Informatiebeveiligingsbeleid ISD BOL

2023 - 2025

Brunssum, 5 september 2022
Versie: 1.0

Inhoudsopgave

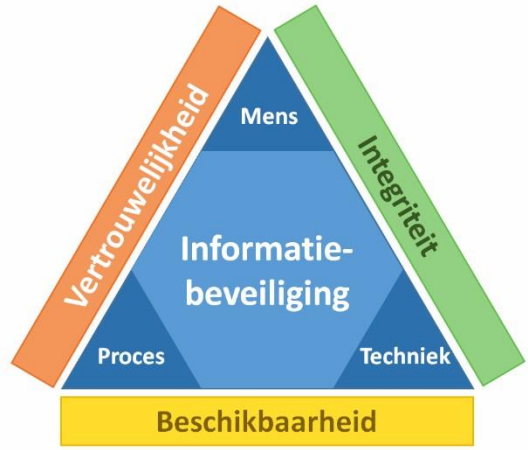
1 Inleiding

1.1 Informatiebeveiliging

Toegankelijke en betrouwbare overheidsinformatie is essentieel voor een sociale dienst om zijn processen uit te voeren. Sociale diensten beschikken over een schat aan (zeer) vertrouwelijke informatie over zowel burgers als bedrijven en daarnaast zijn zij verantwoordelijk voor een betrouwbare en continue dienstverlening. Onze klanten vertrouwen erop dat ISD BOL vertrouwelijke gegevens afdoende beveiligt. Het is daarom belangrijk dat ISD BOL op passende wijze haar informatie beveiligt.

Bij informatiebeveiliging is het belangrijk dat de juiste maatregelen, procedures en processen ervoor zorgen dat de *beschikbaarheid*, *integriteit* (juistheid, volledigheid en tijdigheid) en *vertrouwelijkheid* van informatie op het juiste niveau is beschermd. Voor het ene proces is vertrouwelijkheid van informatie belangrijker, voor het andere beschikbaarheid of integriteit. Mogelijk zijn alle aspecten van belang. Hier is weergegeven wat ISD BOL verstaat onder deze begrippen.

Beschikbaarheid / continuïteit:	Het zorg dragen voor het beschikbaar zijn van informatie en informatie verwerkende bedrijfsmiddelen op de juiste tijd en plaats voor de gebruikers.
Integriteit	Het waarborgen van de juistheid, betrouwbaarheid: volledigheid, tijdigheid en controleerbaarheid van informatie en informatieverwerking.
Vertrouwelijkheid / Exclusiviteit	Het beschermen van informatie tegen kennisname en mutatie door onbevoegden. Informatie is alleen toegankelijk voor degenen die hiertoe geautoriseerd zijn.



ISD BOL wil informatiebeveiliging op een gestructureerde wijze benaderen, zodat de beveiliging op een passend niveau is en blijft, en dat beveiligingsmaatregelen effectief en efficiënt worden ingezet. Omdat ISD BOL verantwoording aflegt aan de BOL-gemeenten

(Gemeente Brunssum en Gemeente Landgraaf), is informatiebeveiliging bij ISD BOL gebaseerd op de Baseline Informatiebeveiliging Overheid (BIO), het normenkader voor gemeenten ten aanzien van informatiebeveiliging. Dit beleid beschrijft de gewenste situatie voor ISD BOL op basis van realiseerbare doelstellingen, voortkomend uit maatregelen beschreven in de BIO.

In dit beleid is weergegeven welke onderdelen vallen onder informatiebeveiliging. Vervolgens staat in het beleid welke kaders en uitgangspunten gelden voor informatiebeveiliging en dat risicomanagement de basis is om beveiliging toe te passen. Daarnaast is de relatie tussen de visie van ISD BOL en informatiebeveiliging weergegeven. Informatiebeveiliging ontstaat niet vanzelf. In het beleid staat hoe dit moet zijn georganiseerd en hoe de rollen en verantwoordelijkheden zijn belegd. Tenslotte is op basis van de BIO weergegeven welke informatiebeveiligingsdoelen bereikt moeten worden om ook de visie van ISD BOL te verwezenlijken.

Het informatiebeveiligingsbeleid moet daarnaast gezien worden als een overkoepelend beleidsstuk, waarbij in onderliggende plannen, documentatie, procedures en instructies verdere detaillering en afspraken zijn of moeten worden vastgelegd.

1.2 Reikwijdte en afbakening informatiebeveiliging

De reikwijdte van dit beleid omvat alle processen, onderliggende informatiesystemen, informatie en gegevens van ISD BOL en externe partijen, het gebruik daarvan door medewerkers en (keten)partners in de meest brede zin van het woord, ongeacht locatie, tijdstip en gebruikte apparatuur. Daarbij maakt ISD BOL gebruik van Software-as-a-Serviceoplossingen (‘cloudapplicaties’) en besteedt een aantal diensten uit, zoals het beheer van de IT-infrastructuur en facilitaire zaken. De in dit beleid beschreven richtlijnen en kaders gelden dan ook voor de verwerking van informatie door dergelijke externe partijen. ISD BOL moet afspraken hieromtrent formeel vastleggen met deze externe partijen. Naast de hoofdovereenkomst, vereist dit ook verwerkersovereenkomsten voor leveranciers die persoonsgegevens verwerken en dienstverlenersovereenkomsten (DVO’s). ISD BOL dient naleving van deze overeenkomsten periodiek te beoordelen zodat zij de betrouwbaarheid van informatieverwerking blijft borgen. Verder zijn wet-, en regelgeving en interne/externe eisen aanvullend op dit beleid.

2 Informatiebeveiligingsbeleid

2.1 Uitgangspunten

Het gehele management geeft een duidelijke richting aan informatiebeveiliging en demonstreert dat zij informatiebeveiliging ondersteunt en zich hierbij betrokken voelt, door het uitdragen en handhaven van een informatiebeveiligingsbeleid van en voor ISD BOL. De strategische doelen van het informatiebeveiligingsbeleid zijn:

- Het managen van de informatiebeveiliging.
- Adequate bescherming van bedrijfsmiddelen.
- Het minimaliseren van risico's van menselijk gedrag.
- Het voorkomen van ongeautoriseerde toegang.
- Het garanderen van correcte en veilige informatievoorzieningen.
- Het beheersen van de toegang tot applicaties.
- Het waarborgen van veilige informatiesystemen.
- Het adequaat reageren op incidenten.
- Het beschermen van kritieke bedrijfsprocessen.
- Het beschermen en correct verwerken van persoonsgegevens van burgers en medewerkers.
- Het waarborgen van de naleving van dit beleid.

De belangrijkste uitgangspunten van het beleid zijn:

- Er is wet- en regelgeving waar altijd aan voldoen moet worden. Dit kan tot gevolg hebben dat hieruit maatregelen ontstaan op het gebied van informatiebeveiliging.
- De BIO is het voornaamste onderliggend kader. ISD BOL stelt dit normkader vast waarbij er ruimte is voor risicoafweging en prioritering op basis van *'pas toe of leg uit'*.
- Alle informatie en informatiesystemen zijn van belang voor ISD BOL. Bepaalde informatie is van vitaal en kritiek belang. Het dagelijks bestuur is eindverantwoordelijke voor de informatiebeveiliging.
- Het lijnmanagement verantwoordt zich over de inrichting en de werking van informatiebeveiliging. Alle informatiebronnen en -systemen die gebruikt worden door ISD BOL hebben een interne eigenaar die de vertrouwelijkheid en/of waarde bepaalt van de informatie die ze bevatten. De primaire verantwoordelijkheid voor de bescherming van informatie ligt dan ook bij de eigenaar van de informatie.
- Door periodieke controle, organisatie brede planning én coördinatie wordt de kwaliteit van de informatievoorziening verankerd binnen de organisatie. Het

informatiebeveiligingsbeleid vormt samen met het informatiebeveiligingsplan het fundament onder een betrouwbare informatievoorziening. Het plan wordt periodiek bijgesteld op basis van nieuwe ontwikkelingen, registraties in het incidentenregister en bestaande risicoanalyses.

- Informatiebeveiliging is een continu verbeterproces. 'Plan, do, check en act' vormen samen het managementsysteem van informatiebeveiliging.
- ISD BOL stelt de benodigde mensen en middelen beschikbaar om haar eigendommen en werkprocessen te kunnen beveiligen volgens de wijze zoals gesteld in dit beleid.
- Regels en verantwoordelijkheden voor het beveiligingsbeleid dienen te worden vastgelegd en vastgesteld.
- Iedere medewerker, zowel vast als tijdelijk, intern of extern, is verplicht waar nodig gegevens en informatiesystemen te beschermen tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht en bij vermeende inbreuken hiervan melding te maken.

2.1.1 Visie ISD BOL

Een informatiebeveiligingsbeleid dient afgestemd te zijn op de (interne en externe) omgeving waarin het beleid wordt gebruikt, op de toekomst en op het beleid en de visie van de organisatie. In dit hoofdstuk wordt ingegaan op de visie van ISD BOL.

Volgens het Meerjarenbeleidsplan ISD BOL 2019-2022 gaat ISD BOL als uitvoeringsorganisatie voor een optimale dienstverlening aan de burgers. Door analyse gestuurd werken ofwel dat medewerkers voorafgaand aan dienstverlening beter inschatten of een burger de relevante informatie, juist en tijdig aanlevert is er minder controle nodig. 'Analyse-gestuurd werken' zal ook integraal worden toegepast in de bedrijfsvoering van ISD BOL, zo staat in het beleidsplan. Verder blijft ISD BOL steeds meer gebruik maken van de mogelijkheden die de digitale snelweg biedt. Vanaf 2016 zet ISD BOL versterkt in op de mogelijkheid tot digitaal aanvragen met oog op de burgers. Het beleidsstandpunt hierbij is: automatisering en digitalisering leidt tot administratieve lastenverlichting bij de klant en ISD BOL. Ook heeft ISD BOL zijn administratie op orde, getuige de Planning & Control cyclus. Werkwijzen, regels, procedures, taken, bevoegdheden en verantwoordelijkheden moeten beschreven zijn maar ook de interne controlemaatregelen hierop. Met uitvoering van de interne controle wordt inzicht verkregen in het bereiken van doelstellingen op het gebied van:

- Effectiviteit en efficiëntie van de processen
- Betrouwbaarheid van de financiële informatieverzorging

- Naleving van relevante wet- en regelgeving, beleidsrichtlijnen en procedures

De informatievoorziening van ISD BOL moet erin kunnen voorzien om bovenstaande visie te kunnen realiseren.

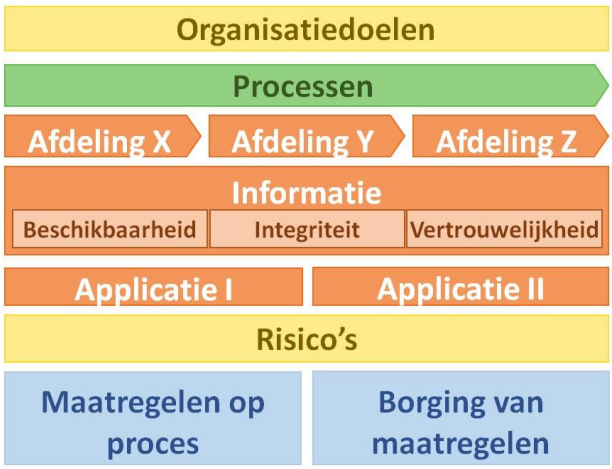
Het waarborgen van informatieveiligheid is een randvoorwaarden voor het uitvoeren van de visie van ISD BOL. Onderstaand is aangegeven hoe de uitgangspunten van ISD BOL zich verhouden met informatiebeveiliging.

- Indien ISD BOL een optimale dienstverlening wil kunnen aanbieden aan de burgers vraagt dit om juiste, volledige en tijdige informatie.
- Analyse gestuurd werken gebeurt binnen de kaders van wet- en regelgeving, waarbij het belang van de burger voorop staat. Informatie-uitwisseling gebeurt daarbij op een veilige wijze waarbij de fysieke en logische toegang voor ongeautoriseerde personen wordt voorkomen.
- Lasten verlichtende digitalisering en automatisering vraagt om technisch volwassen oplossingen (applicaties, systemen, technische infrastructuur, apparatuur), en een organisatie die haar basis op orde heeft en deze oplossingen ondersteunt.
- ISD BOL streeft naar effectieve en efficiënte processen met hierin een regisserende, faciliterende en samenwerkende organisatie met taakvolwassen medewerkers. Dit vergt eigenaarschap van proces, applicatie en informatie waarbij een eigenaar kan sturen en verbeteringen realiseren.
- Vanuit informatiebeveiliging is de PDCA-cyclus onmisbaar voor borging van de maatregelen. Interne controle en informatiebeveiliging versterken elkaar hierbij waardoor dit ten goede komt aan de effectiviteit van processen, betrouwbaarheid van de financiële informatieverzorging en aan het naleven van wet- en regelgeving, richtlijnen en procedures.

2.1.2 Controls en maatregelen

Het BIO-normenkader is specifiek gericht op informatiebeveiliging binnen overheidsinstanties. De BIO maakt onderscheid tussen controls en overheidsmaatregelen. Controls stellen beveiligingsdoelstellingen vast, de overheidsmaatregelen zijn een specifiekere uitwerking van die controls, maar dekken niet de gehele beveiligingsdoelstellingen van de control af. De overheidsmaatregelen zijn verplicht voor overheidsinstanties.

2.1.3 Risicomanagement



Informatiebeveiliging wordt vaak gezien als iets wat er extra bij komt. Informatiebeveiliging ligt echter ten grondslag aan het organisatiedoel dat bereikt dient te worden. Om een doel te bereiken, dienen processen uitgevoerd te worden waarvoor informatie (vaak in meerdere softwareapplicaties) wordt gebruikt en bewerkt. Een goede afweging van de risico's helpt om de juiste maatregelen te treffen om de gegevens in deze processen te beschermen. Hoe waardevoller of gevoeliger de informatie, hoe meer maatregelen er getroffen moeten worden. Ten slotte moeten deze maatregelen in de organisatie geborgd worden, zodat ISD BOL aantoonbaar grip houdt op de veiligheid van haar informatie.

100% beveiliging bestaat echter niet en dient ook niet nagestreefd te worden. De kosten van beveiliging moeten in verhouding zijn tot de risico's (geen dubbeltje met een kwartje beveiligen). De aanpak van informatiebeveiliging (Informatiebeveiligingsbeleid) is daarom ook 'risk based'. Bij informatiebeveiliging gaat het om het vinden van een optimale balans tussen risico's, maatregelen, kosten en werkbaarheid. Hierbij kan het voorkomen dat een risico zich manifesteert, ondanks de getroffen maatregelen. Het is wel van belang dat de risico's bekend zijn en dat een bewuste afweging is gemaakt over de te nemen risico's. Daarnaast dient ISD BOL goed te zijn voorbereid op incidenten en crises. Het informatiebeveiligingsrisico is de som van de kans op beveiligingsincidenten en de impact daarvan op het informatiesysteem: **risico = kans x impact**.

Risicomanagement is een gestructureerde manier om risico's en gevolgen in kaart te brengen, te evalueren en proactief te beheersen door het treffen van maatregelen. De proceseigenaar dient periodiek de risico's te beoordelen. Daartoe inventariseert de proceseigenaar de kwetsbaarheid van zijn werkproces en de dreigingen die kunnen leiden tot een beveiligingsincident, rekening houdend met de beveiligingseisen van de informatie. De proceseigenaar neemt indien nodig maatregelen om de risico's te beperken. De CISO kan hierbij ondersteunen in zowel techniek van risicoanalyse als bij de inhoudelijke analyse zelf. Hierbij kunnen ook applicatie-eigenaren en procesdeskundigen ondersteunen. De 'risk-based' benadering betekent ook dat gefundeerd afgeweken kan

worden van de baseline (BIO) indien ISD BOL hier een geaccepteerd risico loopt. Tegelijkertijd houdt dit in dat mogelijk meer maatregelen getroffen moeten worden ten opzichte van de baseline indien ISD BOL een hoog risico loopt. Risicomanagement is dus de eerste stap bij informatiebeveiliging.

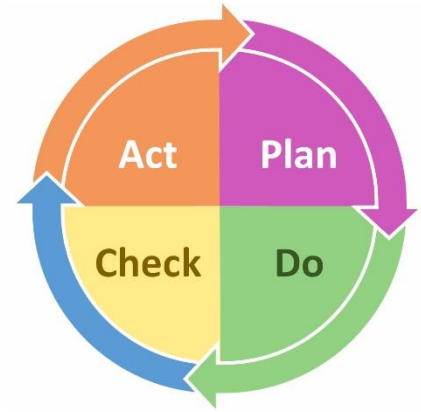
Op deze wijze worden tijd, geld en middelen passend besteed met als gevolg een stelsel van beveiligingsmaatregelen dat bij de organisatie past.

2.1.4 Plan van aanpak

De maatregelen voortkomend uit het beleid dienen te zijn uitgewerkt in het informatiebeveiligingsplan. Door uitvoering van dit plan wordt de kwaliteit van informatiebeveiliging binnen de organisatie naar een hoger niveau gebracht en verankerd. Het informatiebeveiligingsbeleid vormt samen met het informatiebeveiligingsplan het fundament onder een betrouwbare informatiebeveiliging. Zowel het plan als het beleid worden voor een periode van drie jaar vastgesteld. Gezien het feit dat zowel de omgeving als de organisatie kunnen veranderen in deze periode zal jaarlijks beoordeeld worden of het beleid en plan nog in lijn lopen met algehele organisatievisie en/of de stukken nog aansluiten op de risico's. De verantwoording ten aanzien van het informatiebeveiligingsplan wordt door het dagelijks bestuur aan het Algemeen Bestuur afgelegd.

2.2 PDCA

Informatiebeveiliging is een continu verbeterproces. De Deming-circle ('Plan, do, check en act') vormt de basis van het managementsysteem van informatiebeveiliging. Met deze structuur zal ISD BOL haar informatiebeveiliging continu borgen en verbeteren.



Aspect	Omschrijving
Plan	Plannen informatiebeveiligingsmaatregelen op basis van wet- en regelgeving en de BIO. Planning geschiedt op jaarlijkse basis en wordt indien nodig tussentijds bijgesteld. De meerjarenplanning op hoofdlijnen is uitgewerkt in het informatiebeveiligingsplan. Ook wordt de PDCA-cyclus toegepast op specifieke maatregelen.
Do	Implementeren van procedurele en technische maatregelen en naleving van het beleid en plan.
Check	Monitoren en rapporteren is onderdeel van het werkproces met als doel: waarborgen van de effectiviteit van informatiebeveiligings-maatregelen en compliance aan wet- en regelgeving.
Act	Beslissing om bij te sturen en uitvoeren van verbeteracties. De cyclus is een continu proces; de bevindingen van (in- en externe) controles zijn weer input voor de jaarplanning en de beveiligingsplannen.

3 Organisatie van informatiebeveiliging

Dit hoofdstuk gaat in op rollen en verantwoordelijkheden en op de borging van informatiebeveiliging. Een adequaat opgezette informatiebeveiliging vereist een governancestructuur waarin rollen en verantwoordelijkheden op het gebied van Informatiebeveiliging zijn gedefinieerd en waarmee de besluitvorming, rapportage en escalatiestructuren met betrekking tot dit onderwerp zijn gereguleerd.

3.1 Interne organisatie

3.1.1 Rollen

In dit hoofdstuk worden de verschillende rollen, taken en verantwoordelijkheden beschreven die bepalend zijn voor de uitvoering van een gedegen informatiebeveiligingsbeleid.

3.1.1.1 Algemeen Bestuur

Het algemeen bestuur stelt middelen beschikbaar voor informatiebeveiliging. Daarnaast heeft het algemeen bestuur een controlerende functie ten aanzien van de informatiebeveiliging.

3.1.1.2 Dagelijks Bestuur

Het dagelijks bestuur is in de sturende rol eindverantwoordelijk voor de adequate beveiliging van informatie binnen ISD BOL om:

- Het informatiebeveiligingsplan en -beleid vast te stellen;
- Beoordeelt risico's
- Toezicht te houden op de uitvoering van het informatiebeveiligingsplan en -beleid;
- Voorstellen aan het algemeen bestuur voor te leggen om voldoende middelen beschikbaar te stellen voor de adequate inrichting van informatiebeveiliging;
- Risico's te beoordelen en besluiten te nemen over informatiebeveiliging.

Het Dagelijks Bestuur heeft haar taken gemandateerd aan de directeur van ISD BOL.

3.1.1.3 Management

Het management is in haar sturende rol verantwoordelijk voor de kaders en de invulling van het informatiebeveiligingsbeleid. Het management zorgt ervoor dat zij:

- Stuurt op bedrijfsrisico's;
- Heeft een positieve en actieve houding ten aanzien van informatiebeveiliging;
- Draagt zorg dat de medewerkers voldoende security- en privacytraining krijgen om de taken goed te kunnen uitvoeren. Daarbij hoort ook het op peil houden van digitale vaardigheden.
  De benodigde kennis en kunde kunnen per functie verschillen;
- Stuurt op beveiligingsbewustzijn, bedrijfscontinuïteit en naleving van regels en richtlijnen (gedrag en risicobewustzijn);
- Rapporteert over compliance aan wet- en regelgeving en algemeen beleid
- Vervult een voorbeeldrol richting de medewerkers;
- Rapporteert (via de CISO) rondom de relevante informatiesystemen over de voortgang van de planning, status van informatiebeveiliging, incidenten en andere ontwikkelingen;
- Controleert of de getroffen maatregelen overeenstemmen met de betrouwbaarheidseisen en of deze voldoende bescherming bieden;
- Meldt nieuwe verwerkingen van persoonsgegevens bij de FG vóórdat de verwerking begint;
- Geeft wijzigingen in lopende verwerking(en) van persoonsgegevens door aan de FG;
- Voert DPIA's uit of geeft daartoe de opdracht;

- Zorgt voor inbreng van inhoudelijke en functionele kennis bij de uitvoer van DPIA's
- Effectueert de resultaten van DPIA's;
- Neemt verzoeken om inzage, correctie en verzetten ten aanzien van persoonsgegevens in behandeling;
- Draagt zorg voor het afsluiten, beheren en actualiseren van verwerkersovereenkomsten;
- Wijst een decentraal contactpersoon informatieveiligheid en privacy aan;
- Inventariseert feiten en omstandigheden in het geval van een veiligheidsincident;
- Implementeert de adviezen uit rapportages over veiligheidsincidenten;
- Brengt het belang van informatieveiligheid en privacy (periodiek) onder de aandacht van de afdeling;
- Voert het beleid uit ten aanzien van persoonsgegevens die onder zijn verantwoordelijkheid vallen.
- Evalueert periodiek de beleidskaders en stelt deze waar nodig bij;

De eigenaar heeft de volgende ***bevoegdheden***:

- verzoekt periodiek medewerkers (en indien van toepassing relaties) om persoonsgegevens te actualiseren;
- laat persoonsgegevens verwijderen, indien van relaties geen geactualiseerde gegevens worden ontvangen.

3.1.1.4 Functionaris Gegevensbescherming (FG)

De Functionaris Gegevensbescherming (FG) houdt zich bezig het toezicht op alle privacyaspecten binnen ISD BOL. De functie is onafhankelijk van de lijn belegd en de functionaris heeft de bevoegdheid om rechtstreeks naar het hoogste bestuursniveau te rapporteren. De taken van de FG zijn:

- Informeert en adviseert de organisatie en de verwerkers die namens ISD BOL persoonsgegevens verwerken over hun verplichtingen volgens de AVG;
- Ziet toe op naleving van AVG en andere EU wet- en regelgeving en nationale bepalingen omtrent gegevensbescherming;
- Ziet toe op toewijzing van verantwoordelijkheden, bewustmaking en opleiding van het bij de verwerking betrokken personeel en audits;
- Ziet toe op de nakoming van de in verwerkersovereenkomsten met verwerkers gemaakte afspraken;
- Ziet toe op de nakoming van contractuele afspraken met gezamenlijke verwerkingsverantwoordelijken ('joint controllers');

- Adviseert in vraagstukken over de verwerking van persoonsgegevens;
- Adviseert bij veiligheidsincidenten met persoonsgegevens;
- Adviseert bij de uitvoering van Data Protection Impact Assessments (DPIA's) en ziet toe of de uitvoering daarvan in overeenstemming is met de AVG;
- Ziet toe op en adviseert over de afhandeling van vragen en klachten over het gebruik van persoonsgegevens;
- Adviseert en ondersteunt bij het opstellen van privacynormen, -procedures, -beleid, -regelingen of –gedragscodes;
- Rapporteert rechtstreeks aan het hoogste bestuursniveau;
- Stemt waar nodig af met de Autoriteit Persoonsgegevens;
- Treedt op als contactpunt voor de Autoriteit Persoonsgegevens;
- Is contactpunt voor betrokkenen (dit kunnen zowel inwoners als medewerkers zijn) inzake de omgang met persoonsgegevens. De FG is daarbij gehouden aan geheimhouding.
- Signaleert knel- en verbeterpunten naar management en beleid.

De FG heeft de volgende ***bevoegdheden***:

- De FG heeft toegang tot alle diensten binnen de organisatie. Daarbij ontvangt de FG van alle afdelingen de essentiële steun, input en informatie;
- De FG is bevoegd om – op eigen initiatief – onderzoek uit te voeren, daarover (ongevraagd) te adviseren, en om van iedereen in de organisatie medewerking daaraan te eisen.

3.1.1.5 CISO/Chief Information Security Officer

De Chief Information Security Officer (CISO) is verantwoordelijk voor de *organisatie* van informatiebeveiliging. Deze rol is belegd bij het afdelingshoofd Bedrijfsvoering en Business Intelligence. De CISO heeft als taak informatieveiligheid op een hoger niveau te brengen en om het vervolgens structureel te laten borgen in de organisatie. De lijnorganisatie blijft zelf verantwoordelijk voor informatiebeveiliging. De belangrijkste bevoegdheid van de CISO is om op elke plek binnen de organisatie gevraagd en ongevraagd onderzoek te kunnen (laten) doen en zo nodig zaken voor te schrijven. Daarbij rapporteert de CISO jaarlijks over de gang van zaken. De taken van de CISO ten aanzien van informatiebeveiliging zijn als volgt samen te vatten:

- Rapporteert rechtstreeks aan de directeur;
- Opstellen, bijstellen, vernieuwen en herzien van het informatiebeveiligingsbeleid en de daaruit voortvloeiende plannen;

- Ondersteunt management bij het opstellen van informatiebeveiligingsrapportages en beoordeelt deze rapportages.
- Coördineert het formuleren van informatieveiligheidsbeleid;
- Coördineert en adviseert bij afhandelen van beveiligingsincidenten;
- Richt de informatiebeveiligingsorganisatie in;
- Stemt de informatiebeveiliging af met andere beveiligingsdomeinen;
- Stelt de informatieveiligheidsanalyse op en zorgt voor de actualisatie hiervan;
- Adviseert bij en begeleidt informatierisicoanalyses;
- Voert informatiebeveiligingsassessments uit;
- Coördineert de prioritering van informatieveiligheidsmaatregelen uit de informatieveiligheidsanalyse en de uitvoering van het actieplan informatieveiligheid;
- Ziet toe op naleving van de eisen voor informatiebeveiliging;
- Stelt een afstemmingsmechanisme op voor overleg en rapportage met betrekking tot informatieveiligheid;
- Ondersteunt de directeur en het management met kennis over informatieveiligheid en privacy, zodat zij hun verantwoordelijkheid voor de betrouwbaarheid en vertrouwelijkheid van de informatievoorziening juist kunnen invullen;
- Is aanspreekpunt voor medewerkers van de organisatie over het onderwerp informatieveiligheid;
- Volgt de externe invloeden die van invloed zijn op het beleid;
- Draagt zorg voor de voorbereiding op toekomstige informatiebeveiligingsrisico's en ICT-beveiligingsrisico's o.b.v. het dreigingsbeeld Nederlandse Gemeenten;
- Bevordert het informatieveiligheidsbewustzijn in de organisatie;
- Houdt de registratie van informatieveiligheidsincidenten bij in een incidentenregister en is verantwoordelijk voor de juiste afhandeling en evaluatie van incidenten;
- Rapporteert *jaarlijks* over de voortgang van de planning, status van informatiebeveiliging, incidenten en andere ontwikkelingen.

3.1.1.6 Informatiebeveiligingsfunctionaris

Deze rol is erop gericht om - op basis van de Baseline informatiebeveiliging Overheid (BIO) - zorg te dragen voor een samenhangend pakket van maatregelen ter waarborging van de vertrouwelijkheid, integriteit en beschikbaarheid van de informatie binnen ISD BOL.

De informatiebeveiligingsfunctionaris heeft in ieder geval de volgende ***verantwoordelijkheden***:

- Opstellen, bijstellen, vernieuwen en herzien van het informatiebeveiligingsbeleid en de daaruit voortvloeiende informatie(beveiligings-)plannen;
- Optreden als informatiebeveiligingsadviseur (voor het management) bij nieuwe ICT voorzieningen en bij ingrijpende veranderingen in de ICT-infrastructuur;
- Het management adviseren bij de uitwerking van het informatiebeveiligingsbeleid in informatiebeveiligingsplannen voor hun verantwoordelijkheidsgebieden en bij de implementatie van deze plannen;
- Initiëren of laten uitvoeren van periodieke beveiligingsaudits, risico-, afhankelijkheids- en kwetsbaarheidsanalyses;
- Verantwoordelijk voor het opzetten en initiëren van (periodieke) informatiebeveiligings-bewustzijnsprogramma's en adviseren over voorlichting en training van gebruikers in het correct omgaan met informatie(systemen);
- Registreren van informatiebeveiligingsincidenten en deze bijhouden in een incidentenregister. Is verantwoordelijk voor de juiste afhandeling en evaluatie van incidenten;
- Binnen de P&C cyclus rapporteren over het aspect informatiebeveiliging;
- Aanspreekpunt voor medewerkers van ISD BOL over het onderwerp informatiebeveiliging.

Verantwoordelijkheden

- Is productverantwoordelijk voor de kwaliteit en kwantiteit van de output. Deze wordt jaarlijks vastgelegd en besproken in de functioneringscyclus;
- Is bevoegd tot handelen conform het bevoegdhedenbesluit en de mandaatregeling ISD BOL.

3.1.1.7 Beveiligingsfunctionaris Suwinet

Binnen de organisatie het aanspreekpunt en de verantwoordelijke voor alle activiteiten, op het gebied van informatiebeveiliging rondom Suwinet en rapporteert direct aan de directeur.

3.1.1.8 Proceseigenaren

Een proceseigenaar heeft de bevoegdheid om te bepalen hoe een proces verloopt, en heeft de verantwoordelijkheid ervoor te zorgen dat het proces aan het beleid, de klantverwachtingen en bedrijfsdoelstellingen blijft voldoen. Degene bepaalt dus de inrichting en het ontwerp van het proces, en is ook verantwoordelijk voor de resultaten

van het proces. Dit geldt ook voor maatregelen die ondersteunend zijn aan het eigen proces, maar die plaatsvinden in andere teams of afdelingen. Hiervoor dient de proceseigenaar het proces te hebben geanalyseerd, risico's in kaart te hebben gebracht en passende maatregelen te hebben getroffen (of laten treffen) om het proces te beheersen. Proceseigenaren dienen de leiding en bestuur van voldoende informatie te voorzien zodat deze in staat zijn om geïnformeerde beslissingen te nemen ten aanzien van informatiebeveiligingskwesties betreffende het proces.

3.1.1.9 Applicatie-eigenaren

Voor iedere significante vak applicatie dient in de lijnorganisatie een applicatie-eigenaar te zijn belegd. De applicatie-eigenaar heeft de bevoegdheid om te bepalen hoe de applicatie is ingericht, en heeft de verantwoordelijkheid ervoor te zorgen dat de applicatie aan het beleid, informatiebeleid, de klantverwachtingen en bedrijfsdoelstellingen blijft voldoen. Degene bepaalt dus de inrichting en het ontwerp van applicatie, en is verantwoordelijk voor de resultaten van de werking van de applicatie. Dit geldt ook voor maatregelen die ondersteunend zijn aan de eigen applicatie, maar die plaatsvinden in andere teams of afdelingen. Hiervoor dient de applicatie-eigenaar de applicatie en bijbehorende bedrijfsproces(sen) te hebben geanalyseerd, risico's in kaart te hebben gebracht en passende maatregelen te hebben getroffen. Applicatie-eigenaren dienen de leiding en bestuur van voldoende informatie te voorzien zodat deze in staat zijn om geïnformeerde beslissingen te nemen ten aanzien van informatiebeveiligingskwesties betreffende de applicatie. Het kan zijn dat de proces- en de applicatie-eigenaar in één persoon gecombineerd zijn.

3.1.1.10 Applicatiebeheerders

De applicatiebeheerder (uitvoerende rol) zorgt ervoor dat de applicatie is ingericht conform de daarvoor gestelde eisen en richtlijnen van de applicatie-eigenaar. De applicatiebeheerder is verantwoordelijk voor het in stand houden van de programmatuur waarmee de functionaliteit van een applicatie wordt gerealiseerd en van de gegevensverzamelingen waarop die programmatuur bewerkingen uitvoert.

3.1.1.11 Medewerkers

In zijn algemeenheid is iedere medewerker in dit kader verplicht tot:

- Het vertrouwelijk houden van informatie en wachtwoorden en andere vormen van toegangscodes in het bijzonder;
- Het voldoen aan alle wettelijke verplichtingen;
- Het conform interne regelgeving op veilige manier gebruiken van ICT-middelen;

- Het gebruik van software in overeenstemming met de voorwaarden uit licentieovereenkomsten;
- Het dusdanig omgaan met informatie en informatiemiddelen dat de beschikbaarheid, integriteit en betrouwbaarheid daarvan niet in gevaar komt.

Naast deze persoonlijke verantwoordelijkheid geldt voor iedere medewerker dat het belang van ISD BOL vereist dat men oog heeft voor de wijze waarop collega's omgaan met informatie en dat incidenten op dit punt worden gesignaleerd.

3.1.1.12 Werkgroep Privacy en Informatieveiligheid

De werkgroep Privacy en Informatieveiligheid (PIV) moet bestaan uit de CISO, de informatiebeveiligingsfunctionaris / functionaris Gegevensbescherming en medewerkers van verscheidene afdelingen die een sleutelrol spelen op dit thema. De werkgroep Privacy en Informatieveiligheid maakt integraal onderdeel uit van het SIO-overleg (Strategisch Informatie Overleg). Het doel van de werkgroep is het waarborgen dat privacy en informatiebeveiliging met een integrale blik wordt bekeken:

- Een brede, structurele betrokkenheid vanuit de organisatie ten aanzien van informatiebeveiliging;
- Het (sneller) signaleren van risico's op het gebied van informatiebeveiliging;
- Een verbeterde afstemming, formulering en implementatie van verbeteracties en maatregelen;
- Verschillende disciplines met elkaar in contact te brengen ten aanzien van informatiebeveiliging;
- Het doen van voorstellen voor het prioriteren en plannen van beveiligingsmaatregelen op basis van risicoanalyse;
- Klankbord voor de organisatie en management ten aanzien van informatiebeveiliging.

3.1.2 Functiescheiding

Ten aanzien van de inrichting van de organisatie geldt het beleid dat in beginsel geen enkele medewerker over de mogelijkheid beschikt om een volledige cyclus aan handelingen in een applicatie te beheren. Ten behoeve van deze 'functiescheiding' dienen rollen en verantwoordelijkheden binnen processen te zijn vastgesteld. Deze rollen zijn overeenkomstig in de relevante applicaties en systemen ingericht.

Binnen ISD BOL wordt een strikte scheiding tussen IT-functies en gebruikersfuncties, tussen beheertaken en dagelijkse werkzaamheden binnen de bedrijfsprocessen toegepast.

Dit geldt ook in het geval van uitbesteed beheer, waarbij geldt dat ISD BOL te allen tijde verantwoordelijk dient te zijn voor de betrouwbaarheid van uitbestede diensten.

3.1.3 Informatiebeveiliging in projectbeheer

Bij projecten wordt standaard een risicoanalyse uitgevoerd op basis van dit informatiebeveiligingsbeleid en geldende normen. Hiermee wordt beoogd dat informatiebeveiliging een integraal onderdeel is van de projectaanpak. In het programma van eisen voor nieuwe informatiesystemen of uitbreidingen van bestaande informatiesystemen worden ook relevante beveiligingseisen opgenomen.

3.2 Mobiele apparatuur en telewerken

Voor werken op afstand is een thuiswerkomgeving beschikbaar via beveiligde communicatie. Hierbij wordt toegang tot vertrouwelijke informatie verleend via de zgn. HUB-omgeving of op basis van 'multi-factor' authenticatie. Voor het mobiel en/of thuiswerken dient de medewerker een *Verklaring mobiel werken* te tekenen, waardoor de medewerker zich bewust wordt van de geldende regels en de risico's die kleven aan mobiel werken.

Privé-apparaten zullen niet onder het beheer en verantwoordelijkheid van ISD BOL vallen. Derhalve dienen voorzieningen en maatregelen te zijn getroffen zodat deze onbeheerde apparatuur gebruik kan maken van een gastennetwerk middels draadloze toegangspunten (Wifi) welke logisch gescheiden zijn van het bedrijfsnetwerk.

Mobiele bedrijfsapplicaties worden bij voorkeur zo aangeboden dat er geen informatie wordt opgeslagen op het mobiele apparaat ('zero footprint'). Indien dit niet mogelijk is dienen de opgeslagen gegevens versleuteld te zijn. Tevens wordt de informatie versleuteld bij transport en opslag conform de eisen, die daaraan gesteld worden in het kader van dataclassificatie. ISD BOL dient hiervoor gebruik te maken van mobile device managementoplossingen om bovenstaande te faciliteren. In alle gevallen geldt dat de uitvoering van het werk niet of minimaal beperkt wordt door getroffen maatregelen.

4 Veilig personeel

De medewerkers zijn een belangrijk beveiligingsaspect voor de informatie van ISD BOL. Zij kunnen door hun (onveilig) handelen voor een kwetsbare informatiehuishouding zorgen. Bijvoorbeeld als zij een malafide bestand downloaden of inloggegevens vrijgeven via een phishing email. Bewust veilig werkende medewerkers zorgen daarnaast voor minder

fouten, betere kantbeleving en meer efficiëntie. Het management dient daarom de algehele communicatie en bewustwording rondom informatieveiligheid te bevorderen. Op deze wijze zijn alle werknemers, ingehuurd personeel en externe gebruikers zich bewust van bedreigingen en gevaren voor informatiebeveiliging.

Medewerkers dienen zich ook bewust te zijn van hun verantwoordelijkheid en aansprakelijkheid, en dat ze het beveiligingsbeleid van de organisatie in hun dagelijkse werkzaamheden dienen te ondersteunen, en het risico van menselijke fouten te verminderen. Het Management dient zorg te dragen dat medewerkers zich houden aan de beveiligingsrichtlijnen. Ditzelfde dient het Management ook van externe medewerkers te verlangen.

ISD BOL moet in het instroomproces voor nieuwe medewerkers, ingehuurd personeel, stagiaires, WBU-ers en externe gebruikers over een formeel introductieprogramma beschikken. Dit programma behandelt onder meer het informatiebeveiligingsbeleid en de verwachtingen van de organisatie hierover. Onderwerpen die aan de orde komen is het gebruik van Suwinet, Cryptshare, wat te doen bij datalekken, het vergrendelen van je PC bij het verlaten van de werkplek. Daarnaast moeten werknemers, ingehuurd personeel, stagiaires, WBU-ers en externe gebruikers instemmen met de voorwaarden voor informatiebeveiliging. Deze moeten passend zijn voor de aard en de mate van toegang die zij zullen hebben tot de bedrijfsmiddelen van de organisatie die verband houden met informatiesystemen en -diensten.

Bij het indiensttredingsproces dient ISD BOL voor nieuw personeel (ook extern) een verificatie op de achtergrond uit te voeren in overeenstemming met relevante wetten, voorschriften en ethische overwegingen. Minimaal zal zij controle uitvoeren op referenties, diploma's en identiteit. Elke medewerker, ongeacht in welke vorm van dienstverband de medewerker werkzaam is (vast, tijdelijk, stagiaire, WBU enz.) dient tevens een Verklaring Omtrent Gedrag aan te leveren. Ook externe medewerkers overleggen een VOG. De VOG dient te worden aangeleverd voor aanvang van de werkzaamheden.

5 Beheer van bedrijfsmiddelen

5.1 Verantwoordelijkheid voor bedrijfsmiddelen

Binnen ISD BOL worden veel bedrijfsmiddelen gebruikt die toegang geven tot informatie. Om ervoor te zorgen dat het gebruik van deze bedrijfsmiddelen veilig verloopt, is het belangrijk dat er sturing is op deze middelen. Het dient bekend te zijn welke bedrijfsmiddelen belangrijk zijn, welke bedrijfsmiddelen er binnen de organisatie aanwezig zijn, wie de eigenaar is van deze bedrijfsmiddelen, en wie de bedrijfsmiddelen gebruikt. Daarnaast dient bekend te zijn wanneer wijzigingen in deze bedrijfsmiddelen noodzakelijk zijn, en dienen deze bedrijfsmiddelen veilig gebruikt te worden.

De verantwoordelijkheid voor bedrijfsmiddelen ligt bij de eigenaar van het middel indien meerdere medewerkers of meerdere processen het bedrijfsmiddel gebruiken. Voorbeelden hiervan zijn informatiesystemen of informatie. Verantwoordelijkheid voor bedrijfsmiddelen in gebruik bij individuele medewerkers waarmee zij hun taak uit oefenen, ligt bij de medewerker. Bij ontvangst van een dergelijke middel – laptop, tablet, smartphone, headset, beeldscherm, kabels, muis, toetsenbord - dient de medewerker een overeenkomst te tekenen omtrent aanvaardbaar gebruik van bedrijfsmiddelen. Deze overeenkomst beschrijft ook bepalingen ten aanzien van omgang met informatie.

In 2007 is een DVO met Landgraaf vastgelegd dat de gemeente Landgraaf het technisch applicatiebeheer van ISD BOL voor haar rekening neemt. Deze DVO wordt ieder jaar stilzwijgend verlengd. In 2012 heeft de gemeente Landgraaf haar technisch applicatiebeheer neergelegd bij de GR Parkstad-IT. En daarmee is ook het technisch applicatiebeheer van ISD BOL neergelegd bij Parkstad-IT. De DVO tussen gemeente Landgraaf en ISD BOL is nog steeds geldend. Juridisch gezien is de gemeente Landgraaf dan ook voor ISD BOL de partij waarmee zaken wordt gedaan. In praktijk is er inmiddels een situatie ontstaan dat met regelmaat rechtstreeks contact wordt gelegd tussen ISD BOL en Parkstad-IT. Zo ook over de bedrijfsmiddelen waar ISD BOL beschikt (beschikbaarstelling, beheer, beveiliging). De gemeente Landgraaf wordt meegenomen in de afspraken tussen ISD BOL en Parkstad-IT.
De GR Parkstad-IT bevindt zich momenteel in een mogelijke transitie naar een mogelijk andere vorm van gemeenschappelijke regeling en dienstverleningsconcept. In afwachting van deze nieuwe overeenkomst wordt er op dit moment, na overleg met de gemeente Landgraaf, nog geen stappen ondernomen om te komen tot een zelfstandige dienstverleningsovereenkomst tussen ISD BOL en Parkstad-IT. Tot het moment dat het

komt tot een zelfstandige DVO tussen ISD BOL en Parkstad-IT blijft de lopende DVO tussen de gemeente Landgraaf en ISD BOL gelden. Zij het dat een rechtstreeks contact tussen ISD BOL en Parkstad-IT met betrekking tot allerlei zaken die betrekking hebben op technisch applicatiebeheer, uit praktische overwegingen een feit zal zijn.

Alle bedrijfsmiddelen die op enige wijs informatie verwerken of toegang geven tot informatie worden duidelijk geïdentificeerd en ISD BOL houdt een inventaris bij van deze bedrijfsmiddelen.

Voor alle informatie en bedrijfsmiddelen worden maatregelen getroffen ter voorkoming van onbevoegde openbaarmaking, toegang, modificatie, verwijdering of vernietiging. Ten aanzien van verwijderbare media en ICT-apparatuur moeten beheerprocedures zijn beschreven en vastgesteld voor onder andere het gebruik, hergebruik en afvoer. De classificatie van de informatie wordt in acht genomen bij het bepalen van de specifieke technische en procedurele maatregelen.

5.2 Informatieclassificatie

Om te kunnen bepalen welke beveiligingsmaatregelen moeten worden getroffen ten aanzien van processen en informatiesystemen worden beveiligingsclassificaties gebruikt. Classificatie maakt zichtbaar in hoeverre de organisatie een potentieel risico loopt. Daarmee is het vereiste beschermingsniveau zichtbaar en maakt de classificatie duidelijk welke maatregelen nodig zijn om de informatie op het juiste niveau te beschermen. Zo kunnen maatregelen gericht worden getroffen waardoor de middelen (geld, tijd) gericht kunnen worden besteed.

Binnen ISD BOL dient informatie op de drie betrouwbaarheidsaspecten van informatie te zijn geclassificeerd: beschikbaarheid, integriteit (juistheid, volledigheid) en vertrouwelijkheid.

Er worden vier beschermingsniveaus gedefinieerd als zijnde basisbeveiligingsniveaus (BBN). Deze niveaus zijn: niet nodig (BBN0), belangrijk (BBN1), noodzakelijk (BBN2) en essentieel (BBN3). De niveaus zijn in onderstaande tabel weergegeven. Deze niveaus zijn gedefinieerd om het proces van classificeren te vereenvoudigen en bijbehorende maatregelen te kunnen identificeren en uniform te kunnen toepassen. In het geval van verwerking van bijzondere persoonsgegevens in termen van privacywetgeving geldt dat hiertoe te allen tijde de classificatie noodzakelijk (BBN2) van toepassing is.

Niveau	Vertrouwelijkheid	Integriteit	Beschikbaarheid
Geen	**Openbaar (0)** Informatie mag door iedereen worden ingezien. *(Bijv.: algemene informatie op de publieke website van ISD BOL)*	**Niet zeker (0)** Informatie mag worden veranderd, schending integriteit heeft geen vervolgschade. *(Bijv.: templates en sjablonen)*	**Niet nodig (0)** Gegevens kunnen zonder gevolgen langere tijd niet beschikbaar zijn. Schending brengt geen schade toe. *(Bijv.: brochures)*
Belangrijk	**Bedrijfsvertrouwelijk (BBN1)** Informatie is toegankelijk voor alle medewerkers van de organisatie. Schending brengt enige schade toe. *(Bijv.: Personeelsgids)*	**Beschermd (BB1)** Het bedrijfsproces staat enkele (integriteits-) fouten toe. Schending kan enige schade toebrengen *(Bijv.: interne voortgangsrapportages)*	**Belangrijk (BBN1)** Informatie mag incidenteel niet beschikbaar zijn. Schending breng kan enige schade toebrengen. *(Bijv.: administratieve gegevens)*
Noodzakelijk	**Geheim (BBN2)** Informatie is alleen toegankelijk voor een beperkte groep gebruikers. Schending brengt serieuze schade toe. *(Bijv.: cliëntgegevens, zorgdeclaraties)*	**Hoog (BBN2)** Het bedrijfsproces staat zeer weinig fouten toe. Schending brengt serieuze schade toe. *(Bijv.: bedrijfsvoeringinformatie en primaire procesinformatie)*	**Noodzakelijk (BBN2)** Informatie moet vrijwel altijd beschikbaar zijn, continuïteit is belangrijk. Schending brengt serieuze schade toe. *(Bijv.: cliëntdossiers)*
Essentieel	**Geheim (BBN3)** Informatie is alleen toegankelijk voor direct geadresseerde(n). Schending brengt (zeer) grote schade toe.	**Absoluut (BBN2 met aanvullende risicoanalyse[1])** Het bedrijfsproces staat geen fouten toe. Schending brengt (zeer) grote schade toe. *(Bijv.: medische gegevens)*	**Essentieel (BBN2 met aanvullende risicoanalyse)** Informatie mag alleen in uitzonderlijke situaties uitvallen, bijvoorbeeld bij calamiteiten. Schending brengt (zeer) grote schade toe.

[1] In de BIO zijn beveiligingsmaatregelen voor integriteit en beschikbaarheid gedefinieerd tot het niveau BBN2, daarboven moet men een risicoafweging maken voor de extra maatregelen.

	(Bijv.: zorggegevens en strafrechtelijke informatie)		*(Bijv.: zorggegevens)*

Bron: https://www.informatiebeveiligingsdienst.nl/product/handreiking-dataclassificatie-2/

6 Toegangsbeveiliging

ISD BOL beheert maatregelen omtrent toegang tot gegevens en informatiesystemen. Hiermee worden risico's op ongeautoriseerde acties beperkt, zoals het ongeautoriseerd raadplegen, wijzigen, of gebruiken van gegevens en informatiesystemen. Dit verhoogt namelijk de kans op zaken als datalekken, fraude, fouten of foutieve verwijdering van gegevens. Logische toegangsbeveiliging dient gebaseerd te zijn op de classificatie van de informatie, zoals beschreven in hoofdstuk 6.2 van dit informatiebeveiligingsbeleid. De proceseigenaar dient te bepalen wie toegang krijgt tot een bepaalde applicatie (binnen het proces) en welke autorisaties daarvoor van toepassing zijn. De proceseigenaar verleent derhalve goedkeuring voor toekenning of wijziging van toegangsrechten c.q. autorisaties. De proceseigenaar dient ervoor te zorgen dat de applicatiebeheerder de wijzigingen uitvoert.

In het geval zich omstandigheden voordoen waarbij gebruikers informatie in zien waarvoor zij niet bevoegd zijn, dan moet controle achteraf mogelijk zijn. De toegangsbeveiliging zal daarom moeten voorzien in mogelijkheden voor registratie van verleende toegang. Bijvoorbeeld door vastlegging van de noodzaak tot doorbreking reguliere toegang en/of de logging van handelingen tijdens die toegang.

6.1 Authenticatie en autorisatie

Ten aanzien van herleidbaarheid en transparantie van uitgevoerde handelingen geldt als uitgangspunt dat unieke gebruikersidentiteiten aanwezig dienen te zijn. Dit zodat gebruikers kunnen worden gekoppeld aan hun handelingen. Op deze wijze kunnen zij ook verantwoordelijk worden gesteld voor hun handelingen. Het gebruik van generieke identiteiten of groepsaccounts dient te zijn beperkt. Enkel nog bij de balie login wordt

gebruik gemaakt van groepsaccounts. Dit is echter gemotiveerd en vastgelegd door de proceseigenaar. Als het bij wijzigingen in de toekomst nodig blijkt, dan dienen hier specifieke richtlijnen voor opgesteld te zijn die de kaders omschrijven waarbinnen deze groepsaccounts gebruikt worden.

Wachtwoorden dienen te voldoen aan complexiteitseisen, welke worden afgedwongen door het systeem en die voldoen aan de standaard van de BIO. Daarnaast is iedere medewerker verantwoordelijk voor het geheim blijven van zijn inloggegevens. Uitwisseling van deze gegevens is niet toegestaan. Waar technisch mogelijk wordt Single Sign On nagestreefd om gebruikersgemak te verhogen. Dit betekent wel dat gebruikers hun onbeheerde apparatuur moeten vergrendelen.

Het toekennen van autorisaties dient te zijn gebaseerd op gedefinieerde rollen. Rollen worden toegekend aan gebruikers binnen organisatieonderdelen. Indien gebruikers vanaf een onvertrouwde zone toegang verkrijgen naar een vertrouwde zone, bijvoorbeeld wanneer een gebruiker een online applicatie (SAAS-oplossing) van een willekeurige plek benadert, dient authenticatie te gebeuren op basis van twee-factor-authenticatie of logt de gebruiker in in de HUB-omgeving. In het geval twee-factor authenticatie niet mogelijk is dient het wachtwoord te voldoen aan een complexiteitseis, en dient het wachtwoord minimaal iedere zes maanden vernieuwd te worden. Als er wel gebruik gemaakt wordt van twee-factor authenticatie, dan dient het wachtwoord minimaal ieder jaar vernieuwd te worden.

De autorisaties per rol en functie worden vastgelegd in een autorisatiematrix. Periodiek wordt geëvalueerd of de autorisaties zoals ingericht in de IT-systemen en applicaties overeenkomen met de in gewenste situatie als vastgelegd in de matrix. De proceseigenaar dient ervoor te zorgen dat de autorisaties juist zijn toegekend. De proceseigenaar dient dit af te stemmen met degenen die verantwoordelijk zijn voor de applicaties bij ISD BOL. Ook dient het Management de verantwoordelijkheden te bepalen voor het juist afhandelen van de beveiligingsaspecten voor het aangaan, wijzigen, en beëindigen van een dienstverband of een overeenkomst met externen.

6.2 Externe toegang

Aangezien het technisch applicatiebeheer door de gemeente Landgraaf is belegd bij Parkstad-IT betekent dit dat de gemeente Landgraaf afspraken heeft met Parkstad-IT zodat externe partijen niet op eigen initiatief verbinding kunnen maken met het besloten netwerk, tenzij uitdrukkelijk overeengekomen.

ISD BOL heeft afspraken met de gemeente Landgraaf dat de gemeente maatregelen neemt zodat externe partijen niet op eigen initiatief verbinding kunnen maken met het besloten netwerk, tenzij uitdrukkelijk overeengekomen.

Als er sprake is van een externe partij is deze verantwoordelijk voor authenticatie en autorisatie van haar eigen medewerkers. De externe partij dient dit in overeenstemming met de geldende richtlijnen van ISD BOL te doen en zal hierover rapporteren op basis van afspraken vastgelegd in een DVO. In de verwerkersovereenkomst die ISD BOL overeenkomt met externe partijen dient beschreven te zijn dat ISD BOL het recht heeft om controles uit te voeren op de juiste naleving van de richtlijnen en afspraken conform DVO. Periodiek – maar ten minste eens iedere twee jaar – wordt een dergelijke controle uitgevoerd.

Indien de externe partij toegang heeft tot persoonsgegevens of deze in opdracht van ISD BOL verwerkt, dient een (verwerkers)overeenkomst overeengekomen te worden waarin afspraken worden gemaakt over de verantwoordelijkheden en te treffen maatregelen voor de bescherming van die gegevens.

7 Cryptografie

Cryptografie zorgt voor versleuteling van informatie, hetgeen resulteert in een laatste beveiligingsmechanisme in het geval informatie in handen valt van personen die geen toegang behoren te hebben tot deze informatie. Parkstad-IT voert praktisch gezien het technisch beheer voor ISD BOL uit. Parkstad-IT dient dan ook te beschikken over een cryptografiebeleid.

In het cryptografiebeleid is vastgelegd waar cryptografie wordt toegepast, wie verantwoordelijk is voor de implementatie en wie verantwoordelijk is voor het sleutelbeheer. Daarnaast dient het cryptografiebeleid voor te schrijven waar de cryptografie aan moet voldoen, en de wijze waarop het beschermingsniveau wordt vastgesteld. Afspraken hiertoe dienen te zijn opgenomen in de dienstverleningsovereenkomst tussen gemeente Landgraaf en Parkstad-IT.

8 Fysieke beveiliging en beveiliging van de omgeving

ISD BOL heeft haar bedrijfsruimten in het pand de gemeente Brunssum. ISD BOL besteedt daarom aandacht aan de fysieke beveiliging van haar bedrijfsruimten. ISD BOL beschikt hier over een eigen ontvangsthal. Deze hal is afgesloten met een beveiligde toegang.

Achter de toegang bevinden zich de kantoorruimten van ISD BOL. Onbevoegden hebben geen toegang via deze deur naar de kantoorruimten. Medewerkers van ISD BOL betreden het gebouw van de gemeente Brunssum via een centrale ingang. Via deze ingang wordt via een beveiligde deur toegang gegeven tot de kantoorruimten van ISD BOL. Ook hier geldt, onbevoegden kunnen geen gebruik maken van deze ingang.

Alle bedrijfsruimten van ISD BOL zijn toegankelijk voor al haar medewerkers, zij verkrijgen deze toegang door een toegangspas die facilitaire zaken van gemeente Brunssum in het indiensttredingsproces overhandigt. Op dit beheerproces dient periodieke controle plaats te vinden.

Binnen haar bedrijfsruimten hanteert ISD BOL geen aparte zonering. Toegang van medewerkers van andere organisaties, gevestigd in het gemeentehuis van Brunssum, kan ISD BOL wegens de indeling van het pand niet volledig uitsluiten. Deze toegang dient wel beperkt te zijn.

De DVO tussen ISD BOL en de gemeente Brunssum zal in de loop van het jaar 2023 worden geactualiseerd, dan zullen afspraken met de gemeente Brunssum hierover moeten worden vastgelegd in de DVO.

Daarnaast hanteert ISD BOL een clean desk beleid en een clear screen beleid. ISD BOL dient erop toe te zien dat medewerkers dit nastreven zodat in het geval een medewerker van een andere organisatie de bedrijfsruimte van ISDBOL betreedt, informatie van ISD BOL niet toegankelijk is voor de desbetreffende medewerker.

Binnen haar bedrijfsruimten zijn afsluitbare kasten beschikbaar voor haar personeel. De medewerkers dienen gebruik te maken van deze middelen om fysieke informatie veilig op te bergen. Net zoals het clean desk en clear screen beleid, is dit bijzonder belangrijk gezien het feit dat de bedrijfsruimte van ISD BOL vrij toegankelijk is voor alle aanwezige personen in het gemeentehuis van Brunssum. ISD BOL voert zelf hjet beheer van de sleutels van deze kasten.

9 Beveiliging bedrijfsvoering

De bedrijfsvoering van ISD BOL dient beheerst en beveiligd te zijn. Zo houdt ISD BOL toezicht op technische kwetsbaarheden die kunnen resulteren in onbevoegde toegang van buitenaf. Daarnaast is het belangrijk logging en monitoring te houden op de

bedrijfsvoering zodat (beveiligings)incidenten binnen de bedrijfsvoering herkent, en opgepakt worden.

Wijzigingsbeheer voor informatie(middelen) dienen gedocumenteerd te zijn en bijgehouden te zijn zodat wijzigingen in IT-voorzieningen beheerst worden doorgevoerd. Nieuwe systemen, updates en functionele/technische wijzigingen worden getest in een testomgeving alvorens deze geïmplementeerd worden. Testgegevens behoren zorgvuldig te worden gekozen, beschermd en beheerst. Conform de AVG worden er geen tot personen herleidbare gegevens gebruikt als testgegevens.

Ten behoeve van de beschikbaarheid van informatie en continuïteit van bedrijfsvoering wordt in kaart gebracht welke informatie kritisch is. Op basis hiervan wordt bepaald hoe de back-up en restore processen, en infrastructurele maatregelen voor die informatie(middelen) wordt ingericht. Daarnaast wordt het gebruik van middelen gemonitord en worden inschattingen gemaakt voor toekomstige capaciteitseisen. Tevens worden de bedieningsprocedures van IT-voorzieningen gedocumenteerd, bijgehouden en beschikbaar gesteld aan de gebruikers die deze nodig hebben. Dit zorgt voor een correcte en veilige bediening van deze voorzieningen.

Maatregelen ter bescherming tegen malware worden getroffen. Er is een duidelijk gedefinieerd plan en procedure in geval van een uitbraak van een virus of inbreuk op de beveiliging van informatie.

Een deel van deze maatregelen zijn technisch van aard, en zullen door Parkstad-IT moeten worden uitgevoerd. De gemeente Landgraaf heeft hiervoor afspraken gemaakt en vastgelegd in het DVO met Parkstad IT.

10 Communicatiebeveiliging

De bij ISD BOL binnenkomende en uitgaande communicatie dient passend beveiligd te zijn. Deze communicatie kan vertrouwelijke informatie bevatten en moet daarom op een veilige manier plaatsvinden om toegang tot die vertrouwelijke gegevens door onbevoegde te voorkomen. Daarnaast kan communicatie malafide bestanden bevatten. Het is dus belangrijk dat communicatie met malafide bestanden tijdig herkend wordt, en dat wordt voorkomen dat deze schade aanricht op de informatiehuishouding van ISD BOL.

Met betrekking tot de uitwisseling van informatie dienen medewerkers, ingehuurd personeel, stagiaires, WBU-ers en externen de gedefinieerde classificaties en bijhorende beschermingsniveaus in acht te nemen. Persoonsgegevens worden enkel verzameld en uitgewisseld indien dat noodzakelijk is voor het juist kunnen uitvoeren van werkzaamheden.

Beveiligde oplossingen voor de uitwisseling van gevoelige informatie dienen beschikbaar te zijn en dienen te kunnen voorzien in de gewenste functionaliteit, zonder afbreuk te doen aan veiligheid van informatie en naleving van wet- en regelgeving. Het niet-versleuteld uitwisselen van persoonsgegevens via e-mail is niet toegestaan.

ISD BOL dient met Parkstad-IT af te spreken dat dataverkeer wat de organisatie binnenkomt en verlaat wordt bewaakt en gecontroleerd op kwaadaardige elementen. Daarnaast dient gevoelige informatie binnen het netwerk zoveel mogelijk ondergebracht te zijn in netwerksegmenten met gepaste beveiligingsmaatregelen. Verkeer tussen verschillende segmenten wordt gemonitord en waar nodig gefilterd en gescand op virussen, malware en andere, ongewenste vormen van verkeer.

Personeel wordt erop geattendeerd dat zij geen vertrouwelijke gesprekken voeren in openbare plaatsen of open kantooromgevingen en vergaderlocaties waar anderen deze gesprekken kunnen horen.

11 Acquisitie, ontwikkeling en onderhoud van informatiesystemen

Bij de aanschaf, ontwikkeling en het onderhoud van applicaties dient informatiebeveiliging beoordeeld te worden. Nieuwe applicaties verkrijgen toegang tot de IT-omgeving van ISD BOL. Het is daarom van belang dat deze nieuwe applicaties aan bepaalde eisen voldoen zodat zij de informatiebeveiliging van de IT-omgeving niet aantast. Functionele eisen die informatiebeveiliging stelt, worden meegenomen in de aanschaf van applicaties. Daarnaast worden voor een veilig informatiesysteem ook de processen van onderhoud zelf passend beveiligd.

Bij uitbesteding van processen, beheer en onderhoud, dienen afspraken over de aard en kwaliteit van dienstverlening te zijn vastgelegd.

11.1 Softwareontwikkeling en onderhoud

Applicaties worden ontwikkeld en getest op basis van landelijke richtlijnen voor beveiliging, zoals richtlijnen voor beveiliging van webapplicaties. ISD BOL dient ook zorg te dragen voor goed onderhoud van de systemen die zij gebruikt. Dit onderhoud is deels belegd bij Parkstad-IT. ISD BOL dient er daarom op toe te zien dat Parkstad-IT het onderhoud correct uitvoert.

Goed onderhoud houdt onder meer in dat bij zwaktes in software en wanneer nieuwe patches worden uitgebracht, een zorgvuldig proces wordt gevolgd om te bepalen of het uitvoeren van de patch of update wenselijk en/of nodig is.

12 Leveranciersrelaties

Omdat ISD BOL een aantal diensten uitbesteedt aan de gemeente Landgraaf en gemeente Brunssum, dienen duidelijke afspraken rondom deze dienstverlening te zijn vastgelegd in een DVO. Op deze wijze kan ISD BOL controle uitvoeren op de informatiebeveiliging van de processen die zij heeft uitbesteed. Hierbij dienen de informatiebeveiligingseisen voortkomend uit dit beleid specifiek terug te komen in deze overeenkomsten. Specifieke eisen zijn in de des betreffende hoofdstukken benoemd.

De dienstverlening van de leverancier zal ISD BOL monitoren en periodiek beoordelen. Hierbij worden prestatie-indicatoren gebruikt die ISD BOL met de dienstleverancier vooraf overeengekomen zijn. Het Management dient ervoor te zorgen dat toezicht gehouden wordt op de levering van de diensten en de producten van de leveranciers. De CISO heeft hierbij een coördinerende rol en daarnaast zorgt voor de bewaking van de algehele status van informatiebeveiliging bij uitbesteding en draagt zorg dat het informatiebeveiligingsbeleid en bijbehorende plannen en richtlijnen worden aangepast, indien noodzakelijk.

ISD BOL maakt daarnaast gebruik van SaaS-oplossingen (‘Software-as-a-Service’). Dit vereist dat ISDBOL ook duidelijke afspraken maakt met de leveranciers van deze SaaS-oplossingen rondom de omgang met informatie van ISD BOL, en deze vastlegt in DVO’s. Op basis van vigerende privacywetgeving dienen verwerkersovereenkomsten te zijn afgesloten met derden voor de verwerking van persoonsgegevens. Deze verwerkersovereenkomsten beschrijven verantwoordelijkheden rondom de verwerking van persoonsgegevens.

13 Beheer van informatiebeveiligingsincidenten

Ondanks dat de informatiebeveiliging goed op orde is, is de kans groot dat er op enig moment een beveiligingsincident plaats vindt. ISD BOL dient in zo een geval het incident adequaat en efficiënt op te lossen. Om dit te bewerkstelligen is een duidelijk incidentbeheerproces noodzakelijk.
Beveiligingsincidenten worden onverwijld bij de IBF / FG / CISO gemeld, centraal geregistreerd en kortgesloten met andere relevante actoren binnen de organisatie. In geval van het compromitteren van gevoelige informatie (lees: persoonsgegevens) worden de CISO en IBF/FG op de hoogte gesteld.

Daarnaast dient te worden beoordeeld of in het kader van de Meldplicht datalekken melding gemaakt wordt bij de Autoriteit Persoonsgegevens en/of de betrokkene (persoon op wie de gelekte data betrekking heeft). In verwerkersovereenkomsten die met externe partijen zijn afgesloten, dient te zijn opgenomen welke stappen genomen worden in het geval van een datalek of bij het vermoeden daarvan.

De administratie van incidenten wordt onder meer gebruikt om vaak voorkomende incidenten of trends te signaleren. Elk nieuw incident wordt geëvalueerd waarbij op basis van een risicoanalyse wordt afgewogen welke maatregelen genomen kunnen worden om optreden van eenzelfde soort incident in de toekomst te voorkomen. De evaluatie wordt uitgevoerd of gecoördineerd door de IBF ~~CISO~~ die er tevens over rapporteert. Over ernstige incidenten wordt bovendien gerapporteerd in de rapportage van de CISO.

De incidentbeheerprocedure dient uitgewerkt te zijn en vastgesteld te zijn en beschrijft in detail de processtappen, die genomen dienen te worden bij een melding. De procedure voor aanmelding van een incident dient bekend te zijn bij alle medewerkers en ingehuurd personeel.

Bij uitbesteding van gegevensverwerkende processen aan dienstverlener worden middels een verwerkersovereenkomst afspraken gemaakt over de omgang met beveiligingsincidenten.

14 Bedrijfscontinuïteitsbeheer

ISD BOL is voor bedrijfscontinuïteit in grote mate afhankelijk van haar dienstleveranciers.

Desalniettemin dient ISD BOL een plan te hebben voor incidenten waarbij de dienstleverancier of ISD BOL zelf de bedrijfscontinuïteit niet kan waarborgen. Daarnaast dient ISD BOL de eisen rondom bedrijfscontinuïteit vast te leggen in de DVO die ISD BOL met haar dienstleveranciers heeft. Op deze wijze staat ISD BOL paraat om adequaat te handelen in het geval een bedrijfscontinuïteitsincident zich voordoet.

Om dit te kunnen bewerkstelligen dient op de eerste plaats een business impactanalyse te worden uitgevoerd. In dit proces worden de eisen vastgelegd ten aanzien van de bedrijfscontinuïteit. Na de business impact analyse kan er een risicoanalyse worden uitgevoerd om een beter beeld te krijgen van de risico's en de gebeurtenissen die tot onderbreking van de bedrijfsprocessen kunnen leiden en de daarbij horende mogelijke gevolgen. Deze informatie dient vervolgens gebruikt te worden voor het vaststellen van een bedrijfscontinuïteitsplan, en voor het vastleggen van de concrete afspraken met dienstleveranciers.

Afhankelijk van de uitkomsten uit die analyse worden per informatiesysteem of proces maatregelen gepland om de benodigde continuïteit en beschikbaarheid van informatie te waarborgen. Deze maatregelen worden gebundeld in een bedrijfscontinuïteitsplan. In dit plan worden ook maatregelen verwerkt die de continuïteit van informatiebeveiliging tijdens incidenten waarborgen. Het bedrijfscontinuïteitsplan wordt periodiek getoetst aan de hand van oefeningen of testen. Aan de hand van de resultaten worden de plannen bijgesteld en wordt de organisatie bijgeschoold. Elke medewerker die een rol heeft in het bedrijfscontinuïteitsplan dient dan ook op de hoogte te zijn van het bestaan van het bedrijfscontinuïteitsplan en zijn of haar rol in geval van een calamiteit.

15 Naleving

Alle relevante wettelijke en regelgevende eisen en contractuele verplichtingen en de benadering van de organisatie in de naleving van deze eisen, dienen expliciet vastgesteld te zijn, gedocumenteerd te zijn en actueel gehouden te worden voor elk informatiesysteem en voor de organisatie.

De CISO dient over de naleving van het informatiebeveiligingsbeleid, de wet- en regelgeving en de gemaakte afspraken met derde partijen te rapporteren aan het Algemeen Bestuur. Op deze manier kan ISD BOL zich via het Algemeen Bestuur ook verantwoorden aan haar klanten over de status van informatiebeveiliging van de hoofdprocessen. Het Management dient op basis van een bijgewerkte lijst van vigerende

wetten en regelgeving te bewaken of aan overeengekomen vastgestelde verplichtingen is voldaan. Hierin wordt ook meegenomen of ISD BOL voldoet aan wetgeving in het kader van intellectueel eigendom, auteursrechten en gebruiksrechten.

In het kader van privacywetgeving dient ISD BOL zorg te dragen dat tot een persoon herleidbare gegevens niet langer worden bewaard dan noodzakelijk en dat het risico van onbedoelde openbaarmaking van persoonsgegevens waar mogelijk wordt beperkt door vernietigen van de gegevens, dan wel door anonimiseren of pseudonimiseren. De bescherming van gegevens en privacy behoort te bewerkstelligd te zijn in overeenstemming met relevante wetgeving, voorschriften en indien van toepassing contractuele bepalingen.

Proceseigenaren behoren te bewerkstelligen dat alle beveiligingsprocedures die binnen hun verantwoordelijkheid vallen correct worden uitgevoerd om naleving te bereiken van beveiligingsbeleid en –normen. Daarnaast worden informatiesystemen regelmatig, maar tenminste jaarlijks, gecontroleerd op effectieve implementatie van (technische) beveiligingsmaatregelen. Hiervoor dient de proceseigenaar ook afspraken zoals overeengekomen met IT-dienstverleners in de DVO’s te evalueren.