provincie Drenthe

Beleidskader informatiebeveiliging 2017-2020

Veiliger, integer en vertrouwd

Hoe is onze informatie beveiligd?

Team I&A
Okt 2017

Colofon

Datum
Okt. 2017

Auteurs
[redacted]

Adresgegevens
Provincie Drenthe
Westerbrink 1
Postbus 122
9400 AC Assen
Telefoon: (0592) 36 55 55
www.provincie.drenthe.nl

Documentgegevens

Titel	: Beleidskader informatiebeveiliging Provincie Drenthe
Ondertitel	: Veiliger, integere en vertrouwd
Document	: Beleidskader informatiebeveiliging 2017-2020
Status	: Definitief
Versie	: 2.

Inhoud

Versiebeheer

Versie	Omschrijving	Datum	Auteur
1.2	2017-2020 beleidskader informatiebeveiliging provincie Drenthe	3 mei 2017	W. Piek D.B. v.d. Meer
2.0	Aanpassingen n.a.v. bespekingen in Integriteitsplatform provincie Drenthe. Aanpassing t.g.v. besluit IPO/CIBO d.d. 10 oktober 2017 om de ISO27001 toe te passen voor alle provincies.	20 oktober 2017	D.B. v.d. Meer

Referenties

Nr.	Omschrijving	Datum	Auteur

0 Voorwoord

Voor u ligt het beleidskader informatiebeveiliging van de provincie Drenthe. Met dit beleidskader geven wij richting aan de manier waarop de provincie Drenthe omgaat met informatiebeveiliging.

Het gebruik van informatie vormt een belangrijke factor binnen onze bedrijfsprocessen. De overheid behoort veilig, integer en vertrouwd met informatie om te gaan. Hier hechten wij grote waarde aan. Vandaar dat wij tijd en energie besteden aan de beveiliging van onze informatie. Daarmee voldoen wij minimaal aan de Basisnorm Informatie zoals het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) heeft vastgesteld.

Dit kader geldt als een overkoepelende visie voor al onze onderliggende documenten en maatregelen op het terrein van informatiebeveiliging. In dit beleidskader leggen wij vast wat wij verstaan onder informatiebeveiliging, hoe informatiebeveiliging binnen onze provinciale organisatie is vormgeven, welke procesmatige aanpak van informatiebeveiliging wij hanteren, wie welke rollen en taken heeft en wat de hoofdlijnen van ons informatiebeveiligingsbeleid zijn. Hiermee laten wij zien dat wij als provincie informatiebeveiliging serieus nemen én gezamenlijk actief oppakken.

De directie

1 Het informatieplan – in één oogopslag

1.1 Inleiding

De directie, concernmanagers en teamleiders van de provincie Drenthe onderkennen de waarde van informatie voor de bedrijfsvoering. De grote afhankelijkheid en kwetsbaarheid van de informatievoorziening heeft tot het opstellen van het informatiebeveiligingsbeleid geleid. Het informatiebeveiligingsbeleid is in dit document vastgelegd. Daarmee voldoen wij aan de Basisnorm Informatie zoals het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) heeft vastgesteld, als onderdeel van de Basisnormen Integriteit. Deze basisnorm hebben wij als minimale norm verwerkt in ons informatiebeveiligingsbeleid.

Het beleid heeft betrekking op de beveiliging van informatie(verwerking) en geeft een kader voor maatregelen op het gebied van informatiebeveiliging. Dit kader wordt gevormd door de vastlegging van de uitgangspunten van beleid, de inrichting van de beveiligingsorganisatie en de beschrijving van de processtappen die cyclisch in de tijd worden doorlopen.

1.2 Opbouw document

Hoofdstuk 1 beschrijft definities, bereik en context van informatiebeveiliging. In hoofdstuk 2 zijn de doelstelling, beleidsuitgangspunten en verantwoording beschreven. Ten behoeve van de leesbaarheid zijn specifieke onderwerpen als wettelijke kaders, het proces en de hoofdlijnen van beleid opgenomen in bijlagen.

Het wettelijk kader en de daaruit afgeleide uitgangspunten zijn opgenomen in Bijlage A. Het informatiebeveiligingsproces is opgenomen in Bijlage B. Hierbij wordt aangegeven welke stappen binnen dit proces worden onderscheiden. Tevens wordt de organisatie van informatiebeveiliging beschreven. De hoofdlijnen van het informatiebeveiligingsbeleid zijn opgenomen in Bijlage C; het beschrijft de provinciale uitgangspunten voor informatiebeveiliging en de hoofdlijnen van het minimumbeveiligingsniveau gebaseerd op de NEN-ISO 27001/27002.

1.2 Definities

Informatie is voor onze organisatie een “bedrijfsmiddel” en ook vaak een “product”. Informatie heeft waarde voor de organisatie en dient voortdurend op een passende manier beveiligd te zijn. Informatie komt in veel vormen voor (geschreven op papier, elektronisch opgeslagen, per post of via elektronische media verzonden of in gesproken vorm). Welke vorm de informatie ook heeft of op welke manier ze ook wordt gedeeld of verzonden, ze dient altijd passend beveiligd te zijn.

Informatiebeveiliging bestaat uit het stelsel van maatregelen die beogen te voorkomen dat onbevoegden vertrouwelijke gegevens kunnen bezitten, raadplegen of beschadigen.
Informatiebeveiliging wordt gekarakteriseerd als het waarborgen van:

- *Veilige beschikbaarheid (Het juiste moment)*: geautoriseerde gebruikers hebben op de juiste momenten tijdig toegang tot informatie en aanverwante bedrijfsmiddelen;
- *Integriteit (de juiste informatie)*: correctheid en volledigheid van informatie en de verwerking daarvan;
- *Vertrouwelijkheid (de juiste persoon)*: informatie is alleen toegankelijk voor degenen, die hiertoe geautoriseerd zijn en daarmee op de juiste wijze omgaan.

1.3 Bereik

Dit beleidskader is een overkoepelende visie voor al onze onderliggende documenten en maatregelen op het terrein van informatiebeveiliging. Hierbij gaat het om ons integraal informatiebeveiligingsbeleid voor zowel de ambtelijke als de bestuurlijke organisatie van de provincie Drenthe. Ons informatiebeveiligingsbeleid werken wij nader uit in beleidsdocumenten zoals bijvoorbeeld een wachtwoordbeleid, dataclassificatiebeleid, beleid rond meldplichten etc. Met daarin beheersmaatregelen voor het verplichte minimum informatiebeveiligingsniveau. Zowel organisatiebreed als indien nodig per team. Het informatiebeveiligingsbeleid kan niet los worden gezien van organisatiebeleid en doelstellingen van de provincie Drenthe. Daarnaast heeft het beleid relatie met of betrekking op beleidsplannen van alle teams van de provincie Drenthe.

Het beleid is een duurzaam kader waarbinnen maatregelen worden gedefinieerd. Wij streven er naar de maatregelen voortdurend te beoordelen op hun toereikendheid en toegevoegde waarde. Daarom zijn de maatregelen zelf geen onderdeel van dit beleidskader.

Als basis voor het informatiebeveiligingsbeleid hanteren wij de Code voor Informatiebeveiliging (NEN/ISO 27001 en 27002), die is ontwikkeld door een groot aantal vooraanstaande organisaties en die in 2005 in Nederland (opnieuw) is uitgebracht door het Nederlands Normalisatie-instituut (NNI) onder auspiciën van het Ministerie van Economische Zaken (EZ). Deze standaard is inmiddels uitgegroeid tot de breedst geaccepteerde *de facto* standaard voor de beheersing van informatiebeveiliging in organisaties. De Code voor Informatiebeveiliging voldoet aan de Basisnorm Informatie van het ministerie van Binnenlandse Zaken & Koninkrijksrelaties. Gedurende 2017 is door het IPO/CIBO uitgesproken de Code te hanteren als de leidende norm voor alle provincies en het vervangt derhalve de tot nu toe gehanteerde normenkader, genaamd IBI. Dit besluit wordt onderschreven door het IPO/SIO. Door de provincies zal een gezamenlijk plan worden opgesteld om medio 2018 een nulmeting uit te voeren. Elke provincie zal in 2018 een implementatieplan opstellen voor de implementatie van ISO27001 in haar organisatie met een doorlooptijd van 3 jaren. Het eindstreven is dat alle provincies ISO27001 gecertificeerd zullen zijn en daarmee een bijzonder sterke positie in te nemen qua informatieveiligheid.

De Code voor Informatiebeveiliging definieert de volgende veertien categorieën noodzakelijke beveiligingsmaatregelen:

1. Informatiebeveiligingsbeleid
2. Organiseren van Informatiebeveiliging
3. Veilig Personeel
4. Beheer van bedrijfsmiddelen
5. Toegangsbeveiliging
6. Cryptografie
7. Fysieke beveiliging en beveiliging van de omgeving
8. Beveiliging bedrijfsvoering
9. Communicatiebeveiliging
10. Acquisitie, ontwikkeling en onderhoud van informatiesystemen
11. Leveranciersrelaties
12. Beheer van informatiebeveiligingsincidenten
13. Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer
14. Naleving

De Code voor Informatiebeveiliging heeft als doel het beveiligingsniveau binnen organisaties op een noodzakelijk minimum peil te brengen en zo het wederzijdse vertrouwen tussen organisaties en/of organisatieonderdelen te bevorderen.

De Code voor Informatiebeveiliging gaat uit van een integrale opzet van informatiebeveiliging. Om dit te realiseren zijn waar nodig alle teams met hun eigen beleidsterreinen betrokken bij het inrichten en handhaven van het beleid. De afstemming tussen de beleidsterreinen is in de organisatie geborgd. In Bijlage B, paragraaf 3 is borging van informatiebeveiliging nader uitgewerkt.

1.4 Context van het provinciale informatiebeveiligingsbeleid

Het provinciale informatiebeveiligingsbeleid dient te worden gezien in de context van geaccepteerde standaarden, zoals de NEN-ISO 27001/27002, het bestuurlijk convenant, het convenant interprovinciale regulering informatieveiligheid en (tot 2017) de interprovinciale baseline.

Het Drentse informatiebeveiligingsbeleid is derhalve geen vrije interpretatie van de omgang met informatie maar is afgeleid van geaccordeerde en geaccepteerde convenanten die zorg dragen voor een periodieke toetsing en rapportage.

Het informatiebeveiligingsbeleid is overkoepelend voor specifieke IB-beleidsgebieden, zoals wachtwoordenbeleid en dataclassificatiebeleid. Deze beleidsstukken vallen ook onder het informatiebeveiligingsbeleid.

2 *Doelstelling, beleidsuitgangspunten en verantwoordelijkheden*

2.1 Doelstelling

De doelstelling van het informatiebeveiligingsbeleid van de provincie Drenthe luidt:
"Het bieden van een kader met beleidsuitgangspunten dat beoogt te voorkomen dat onbevoegden vertrouwelijke gegevens kunnen bezitten, raadplegen of beschadigen.

2.2 Provinciale beleidsuitgangspunten

2.2.1. Code voor informatiebeveiliging NEN-ISO/IEC 27001

De provincie Drenthe hanteert de Code voor Informatiebeveiliging (NEN-ISO/IEC) als basis voor het inrichten en onderhouden van maatregelen voor het waarborgen van de veilige beschikbaarheid, integriteit en vertrouwelijkheid van haar bedrijfsgegevens. Daarnaast worden indien van toepassing andere normen (zoals NORA-informatiebeveiliging), complementair gebruikt.
Toelichting: de Code voor Informatiebeveiliging is een algemeen geaccepteerde basis voor informatiebeveiliging en is in 2017 onderschreven door het IPO/CIBO.

2.2.2. Beleid is van toepassing op interne en externe medewerkers

Het beleid is van toepassing op alle bij de provincie Drenthe werkzame (interne en externe) medewerkers en bestuurders. Hieronder wordt verstaan zowel de ambtelijke organisatie, de griffie als het bestuur.
Toelichting: het gewenste resultaat van implementatie en naleving van het informatiebeveiligingsbeleid kan alleen worden bereikt indien het bindend is voor alle medewerkers en bestuurders die werkzaam zijn bij of voor de provincie Drenthe.

2.2.3. Afwijking van het beleid het beleid vereist schriftelijk akkoord van de CISO

Afwijking van het beleid vereist toestemming van de CISO. De CISO is verantwoordelijk voor een consistente uitvoering van het beleid en legt hierover verantwoording af aan de directie van de provincie Drenthe.

2.2.4. Informatiebeveiliging is een lijnverantwoordelijkheid.

Toelichting: informatiebeveiliging is onderdeel van integraal management. De manager en de teamleider zijn verantwoordelijk voor de naleving van het informatiebeveiligingsbeleid en de getroffen maatregelen.

2.2.5. Informatiebeveiliging is een persoonlijke verantwoordelijkheid

Toelichting: de persoonlijke verantwoordelijkheid van iedere medewerker en bestuurder van de provincie Drenthe ten aanzien van informatiebeveiliging zijn vastgelegd in gedragscodes, regelementen, richtlijnen dan wel bruikleenovereenkomsten m.b.t. ict apparatuur.

2.2.6. Iedere beveiligingsmaatregel moet controleerbaar zijn.

Toelichting: maatregelen waarvan de naleving niet goed is te handhaven, kunnen aanleiding geven tot ontwijkend gedrag, wat impliceert dat de maatregelen niet effectief zijn. Bij iedere maatregel wordt vooraf nagegaan op welke wijze de naleving en het functioneren kunnen worden gecontroleerd.

2.2.7. Beveiligingsmaatregelen zoveel mogelijk technisch handhaven

Toelichting: technische middelen voor handhaving van beveiligingsmaatregelen voorkomen afhankelijkheid van naleving van organisatorische en procedurele maatregelen. Nadrukkelijk wordt hieraan toegevoegd dat technische middelen niet voor alle maatregelen kunnen worden toegepast.

2.2.8. Het beveiligingsbewustzijn en morele oordeelsvorming van alle medewerkers, griffie en bestuurders wordt actief en stuctureel gestimuleerd

Toelichting: het resultaat van het informatiebeveiligingsbeleid hangt voor een groot deel af van het beveiligingsbewustzijn van alle betrokkenen. Het is daarom van groot belang dit bewustzijn omtrent informatoeveiligheid en morele oordeelsvorming actief en structureel te bevorderen. Daartoe wordt jaarlijks een iBewustzijn plan opgesteld

2.2.9. Informatiebeveiligings aspecten worden in overeenkomsten tussen de provincie Drenthe en externe partijen vastgelegd.

De provincie (op voorspraak van teamleider I&A/CISO) zal per overeenkomst met derden bepalen of al dan geen informatiebeveiligingsparagraaf wordt opgenomen.

Toelichting: overeenkomsten met externe organisaties en instellingen over de behandeling van informatie gegenereerd in het kader van activiteiten van of voor de provincie Drenthe worden in samenwerkingscontracten en/of projectplannen vastgelegd.

2.2.10. Periodiek controle / audit

De werking en de naleving van de uit het beveiligingsbeleid en de beveiligingsplannen voortvloeiende maatregelen worden periodiek gecontroleerd door middel van een screening (tenminste één keer per jaar) door een interne deskundige(n) of een audit (tenminste één keer per drie jaar) door extern onafhankelijk deskundige(n). Zie ook bijlage C voor een schets van het normenkader.

Toelichting: een screening en een onafhankelijke audit, waarbij bevindingen en aanbevelingen rechtsreeks aan het bestuur en de directie worden gerapporteerd, geeft de beste garantie dat de provincie Drenthe waakzaam blijft op het gebied van de informatiebeveiliging en stimuleert een proces van continue aanpassing en verbetering van maatregelen. De werkwijze sluit aan bij de provinciale implementatie van ISO27001.

2.2.11. Overtreding informatiebeveiligingsbeleid kan leiden tot sancties.

Toelichting: in geval van overtreding van regels voor informatiebeveiliging worden betrokkenen hierop persoonlijk aangesproken en gehandeld overeenkomstig het CAP (de Collectieve Arbeids voorwaardenregeling Provincies), ambtenarenwet. De mogelijkheid tot het opleggen van sancties geeft aan dat naleving van het beveiligingsbeleid niet vrijblijvend is, maar bindend is voor alle afdelingen en eenheden.

2.2.12. Jaarlijkse rapportage

Over de voortgang van de activiteiten op het gebied van informatiebeveiliging, die opgenomen zijn in het beleid, wordt door de betrokken teams jaarlijks gerapporteerd aan de

directie van de provincie Drenthe. In deze rapportage wordt tevens een bijlage toegevoegd van alle bekende beveiligingsincidenten die plaats hebben gevonden in de provincie Drenthe alsmede de evaluatie ervan.

Toelichting: jaarlijkse rapportage aan de directie over de voortgang van activiteiten op het gebied van informatiebeveiliging bevordert de waakzaamheid en stimuleert een proces van continue aanpassing en verbetering van maatregelen.

2.3 Verantwoordelijkheid

De algehele, organisatie brede verantwoordelijkheid voor informatiebeveiliging is belegd bij de directie en gemandateerd bij een CMT lid. In Bijlage 3, paragraaf 3 is borging van informatiebeveiliging in de organisatie nader gespecificeerd. Een portefeuillehouder in GS is bestuurlijk gezien eindverantwoordelijk.

BIJLAGE A: Wettelijk kader en uitgangspunten

A.1 Wettelijk kader

Voor de Nederlandse overheid bestaat ten aanzien van de beveiliging een groot aantal wettelijke regelingen en voorschriften. Eén van de belangrijkste voorschriften voor Provincies voor de informatiebeveiliging is het convenant “Interprovinciale regulering informatieveiligheid”. Dit zijn interprovinciale bindende afspraken m.b.t. het verankeren van het basis normenkader, het (door)ontwikkelen van monitoring, zelfevaluatie en onafhankelijke toetsing en het versterken van bewustwording en deskundigheid m.b.t. informatiebeveiliging.

Verder bestaat het wettelijk kader uit de volgende wet- en regelgeving: Grondwet, Ambtenarenwet, Wet Bescherming Persoonsgegevens (Wbp), Algemene Verorderning Gegevensbescherming, Wet Openbaarheid van Bestuur (WOB), Wet Computercriminaliteit, Archiefwet en Archiefregeling etc..

Per 1-1-2016 is de Wet Meldplicht Datalekken in werking getreden. De Europese Algemene Verordening Gegevensbescherming (AVG) is in mei 2016 door het Europese parlement aangenomen. De AVG treedt op 25 mei 2018 in werking en vervangt de Nederlandse Wbp en Meldplicht Datalekken. Vanaf dat moment geldt in Europese één privacy-verordening. De grootste veranderingen zijn dat de belangen van de burger stringenter worden behartigd m.b.t. privacy. Organisaties moeten inzicht verschaffen in de opgeslagen gegevens van en over burgers. Tevens worden overheden verplicht een Functionaris Gegevensbescherming aan te stellen. Organisaties dienen aantoonbaar passende beveiligingsmaatregelen te treffen; bij laakbaarheid en nalatigheid heeft de landelijke privacy-waakhond (Autoriteit Persoonsgegevens) een boetebevoegdheid.

A.2 Uitgangspunten voor informatiebeveiligingsbeleid

Onderstaande uitgangspunten kaderen het beleid rond informatiebeveiliging af:

- **Interprovinciale Baseline Informatieveiligheid (IBI) vervangen door ISO27002**

De interprovinciale baseline is gebaseerd op de code van informatiebeveiliging (landelijke standaard NEN-ISO 27001 en 27002). Hierin staan de minimaal benodigde beveiligingseisen en maatregelen. Het toetsen van de werkelijke situatie aan de normen/maatregelen van de IBI leidt tot inzicht in het veiligheidsniveau op basis waarvan de provincie een actieplan inclusief advies maakt.
Voor kritische bedrijfsprocessen of informatiesystemen wordt een (business/privacy) impact analyse uitgevoerd. Hierbij wordt vastgesteld wat de impact is indien de beveiliging van informatie niet gewaarborgd of zelfs geschaad is. Vervolgens worden de risico’s in kaart gebracht en worden passende maatregelen getroffen ter vermindering of opheffing van risico’s. Overigens betreft dit ook de beveiliging van de fysieke informatie. Bij de selectie van maatregelen is de waarde van informatie voor de Provincie een belangrijke factor.
Echter in 2017 is besloten door het IPO/CIBO om zich volledig te focussen op de ISO27001. De IBI zal derhalve als maatregelenset vervangen worden door de ISO27002.

- **NCSC-richtlijnen en Forum Standaardisatie gelden als toetsingskader voor cloud oplossingen en webapplicaties.**

De ICT-Beveiligingsrichtlijnen van het Nationaal Cyber Security Center (NCSC) zijn leidraad voor het toetsen van provinciale cloud-oplossingen en webapplicaties op basis van een risicoanalyse. De jaarlijkse Digid-audit is mede gebaseerd op de normen van het NCSC.
Het normenkaders die door het ‘Bureau Forum Standaardisatie’ worden uitgegeven gelden als basis voor het webdomein en email-domein van de provincie Drenthe en aanpalende websites/emails.

- **Informatie is vrij beschikbaar, tenzij (cf. uitsluitingsgronden Wet Openbaarheid van Bestuur en EU-richtlijn Aarhus):**
  - Er wettelijke belemmeringen zijn in het kader van privacy, vertrouwelijkheid, veiligheid en auteursrechten;
  - Er persoonlijke beleidsopvattingen van bestuurders, ambtenaren en andere betrokkenen zijn vermeld, die zijn te herleiden naar de persoon;
  - Er concurrentieverhoudingen kunnen worden geschaad;
  - Het economisch of financieel belang van de organisatie wordt geschaad.

- **Er zijn aanvullende beveiligingsmaatregelen nodig voor niet openbare informatie**

De rubricering hiervan sluit aan op de dataclassificatie Informatiebeveiligingsdienst Gemeenten (IBD) die de volgende indeling hanteert:

- INTERN/BEDRIJFSVERTROUWELIJK: informatie waarvan het gebruik of de inzage er van beperkt moet blijven tot de provinciale organisatie;
- VERTROUWELIJK: informatie waarvan de toegang beperkt moet blijven tot een beperkte groep personen:
- GEHEIM: informatie waarvan de toegang beperkt moet blijven tot een zeer beperkte groep personen en waarvan compromittering grote consequenties kan hebben voor de provinciale organisatie en haar werkgebied.

De maatregelen voor informatiebeveiliging zullen worden afgestemd op deze categorisering en defitief worden verwoord in een dataclassificatie beleid dat toepasbaar zal zijn voor de (nieuwe) Microsoft 365-omgeving

- **Er is een beveiligingsprocedure voor inbreuken op de informatiebeveiliging**

Inbreuken op de informatiebeveiliging worden gemeld, vastgelegd en beoordeeld door middel van het datalek proces.

- **Informatiebeveiliging is een gemotiveerde risico-afweging**

Op een aantal onderdelen legt informatiebeveiliging beperkingen op aan de bedrijfsvoering. In deze gevallen gaan maatregelen in het kader van informatiebeveiliging voor op wensen van medewerkers. Indien dit niet acceptabel is wordt een risicoanalyse uitgevoerd. Op basis van de uitkomst van deze analyse en de pro- en contra's neemt het CMT een besluit. De implementatie van ISO27001 is ten principale gebaseerd op risico afweging, zodat met de invoering hiervan risico afweging wordt bevorderd.

- **Informatiebeveiliging raakt alle vormen van informatie**

Informatiebeveiliging moet gericht zijn op het passend beschermen van informatie, in welke vorm dan ook. Dit betreft alle vormen van informatie (analoog of digitaal) en alle informatiedragers (papier, CD/DVD, usb etc.)

- **Informatiebeveiliging is een voorwaarde bij diverse beleidsterreinen**

Bij ontwikkeling van nieuw beleid wordt rekening gehouden met de betrouwbaarheidseisen die vanuit de informatiebeveiliging worden gesteld. Gerelateerde beleidsterreinen zijn bijvoorbeeld de Administratieve Organisatie/Interne Controle, de beveiliging van gebouwen, personeelsbeleid, documentaire informatievoorziening en informatiebeleid. Bij de implementatie van nieuwe technologieën voor extern ICT-beleid (bijv. internet, inzet van sociale media, flexibel werken) wordt voldaan aan de beveiligingsvoorwaarden integriteit, vertrouwelijkheid en beschikbaarheid van informatie.

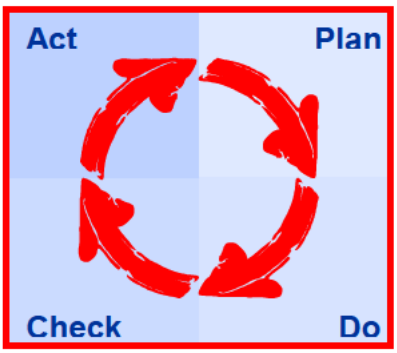
- **Veilige informatie-uitwisseling tussen provincie en ketenpartners is geborgd**

Bij uitwisseling van bestanden of gegevens tussen de provincie en één of meer andere overheidsinstanties en bedrijven/instellingen wordt vastgelegd onder wiens verantwoordelijkheid deze uitwisseling plaats vindt en aan welke kwaliteitseisen de uitwisseling moet voldoen.

BIJLAGE B: Het proces van informatiebeveiliging

B.1 Inleiding

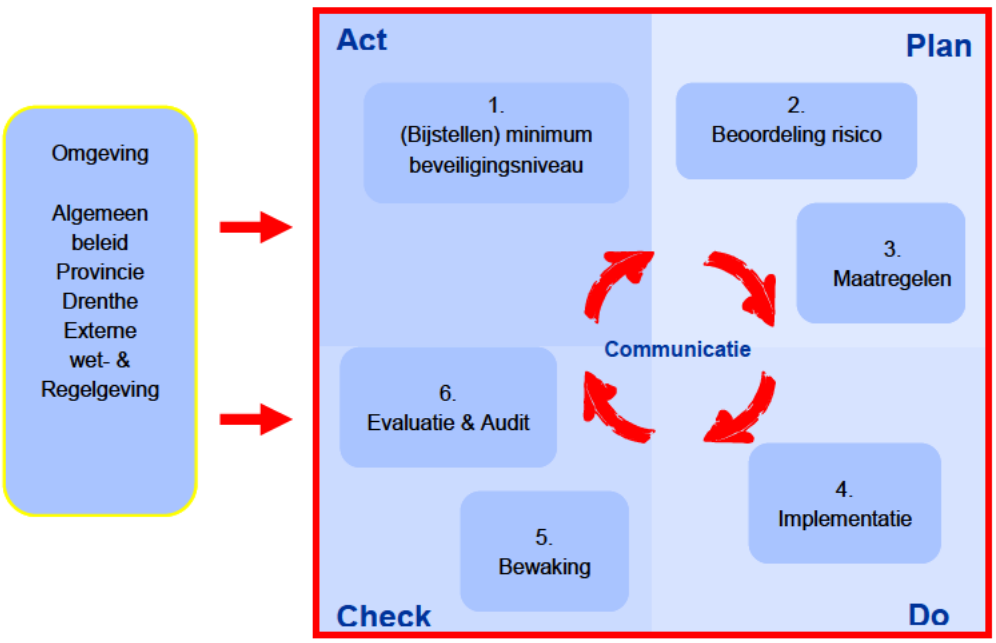
Het proces van informatiebeveiliging is opgehangen aan de kwaliteitscirkel van Deming; Deze kwaliteitscirkel is opgedeeld in een viertal processtappen *Plan-Do-Check-Act*. Deze processtappen vormen een sluitend proces met een begin en een einde gericht op een constante kwaliteitsverbetering. Bij de provincie Drenthe geldt de Deming cirkel als algemeen geaccepteerd proces metamodel.



Kwaliteitscirkel van Deming

B.2 Toelichting informatiebeveiligingsproces

Het proces van informatiebeveiliging bij de provincie Drenthe ziet er dan als volgt uit:



1. (Bijstellen) minimumbeveiligingsniveau
Het informatiebeveiligingsbeleid bestaat uit beleid en een basisnorm informatiebeveiliging (ook wel het minimum beveiligingsniveau). Dit minimum beveiligingsniveau is een door de directie vastgestelde set van beheersmaatregelen, welke geldt als het minimale niveau van informatiebeveiliging waaraan de gehele organisatie of specifieke teams dienen te voldoen. Na evaluatie van de implementatie van het minimale beveiligingsniveau of na een jaarlijkse audit kan blijken dat aanpassing van het informatiebeleid en het daarbij behorende minimum beveiligingsniveau noodzakelijk of gewenst is.

2. Beoordeling risico
Om te bepalen of een team aan het minimum beveiligingsniveau voldoet, worden risicoanalyses uitgevoerd. De processtappen "minimum beveiligingsniveau" en "Evaluatie & Audit" zijn hiervoor belangrijke bronnen.

De beoordeling van beveiligingsrisico's wordt bepaald door drie aspecten:
1. De waarschijnlijkheid van het optreden van een beveiligingsincident;
2. De schade voor de organisatie die ontstaat als gevolg van het optreden van dat beveiligingsincident;
3. De kosten van beveiligingsmaatregelen om het risico van het beveiligingsincident tot een aanvaardbaar niveau te reduceren.

3. Maatregelen
Op basis van de beoordeling moet ieder team bepalen welke maatregelen dienen te worden getroffen of bijgesteld om (blijvend) aan het minimum beveiligingsniveau te voldoen.

4. Implementatie
Na het ontwerpen van de maatregelen worden deze geïmplementeerd. De verantwoording voor het implementeren van de maatregel ligt bij teamleider die primair verantwoordelijk is voor het beleidsterrein waar de maatregel op van toepassing is. De beveiligingsorganisatie ondersteunt de manager/het hoofd bij deze invoering.

5. Bewaking
Informatiebeveiliging is een lijnverantwoordelijkheid. Dit houdt in dat de bewaking van maatregelen bij het CMT en teamleiders ligt. Zij dienen ervoor zorg te dragen dat de in het informatiebeveiligingsbeleid geformuleerde beleidsuitgangspunten en daaraan gekoppelde maatregelen, als integraal onderdeel van hun bedrijfsvoering worden meegenomen.

6. Evaluatie & Audit
Het informatiebeveiligingsbeleid (incl. minimum beveiligingsniveau) en de beveiligingsmaatregelen, worden periodiek geëvalueerd en waar nodig bijgestuurd.

Interne screening vindt regelmatig plaats. Deze wordt gecoördineerd door de Functionaris Gegevensbescherming.

Externe audit vindt minimaal één keer per drie jaar plaats en wordt uitgevoerd door een objectieve deskundige derde partij onder de coördinatie van de Functionaris Gegevensbescherming.

Bevindingen en aanbevelingen vanuit de interne screening en externe audit worden meegenomen in de processtap '(bijstellen) minimumniveau'. Het resultaat van de beoordeling bepaalt voor welke beveiligingsrisico's (boven op het minimum beveiligingsniveau) en met welke prioriteit, maatregelen moeten worden getroffen.

Communicatie
Communicatie maakt geen deel uit van de processtappen maar is wel relevant bij alle processtappen. Het heeft, naast het informeren en instrueren van bestuurders en medewerkers, tot doel de bewustwording ten aanzien van informatiebeveiliging te verhogen.

B.3 Borging informatiebeveiligingsbeleid

Bij de borging van de informatiebeveiliging in de organisatie is onderscheidt gemaakt tussen het beheer van het informatiebeveiligingsbeleid en de uitvoering van dit beleid. Zowel het beheer als de uitvoering zijn belegd bij actoren in de reguliere aansturinglijn. De taken, bevoegdheden en verantwoordelijkheden met betrekking tot het informatiebeveiligingsbeleid zijn voor beheer en uitvoering in een aantal, aan het onderwerp gerelateerde, functies belegd.

Het beheer van het beleid ligt bij de directie, maar is gedelegeerd aan de Functionaris Gegevensbescherming (FG). De FG treedt op als IB-adviseur voor de organisatie. De teamleider I&A is verantwoordelijk voor de IT-voorzieningen en de teamleider Bestuursservice & Gebouwen is verantwoordelijk voor de fysieke beveiliging.

Informatiebeveiliging is een van de basisnormen Integriteit welke door het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) voorgeschreven. De functionaris Integriteit bij de provincie Drenthe (belegd bij de afdeling Management Ondersteuning) is hierdoor gelieerd aan het informatiebeveiligingsbeleid en daarom medeverantwoordelijk voor het beheer van dit beleid.

Het beheer van het beleid richt zich voornamelijk op de processtappen: *Act* (1. (Bijstellen) minimum beveiligingsniveau), *Plan* (2. Mede beoordeling risico en 3. mede bepalen maatregelen) en *Check* (5. Bewaking en 6. evaluatie & Audit) kwadranten van het proces.

De uitvoering van het informatiebeveiligingsbeleid (het handelen naar) is de verantwoordelijkheid van ‘de lijn’. Als verantwoordelijke voor een team, is de teamleider verantwoordelijk voor het handelen van de medewerker naar dit beleid.

De uitvoering van het beleid is geconcentreerd in de processtappen: *Plan* (2. Beoordeling risico en 3. bepalen maatregelen) en *Do* (4. Implementatie).

B.4 Taken & rollen ten behoeve van borging informatiebeveiliging
De taken en rollen worden beschreven uitgaande van de beleidsmatige cyclus van informatiebeveiliging, daarin wordt onderscheid gemaakt naar de volgende taken:

- Beleidsvoorbereiding;
- Beleidsbepaling;
- Uitvaardigen van regelgeving met betrekking tot informatiebeveiliging;
- Coördinatie van informatiebeveiliging;
- Communicatie en voorlichting;
- Uitvoering van beveiligingsactiviteiten;
- Controle;
- Evaluatie;
- Rapportage.

Een confrontatie van verschillende rollen met de beveiligingstaken geeft de volgende matrix:

Rol Taken	GS	Directie	Functionaris Gegevens-bescherming	CISO (I&A)	Functionaris Integriteit (P&O)	Team-leider
Beleidsvoorbereiding		X	X	X	X	
Beleidsbepaling		X				X
Besluitvorming IB (bestuurlijk)	X					
Besluitvorming (ambtelijk/operationeel)		X				
Coördinatie			X			
Communicatie	X	X	X	X	X	X
Controle			X			
Uitvoering						X
Evaluatie		X	X	X	X	
Rapportage			X			X

Uitwerking van de toewijzing van beveiligingstaken:
Gedeputeerde Staten van de provincie Drenthe heeft in het kader van informatiebeveiliging de volgende taken:

- Het bestuurlijk vaststellen van het informatiebeveiligingsbeleid en wijzigingen daarop;
- Bevorderen van het bewustzijn voor informatiebeveiliging bij bestuurders en medewerkers van de provincie Drenthe;

De directie & CMT van de provincie Drenthe heeft in het kader van informatiebeveiliging de volgende taken:

- Het ambtelijk voorberieden van het informatiebeveiligingsbeleid voor de organisatie en wijzigingen daarop;
- Evalueren en beoordelen van rapportages over informatiebeveiliging.
- Bevorderen van het bewustzijn voor informatiebeveiliging bij bestuurders en medewerkers van de provincie Drenthe;

De Functionaris Gegevensbescherming heeft een wettelijke verantwoordelijkheid: "*De FG houdt toezicht op en geeft advies over de verwerking van persoonsgegevens en heeft een geheimhoudingsplicht*". De FG heeft de volgende taken die voortvloeien uit de wettelijke verantwoordelijkheid:

- Inventariseren van gegevensverwerkingen en het bijhouden van een openbaar register van (niet van melding vrijgestelde) gegevensverwerkingen;
- Afhandelen van klachten over het gebruik van persoonsgegevens;
- Een deskundig aanspreekpunt voor betrokkenen m.b.t. verwerking van persoonsgegevens;
- Geven van voorlichting en informatie aan bestuur, management en medewerkers, alsmede het adviseren, over Informatiebeveiliging en het verwerken van persoonsgegevens.
- Ontwerpen en initiëren van toezicht-instrumentarium op basis van wet en (interne)regelgeving m.b.t. verwerking van persoonsgegevens.
- Bevorderen van het bewustzijn voor informatiebeveiliging bij bestuurders en medewerkers van de provincie Drenthe;
- Uitvoeren van interne screenings op basis van een hiervoor opgesteld controleplan;
- Coördineren van externe audits, die door de externe auditor worden uitgevoerd;

- Rapporteren aan de directie, onder andere over naleving van het informatiebeveiligingsbeleid, de voortgang van de implementatie van informatiebeveiligingsmaatregelen en over de uitkomsten van interne screenings en externe audits;
- Onderhouden van interne en externe contacten op het terrein van informatiebeveiliging, alsmede het optreden als intermediair tussen Provincie en Autoriteit Persoonsgegevens.

De teamleider I&A en de Functionaris Gegevensbescherming hebben in het kader van informatiebeveiliging de volgende taken:
- Advies uitbrengen aan de directie op het gebied van vast te stellen en uit te vaardigen (wijzigingen) regelgeving met betrekking tot informatiebeveiliging;
- Bevorderen van het bewustzijn voor informatiebeveiliging bij bestuurders en medewerkers van de provincie Drenthe;
- Adviseren van het GS, directie en managers met betrekking tot informatiebeveiliging.

De teamleiders hebben de volgende taken:
- Bewaken van beveiligingsrisico's met betrekking tot eigen beleidsterreinen;
- Implementeren van de technische informatiebeveiligingsmaatregelen;
- Rapporteren aan directie en Functionaris Gegevensbescherming, onder andere op het gebied van implementatie en uitvoering van informatiebeveiligingsmaatregelen;
- Toezien op de naleving van regelgeving door de medewerkers van het team en toezien op naleving van getroffen beveiligingsmaatregelen.

De medewerkers, teamleiders, CMT en bestuur hebben de volgende taken:
- Actief melden van veiligheidsincidenten.

De Functionaris Gegevensbescherming, de teamleider I&A, medewerker met Security Officer-rol en de Coördinator Servicedesk hebben vanuit de aard van hun werkzaamheden een regelmatig contact. De FG, teamleider I&A en de medewerker met Security Officer-rol overleggen periodiek over de te implementeren maatregelen en evalueren deze op regelmatige basis.
De FG en de Coördinator Servicedesk maken gezamenlijk deel uit van het Rapid Response Team in het kader van datalekken.

BIJLAGE C: Hoofdlijnen informatiebeveiligingsbeleid

C.1 Inleiding

In deze bijlage worden de hoofdlijnen van het informatiebeveiligingsbeleid beschreven. Deze beschrijving bestaat uit een aantal kernachtige uitspraken die het informatiebeveiligingsbeleid weergeven. Bij de beschrijving is de indeling van de NEN/ISO Code voor Informatiebeveiliging als leidraad gehanteerd.

C.2 Informatiebeveiligingsbeleid

De provincie Drenthe heeft de doelstellingen, uitgangspunten en randvoorwaarden met betrekking tot de beveiliging van informatie vastgelegd in het onderhavige document, getiteld ‘Beleidskader informatiebeveiliging provincie Drenthe’.
De provincie Drenthe heeft het convenant ‘Interprovinciale regulering informatieveiligheid’, d.d. sept. 2014, onderschreven. Uitvloeisel van dit convenant was de Interprovinciale Baseline Informatieveiligheid; het vigerende toetsingskader van het beveiligingsniveau.

In het convenatn is afgesproken dat de directie verantwoordelijk is voor het beheer van het Beleidskader informatiebeveiliging. Dit document zal derhalve ambtelijk vastgesteld dienen te zijn door de directie en bestuurlijk door Gedeputeerde Staten.

Het informatiebeveiligingsbeleid wordt bijgewerkt indien dit gewenst is, echter met een minimum van éénmaal per drie jaar.

C.3 Organiseren van Informatiebeveiliging

De taken en verantwoordelijkheden met betrekking tot informatiebeveiliging zijn vastgesteld en formeel toegewezen. De rollen m.b.t. informatiebeveiliging zijn beschreven in bijlage B van het beleidskader informatiebeveiliging. Aangezien de vastlegging van de beveiligingsorganisatie onderdeel uitmaakt van het Beleidskader informatiebeveiliging wordt deze rollen met dezelfde frequentie geëvalueerd en onderhouden.

De verantwoordelijkheid voor het verzorgen en implementeren van beheersmaatregelen is een taak van individuele managers/teamleiders. De provincie Drenthe streeft ernaar voor elk bedrijfsmiddel een eigenaar te benoemen die verantwoordelijk is voor de dagelijkse bescherming ervan.

C.4 Veilig personeel

De provincie Drenthe onderschrijft het belang van de factor bestuur en ‘personeel’ voor het welslagen van informatiebeveiliging. Voorlichting van het bestuur, management en medewerkers is van groot belang voor een succesvolle implementatie en onderhoud van informatiebeveiliging. Hiervoor wordt door de Functionaris Gegevensbescherming in samenwerking met het team Bestuur en Communicatie (BC) een communicatieplan opgesteld en uitgevoerd. Het effect van dit plan wordt periodiek gemeten en op grond hiervan worden de (communicatie) activiteiten bijgesteld.

Het team Personeel en Organisatie) is verantwoordelijk voor het personeelsbeleid. De realisatie van beveiligingseisen ten aanzien van personeel, zoals geheimhouding, vaststelling van kritische functies, et cetera valt onder de verantwoordelijkheid van dit team.

C.5 Beheer van bedrijfsmiddelen

De provincie Drenthe houdt een nauwkeurige administratie bij van bedrijfsmiddelen. Aan de bedrijfsmiddelen is tevens een eigenaar toegewezen. Bedrijfsmiddelen die in gebruik zijn gegeven bij (tijdelijke) medewerkers worden bij beëindiging van hun dienstverband, contract of overeenkomst geretourneerd.

De provincie Drenthe past classificatie van informatie toe; classificatie vindt plaats op wettelijke eisen, waarde, belang en gevoeligheid voor onbevoegde bekendmaking. De afdeling I&A is verantwoordelijk voor het beheer en onderhoud van de classificatie en ondersteunt de provinciale organisatie bij het gebruik hiervan.

C.6 Toegangsbeveiliging

Voor de beveiliging van informatie en informatiesystemen wordt een evenwichtig pakket van technische en organisatorische beveiligingsmaatregelen getroffen op het niveau van het netwerk, het besturingssysteem, de applicatie en de gegevens.

Voor de beveiliging van de uitwisseling van gegevens met derden met behulp van IT-bedrijfsmiddelen worden passende maatregelen getroffen. De provincie Drenthe heeft een gebruikerstoegangsprocedure geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen en in te trekken.

C.7 Cryptografie

Het team I&A treft passende maatregelen ter beperking van de kans op en de gevolgen van het optreden van incidenten met betrekking tot ‘kwaadaardige’ programmatuur. Wanneer netwerken en/of computers van de provincie met externe netwerken worden verbonden, worden adequate beveiligingsmaatregelen ter beperking van de risico’s van deze koppeling getroffen.

C.8 Fysieke beveiliging en beveiliging van de omgeving

Het team Bestuursservice & Gebouwen is verantwoordelijk voor het beleid ten aanzien van fysieke beveiliging. De realisatie van beveiligingseisen ten aanzien van de fysieke beveiliging van bedrijfsmiddelen, zoals het opstellen van een bezoekersregeling, het ontwikkelen en implementeren van een clear desk beleid, het op passende wijze beveiligen van de toegang tot ruimtes, valt onder de verantwoordelijkheid van dit team.

Het team I&A adviseert het CMT over de beveiligingsmaatregelen die minimaal in de computerruimte(n) dienen te worden getroffen. Het team I&A is, na besluitvorming door het CMT, verantwoordelijk voor de realisatie hiervan.

C.9 Beveiliging bedrijfsvoering

Om de continuïteit in de bedrijfsvoering te borgen worden veranderingen in de organisatie, bedrijfsprocessen, informatie verwerkende faciliteiten en systemen die van invloed zijn op de informatiebeveiliging beoordeeld voordat deze veranderingen worden doorgevoerd.

Uitgangspunt voor de beveiliging van informatie binnen de geautomatiseerde informatievoorziening van de afdelingen en eenheden is het minimum beveiligingsniveau. Zoals aangegeven in paragraaf 3.2 worden risicoanalyses uitgevoerd om te bepalen of een team aan het minimum beveiligingsniveau voldoet. Er worden specifieke risicoanalyses uitgevoerd voor de bepaling van de aanvullende beveiligingseisen wanneer uit globale beveiligingsrisicoanalyses blijkt dat het minimum beveiligingsniveau voor een informatiesysteem ontoereikend is.

Provincie Drenthe heeft de productie-omgeving afgescheiden van de test- en ontwikkelomgeving om onbevoegde toegang tot of veranderingen aan de productie-omgeving te voorkomen.
Tegen malware worden passende beheersmaatregelen getroffen in combinatie met een passend bewustzijn van gebruikers.

C.10 Communicatiebeveiliging

De provincie Drenthe beveiligt de informatie die via netwerken wordt getransporteerd op passende wijze. Beveiliging van mail voldoet aan de eisen die hiertoe in algemeen verkeer worden gesteld. Medewerkers zijn op de hoogte van de regels die gelden rond het verzenden van vertrouwelijke (persoons-)gegevens.

C.11 Acquisitie, ontwikkeling en onderhoud van informatiesystemen

Bij ontwikkeling en wijziging van een informatiesysteem wordt bij de aanvang hiervan (plan van aanpak) aandacht besteed aan IT-beveiliging; specifiek wordt aandacht besteed aan privacy by design en privacy by default[1]. De wijze waarop dit plaatsvindt, is vastgelegd in de eisen die team I&A hanteert bij de selectie van systemen of bij eigen systeemontwikkeling. Hierbij wordt allereerst bekeken of het minimumbeveiligingsniveau toereikend is. Indien dit niet het geval is, worden bij de definitiestudie aanvullende eisen op basis van een risicoanalyse bepaald.

C.12 Leveranciersrelaties

De provincie Drenthe stelt eisen aan haar leveranciers en contractpartijen t.a.v. informatiebeveiliging. Met bewerkers, die in opdracht van de provincie haar informatie be- of verwerken, worden bewerkersovereenkomsten afgesloten.

C.13 Beheer van informatiebeveiligingsincidenten

Provincie Drenthe heeft maatregelen getroffen om zo goed en zo snel mogelijk te kunnen reageren op informatiebeveiligingsincidenten.
Het team I&A is verantwoordelijk voor het beheer van computer- en communicatieprocessen. Afspraken hierover, waaronder over de uitvoering van beveiligingstaken, worden schriftelijk vastgelegd.
Naast het formuleren van IT-beveiligingseisen wordt bij de ontwikkeling en wijziging van een informatiesysteem ook aandacht besteed aan de inrichting van de administratieve organisatie en de interne controle. Zowel het formuleren van IT-beveiligingseisen, als de administratieve organisatie en interne controle vallen onder de verantwoordelijkheid van de eigenaar van het informatiesysteem. Daarbij vervult team BC voor de aspectgebieden administratieve organisatie en interne controle een coördinerende rol.

C.14 Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer

Binnen de provincie Drenthe wordt een proces voor continuïteitsplanning ingericht. Dit proces is erop gericht de voortgang van de kritische bedrijfsprocessen te garanderen, ook na het ontstaan van een calamiteit. Managers en teamleiders zijn verantwoordelijk voor de coördinatie van alle activiteiten (op hun specifieke terrein) die in het kader van de waarborging van de continuïteit van de kritische bedrijfsprocessen worden verricht.

Het waarborgen van de beschikbaarheid van IT-bedrijfsmiddelen vormt een onderdeel van de overall continuïteitsplanning. Hiervoor is door de Security manager IT een IT-uitwijkbeleid geformuleerd. Het realiseren van de maatregelen, voorzieningen en plannen op basis van de eisen van de systeemeigenaren valt onder de verantwoordelijkheid van de team I&A. Hierbij leveren team I&A en B&G de kaders in de vorm van het IT-uitwijkbeleid. Team I&A is verantwoordelijk voor het operationaliseren van de maatregelen.

Naast uitwijkvoorzieningen en -plannen worden ook andere maatregelen getroffen die de beschikbaarheid van de IT-bedrijfsmiddelen bevorderen, zoals back-upmaatregelen en het voorzien in

[1] Dit houdt in dat organisaties al tijdens het ontwikkelen van producten en diensten privacyverhogende maatregelen treffen en dataminimalisatie toe passen. Een voorbeeld van privacyverhogende maatregelen is het gebruiken van privacy enhancing technologies (PET); dit zijn tools, die kunnen helpen bij het borgen van privacy en security in informatiesystemen.

redundantie in de IT-infrastructuur. Alle maatregelen worden regelmatig getest en op basis van de uitkomsten van de tests bijgesteld.

C.15 Naleving

Het proces van informatiebeveiliging is niet sluitend zonder controle op de naleving van het beleid en de richtlijnen. Bij de controle op de naleving wordt onderscheid gemaakt naar een interne screening (operationele controle) en externe screening (onafhankelijke controle). De eerste vorm van controle valt onder de verantwoordelijkheid van het lijnmanagement in de vorm van interne screening. De tweede vorm van controle is een taak van de Auditfunctie (uitgevoerd onder coördinatie van de Concernstaf).

Privacy en bescherming van persoonsgegevens worden geborgd in overeenstemming met relevante wet- en regelgeving.
Periodiek vindt er rapportage plaats aan het CMT omtrent de stand van de informatiebeveiliging.