitsbeheer geïmplementeerd om de verstoring als gevolg van calamiteiten en beveiligingsincidenten tot een aanvaardbaar minimum te beperken.
- ☐ De instelling beschikt over een continuïteitsstrategie.
- ☐ *Er zijn plannen ontwikkeld om de bedrijfsactiviteiten na een onderbreking of verstoring in stand te houden of tijdig te herstellen.*
- ☐ Continuïteitsplannen worden regelmatig onderhouden, getest en geëvalueerd.
- ☐ De procedures zijn opgenomen in het wijzigingsbeheer die ervoor zorgen dat de voor de continuïteit van de bedrijfsvoering belangrijke zaken zonodig worden aangepast.
- ☐ *Alle van toepassing zijnde wettelijke, reglementaire en contractuele eisen zijn expliciet gespecificeerd en gedocumenteerd.*
- ☐ *Alle specifieke maatregelen en individuele verantwoordelijkheden om aan de wettelijke en contractuele verplichtingen te voldoen zijn gespecificeerd en gedocumenteerd.*
- ☐ Passende maatregelen zijn genomen om te waarborgen dat wordt voldaan aan wettelijke beperkingen met betrekking tot het gebruik van materiaal waarop intellectuele eigendomsrechten rusten.
- ☐ *Maatregelen zijn geïmplementeerd om belangrijke documenten en informatie tegen verlies, vernietiging en vervalsing te beveiligen.*
- ☐ *Toepassingen waarin gegevens over personen worden verwerkt voldoen aan de Wet Bescherming Persoonsgegevens.*
- ☐ *Maatregelen zijn genomen om ervoor te zorgen dat de informatievoorziening van de instelling alleen voor geautoriseerde doeleinden worden gebruikt.*
- ☐ Bij de toepassing van cryptografie wordt rekening gehouden met maatregelen die gelden voor de invoer en de uitvoer van cryptografische technologie.
- ☐ Alle verantwoordelijkheidsgebieden worden regelmatig onderworpen aan een beoordeling van de naleving van het beveiligingsbeleid en de beveiligingsnormen.
- ☐ Informatiesystemen worden regelmatig geaudit op de naleving van beveiligingsnormen.
- ☐ Er worden audits van operationele systemen gepland en goedgekeurd.
- ☐ De toegang tot hulpmiddelen voor systeemaudits wordt beheerd.
- ☐ *Er wordt een auditlogboek van bijzondere gebeurtenissen bewaard.*
- ☐ Er zijn procedures opgesteld voor het bewaken en vastleggen van het systeemgebruik.
- ☐ De systeembeheerders houden een logboek bij van hun werkzaamheden.
- ☐ *Er is een procedure voor het melden en afhandelen van storingen.*
- ☐ Door gebruikers gemelde storingen worden in computer- of communicatiesystemen geregistreerd.

- ☐ Systeemklokken worden gesynchroniseerd teneinde gegevens nauwkeurig te kunnen vastleggen.
- ☐ Er zijn regels aanwezig voor het verzamelen van bewijs dat gebruikt kan worden als ondersteuning bij een actie tegen een bepaalde persoon of organisatie conform wettelijke bepalingen.
- ☐ *Er is een procedure vastgesteld voor het melden van incidenten.*
- ☐ *Medewerkers zijn verplicht om onvolkomenheden in programmatuur zo snel mogelijk te melden bij de verantwoordelijke contactpersoon.*
- ☐ *Medewerkers zijn op de hoogte gesteld dat zij mogelijke aanwezigheid van een zwakke plek in de beveiliging moeten rapporteren.*
- ☐ *Er is een procedure vastgesteld voor de afhandeling van incidenten.*
- ☐ Er is een mechanisme aanwezig die de instelling in staat stelt de aard, de omvang en de kosten van incidenten en storingen te kwantificeren en bewaken.