Informatiebeveiligingsplan ISD BOL

2023 - 2025

Brunssum, 30 augustus 2022
Versie 1.0
Snackers, Pascal (ISD BOL)

Inhoudsopgave

1 Informatiebeveiligingsplan ISD BOL

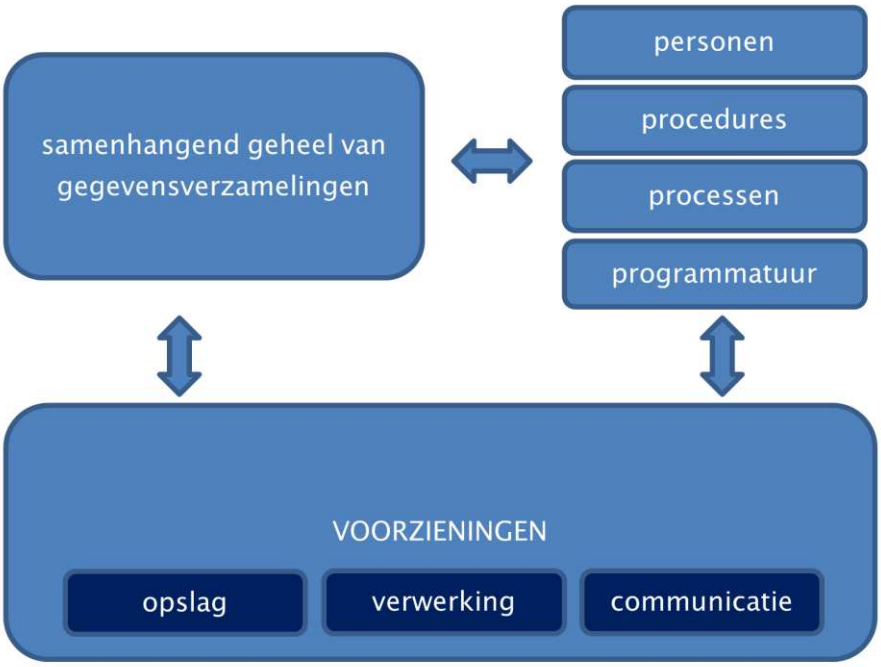
Voor u ligt het *'Informatiebeveiligingsplan ISD BOL 2023-2025'*. Dit plan beschrijft hoe ISD BOL de richtlijnen uit het *'Informatiebeveiligingsbeleid 2023-2025'* – dat zijn basis vindt in de Baseline Informatiebeveiliging Overheid (hierna: BIO) - ten uitvoer brengt.

Eind 2019 is een organisatiebrede GAP-analyse uitgevoerd. Een GAP-analyse zet de aanwezige maatregelen af tegen de maatregelen die vanuit de BIO worden verwacht. Dit plan beschrijft de te implementeren beveiligingsmaatregelen.

2 Plan en aanpak

Dit plan is opgesteld om concreet invulling te geven aan informatiebeveiliging. Het plan stelt duidelijke doelen met een specifieke tijdslijn voor de komende drie jaar.

In dit informatiebeveiligingsplan kijken we naar de organisatie als een set informatiesystemen. Een ***informatiesysteem*** is een samenhangend geheel van gegevensverzamelingen, de daarbij behorende personen, procedures, processen en programmatuur en de voor het informatiesysteem getroffen voorzieningen voor opslag, verwerking en communicatie (bron: BIO v1.04 – pag. 8-9). Hieronder is de samenhang van de onderdelen in een informatiesysteem schematisch weergegeven:



Figuur 1 Informatiesysteem

Binnen ISD BOL zijn er verschillende informatiesystemen die *organisatiebreed* de beveiliging afdekken. Denk hierbij aan beveiligingsmaatregelen die worden getroffen op facilitair gebied, gebouwbeheer, ICT-beheer en personeelszaken. Deze ***organisatiebrede informatiebeveiliging*** - inclusief de benodigde maatregelen - komt verder aan bod in ***hoofdstuk 3*** met aandacht voor:

1. Rollen, verantwoordelijkheden en overlegstructuren
2. Bewustwording en opleiding
3. Beveiliging van dienstverlenende partijen

De organisatiebrede maatregelen bieden een basis-beschermingslaag voor de ***andere informatiesystemen***. In deze andere informatiesystemen moeten ***specifieke informatiebeveiligingsmaatregelen*** ingericht worden.

Het bepalen van deze *andere informatiesystemen* en de wijze waarop hiervoor specifieke maatregelen ingericht worden, komt verder aan bod in ***hoofdstuk 4***. In dat hoofdstuk komt ook aan bod op welke wijze ***rapportage en sturing*** ingericht moeten worden om ISD BOL '*in control*' te laten zijn op het gebied van informatiebeveiliging. Rapportage en sturing moet niet alleen toegepast worden op de *specifieke* informatiesystemen, maar ook op de *organisatiebrede* informatiesystemen.

3 Organisatiebrede maatregelen en afspraken met dienstverleners

De maatregelen die ISD BOL moet treffen komen voort uit het informatiebeveiligingsbeleid en de BIO. De BIO bevat een groot aantal controls en onderliggende overheidsmaatregelen die geïmplementeerd dienen te worden. De BIO stelt dat implementatie van de overheidsmaatregelen ***verplicht*** is voor gemeenten en dus ISD BOL. Onderstaand een overzicht van drie belangrijke onderwerpen rondom ***organisatiebrede*** informatiebeveiliging.

#	Onderwerp	Verantwoordelijke
1	Benoemen rollen, verantwoordelijkheden en overlegstructuren (§ 3.1)	Management
2	Bewustwording en opleiding (§ 3.2)	CISO
3	Evalueren en eventueel herzien contracten met dienstverlenende partijen (§ 3.3)	CISO/Management

Planning

	2023				2024				2025			
	1	2	3	4	1	2	3	4	1	2	3	4
Benoemen rollen, verantwoordelijkheden en overlegstructuren												
Bewustwording en opleiding												
Evalueren en eventueel herzien contracten met dienstverlenende partijen												

3.1 Benoemen rollen, verantwoordelijkheden en overlegstructuren

- Het informatiebeveiligingsbeleid beschrijft de verschillende rollen. Deze rollen moet het management formeel vaststellen en vervolgens in de organisatie beleggen.
- De CISO zet de werkgroep Privacy en Informatieveiligheid (PIV) op. Deelnemers zijn de CISO, de informatiebeveiligingsfunctionaris/functionaris Gegevensbescherming en medewerkers van verscheidene afdelingen die een sleutelrol spelen op het thema Het doel van de werkgroep is waarborgen dat privacy en informatiebeveiliging met een integrale blik worden bekeken.
- Elk proces krijgt een proceseigenaar. Zo is duidelijk wie rapporteert en verantwoordelijk is.
- Rapportage en sturing komen verder aan bod in het informatiebeveiligingsbeleid en in hoofdstuk 4 van dit plan.

#	Actie	Verwachte tijdsbesteding	verantwoordelijke	Opmerking
1	Rol en taken van CISO beschrijven en formaliseren in functieprofiel	8-10 uur	CISO/P&O	De CISO-taken gaan belegd worden bij het afdelingshoofd BBI en zullen onderdeel gaan uitmaken van dat functieprofiel. Het afdelingshoofd is reeds benoemd in de functie CISO.
2	Koppel processen aan proceseigenaren	24-30 uur	CISO/proceseigenaren/lijnmanagement	

3	Opzetten werkgroep PIV (Privacy en Informatieveiligheid), planning maken en meetings voorbereiden	8-10 uur	CISO	De werkgroep Privacy en Informatieveiligheid maakt integraal onderdeel uit van het SIO-overleg (Strategisch Informatie Overleg).

Planning

	2023											
	jan	feb	mrt	apr	mei	jun	jul	aug	sep	okt	nov	dec
Rol en taken CISO beschrijven en formaliseren in functieprofiel												
Koppel processen aan proceseigenaren												
Werkgroep PIV opzetten												

3.2 Bewustwording en opleidingen

Het maatschappelijk en zakelijk verkeer leunt steeds meer op internet. Bedrijven en overheden gaan steeds verder met het digitaliseren van hun dienstverlening. En verzamelen steeds meer gegevens. Dat geldt ook voor ISD BOL. Deze ontwikkeling zorgt voor nieuwe beveiligingsrisico's.

De mens is een belangrijke schakel in het grotere geheel van informatiebeveiliging. De mate waarin medewerkers zich ***bewust zijn*** van de dreigingen en de mate waarin ze ***veilig gedrag*** vertonen, bepaalt de sterkte en zwakte van deze schakel. De meeste inbreuken op de vertrouwelijkheid en integriteit worden veroorzaakt door onbewust of ongewenst verkeerd handelen. Het wegen van risico's en bedreigingen moet een onderdeel zijn van ieders dagelijkse routine. Dat hoort bij een goede ***veiligheidscultuur***.

Informatiebeveiliging en privacy zijn onlosmakelijk met elkaar verbonden. Bij ISD BOL komen veel gevoelige persoonsgegevens bijeen. Het beschermen van de privacy van de klanten vereist een zorgvuldige omgang met die persoonsgegevens in de zin van de Algemene verordening gegevensbescherming (AVG). Privacy verdient aparte aandacht in ieders bewustzijn.

Om privacy en informatieveiligheid te verankeren in de organisatiecultuur:
- komen de thema's informatiebeveiliging en privacy vanaf medio maart 2022 structureel aan de orde

    - op de themapagina *'Informatiebeveiliging & Privacy'*
    - in de vorm van korte berichten op de homepage van het intranet van ISD BOL.
- bespreken we beveiligingsincidenten en datalekken in vergaderingen.
- volgt iedere gebruiker van Suwinet een e-learning over veilig gebruik daarvan.
- is in 2021 het organisatiebrede project *'iBewustzijn'* gestart.

Met het **project 'iBewustzijn'** geven we extra aandacht aan informatieveiligheid en bewust omgaan met informatie. SEP helpt ons daarbij.

- In juli 2021 is het project gestart met een nulmeting in de vorm van een enquête. De uitkomsten van de nulmeting hebben we gebruikt we om
    - het traject verder vorm te geven,
    - te bepalen welke onderwerpen aandacht zullen krijgen
    - vast te stellen of er dringende zaken zijn die direct moeten worden opgepakt.
- in december 2021/januari 2022 is een 1e phishingmail gestuurd om de alertheid van de medewerkers te testen. De resultaten zijn in briefing/afdelingsoverleg besproken
- in de tweede helft van juni 2022 is een 2e phishingmail verstuurd. De resultaten zijn in briefing/afdelingsoverleg besproken.
- de 3e phishingmail staat gepland voor de 2e helft van 2022
- vanaf medio maart 2022 hebben de medewerkers de training 'Informatieveiligheid' via de SEP-Academie gevolgd. Medewerkers die de bijbehorende examens met goed gevolg hebben afgelegd, hebben een certificaat ontvangen. De training blijft voor eenieder als naslagwerk beschikbaar in de Academie en kan desgewenst als opfrisser nog een keer gevolgd worden.
- nieuwe medewerkers krijgen bij indiensttreding – als onderdeel van hun introductieprogramma – een uitnodiging om de training 'Informatieveiligheid' via de SEP-Academie te volgen.
- In de loop van de 2e helft van 2022 (na de zomervakantieperiode) zal iedereen een uitnodiging ontvangen om module 2 ('Privacy') te volgen via de SEP-Academie.

Bewustwording is een kwestie van lange adem. De kracht schuilt in de herhaling. Om een bewustwordingstraject goed te borgen in de organisatie moet **permanent en cyclisch leren** worden geïmplementeerd, waardoor periodiek aandacht wordt gevraagd aan alle aspecten van leren over deze onderwerpen op een natuurlijke en blijvende manier.

De volgende terugkerende acties dienen periodiek uitgevoerd te worden:
*(inclusief indicatie voor de tijd die in een dergelijk **cyclisch plan** ingeruimd moet worden voor uitvoering van de diverse elementen)*

#	Actie	Verwachte tijdsbesteding	Verantwoordelijke	Toelichting
1	Stel een plan op voor permanent en cyclisch leren. Beschrijf: - De doelstellingen - De relevante stappen - De start - De planning	4 uur	CISO	GEREED: We hebben op 25 mei 2021 met Cuccibu overeenstemming bereikt over inzet van instrumenten, startdatum, planning etc. *('Voorstel Bewustwording informatieveiligheid en privacy'* met kenmerk 2021FR633)
2	Creëer het materiaal voor het traject	n.v.t.	CISO	GEREED: We gebruiken voor de e-learnings het digitale leerplatform van SEP, de SEP-Academie.
3	Creëer een korte interne opleiding ten aanzien van informatiebeveiliging en privacy voor tijdens het indiensttredingsproces	n.v.t.	CISO	GEREED: Nieuwe medewerkers volgen verplicht de trainingen 'Informatiebeveiliging' en 'Privacy' via de SEP-Academie. Bij indiensttreding wordt een account aangemaakt en een uitnodiging verstuurd.
4	Voer het traject uit	n.v.t.	CISO	LOOPT
5	Meet de resultaten van het bewustwordingstraject (phishingtest, nieuwe nul-meting, etc.)	2 uur	CISO	Periodieke inventarisatie van de vooruitgang: waar staan we NU, vergeleken met TOEN?
6	Pas het plan aan op basis van de testresultaten	4-8 uur	CISO	Als terugkerend onderdeel van de PDCA-cyclus.

Planning

	2023/2024/2025											
	jan	feb	mrt	apr	mei	jun	jul	aug	sep	okt	nov	dec
Stel een plan voor permanent en cyclisch leren op in de vorm van een bewustwordingscampagne												
Creëer het materiaal voor de campagne												
Creëer een korte interne opleiding ten aanzien van Privacy en Informatiebeveiliging voor het indiensttredingsproces												
Voer de bewustwordingscampagne uit (workshop, e-learning, etc…												
Meet de resultaten van de bewustwordingscampagne												
Pas het plan aan op basis van de resultaten												

3.3 Evalueren en eventueel herzien contracten dienstverlenende partijen

Onderwerpen als facilitaire zaken, gebouwbeheer en ICT hebben een grote impact op informatiebeveiliging. ISD BOL besteedt een deel van deze processen aan de gemeente Landgraaf en gemeente Brunssum uit. Daarom moeten deze gemeenten een aantal zaken ten aanzien van informatiebeveiliging op orde hebben. ISD BOL moet *duidelijke en heldere afspraken* met de gemeenten of andere partijen vastleggen in zogenaamde ***dienstverlenersovereenkomsten*** (hierna: DVO's). Voor de gemeenten Brunssum en Landgraaf is een DVO aanwezig. Deze DVO's worden jaarlijks stilzwijgend verlengd. Echter zijn deze gedateerd en moeten geactualiseerd worden. Aanpassing van de DVO's met Brunssum is gepland in de eerste helft van 2023. Sanne Dieteren gaat de DVO's met Landgraaf in kaart brengen. Aanpassingen zijn voorzien in de tweede helft van 2023.

De volgende acties dienen uitgezet te worden om de relevante onderdelen, zoals hieronder in de tabel nader uitgewerkt, vast te leggen.

#	Actie	Verwachte tijdsbesteding	Verantwoordelijke
1	Actualiseren afspraken DVO gemeente **Brunssum** ten aanzien van fysieke veiligheid	16-24 uur	Dagelijks Bestuur
2	Actualiseren afspraken DVO gemeente **Brunssum** ten aanzien van bedrijfscontinuïteit	16-24 uur	Dagelijks Bestuur
3	Actualiseren afspraken DVO gemeente **Brunssum** ten aanzien van gebouwbeheer	16-24 uur	Dagelijks Bestuur
4	Actualiseren afspraken DVO gemeente **Landgraaf** ten aanzien van ICT	16-24 uur	Dagelijks Bestuur
5	Actualiseren afspraken DVO gemeente **Landgraaf** ten aanzien van Burgerhoes	16-24 uur	Dagelijks Bestuur
6	Actualiseren afspraken DVO gemeente **Landgraaf** ten aanzien van ADP (salarisadministratie)	16-24 uur	Dagelijks Bestuur

Planning

	2023											
	jan	feb	mrt	apr	mei	jun	jul	aug	sep	okt	nov	dec
Actualiseren afspraken DVO gemeente **Brunssum** ten aanzien van fysieke veiligheid												
Actualiseren afspraken DVO gemeente **Brunssum** ten aanzien van bedrijfscontinuïteit												
Actualiseren afspraken DVO gemeente **Brunssum** ten aanzien van gebouwbeheer												
Actualiseren afspraken DVO gemeente **Landgraaf** ten aanzien van ICT												

Actualiseren afspraken DVO gemeente **Landgraaf** ten aanzien van Burgerhoes													
Actualiseren afspraken DVO gemeente **Landgraaf** ten aanzien van ADP (salarisadministratie)													

3.4 Controls en overheidsmaatregelen

Eind 2019 is een GAP-analyse uitgevoerd ten aanzien van de ***organisatiebrede*** informatiesystemen van ISD BOL. Het gaat dan concreet om *facilitaire zaken*, *gebouwenbeheer*, *ICT-beheer* en *personeelszaken*. Van deze organisatiebrede informatiesystemen is de status van informatiebeveiliging in kaart gebracht. Het schema hieronder geeft een overzicht van controls en overheidsmaatregelen voor ***organisatiebrede*** beveiliging die nog opgepakt moeten worden. Het overzicht bevat ook een *korte omschrijving* en een *vertaling naar de BIO-maatregelen*. Verder bevat het een *korte toelichting* vanuit de GAP-analyse. De ***volgorde van de maatregelen geeft de prioritering weer***: maatregel nummer één heeft de hoogste prioriteit.

#	Maatregelen	Korte omschrijving	Toelichting	Opmerking
1	Rollen en verantwoordelijkheden bij informatiebeveiliging *BIO 6.1.1; 6.1.1; 6.1.1.2; 6.1.1.3; 6.1.1.4; 6.1.5*	Alle verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen.	Rol en verantwoordelijkheden CISO definiëren, vaststellen en opnemen in **functieprofiel**. Verder dient Informatiebeveiliging aan de orde te komen in **projectbeheer**, ongeacht het soort project.	ISD BOL heeft géén PO Privacy Officer. Er is wél een Informatiebeveiligings-functionaris. Voor de CISO is in het functieboek 2019 (laatst vastgestelde versie) geen functieprofiel opgenomen. Wél voor de informatiebeveiligingsfunctionaris (functie 31 in het functieboek 2019). In november 2021 is gestart met het actualiseren van het functieboek en de functiebeschrijvingen. De nieuwe versie is op het moment van schrijven van

				dit plan (nog) niet beschikbaar. ***De CISO-taken*** zullen onderdeel uitmaken van het functieprofiel van het afdelingshoofd BBI. Informatiebeveiliging is sedert 2022 vast onderdeel van ***projecten*** en als zodanig opgenomen als rubriek 11 in het sjabloon voor projectplannen.
2	Privacy en bescherming van persoonsgegevens *BIO 18.1.4; 18.1.4.2*	Privacy en bescherming van persoonsgegevens behoren, voor zover van toepassing, te worden gewaarborgd in overeenstemming met relevante wet- en regelgeving.	Een **register van verwerkingen** moet samengesteld worden. Daarnaast bij relaties zullen ontbrekende **verwerkersovereen komsten** afgesloten moeten worden.	Een ***register van verwerkingen*** hebben we voor die gegevensverwerkingen waarvoor we de beveiligings- en privacyrisico's met behulp van de IRPA-tool van de Informatiebeveiligings-dienst in kaart hebben gebracht. De IRPA-tool levert dan namelijk een instant verwerkingsregister op. Er zijn ook andere oplossingen voor het verwerkingsregister. ACTIE: z.s.m. een gemotiveerde keuze maken. Met de ***verwerkersovereenkoms ten*** zijn we begonnen aan een inhaalslag (Werkmeester, CMWW, ACC, SozaXpert, WoltersKluwer). Bovendien loopt er een traject *('e-nnovatie VWO')* met het doel om te komen tot een sjabloon waarbij verwerkersovereen-komsten modulair

				opgebouwd worden: dat wil zeggen een raamovereenkomst + toepasselijke addenda per project.
3	Arbeidsvoorwaarden *BIO 7.1.2; 7.1.2.1; 7.2.1*	De contractuele overeenkomst met medewerkers en contractanten moet *hun* verantwoordelijkheden voor informatiebeveiliging en *die van de organisatie* vermelden.	Herzien van de **integriteits-verklaring** t.b.v. informatie-beveiliging.	
4	Leveranciersrelaties *BIO 15.1.1; 15.1.1.1; 15.1.1.2; 15.1.1.3; 15.1.2; 15.1.2.3; 15.1.2.4; 15.1.2.5; 15.1.2.6; 15.2.1*	Met de leverancier behoren de informatiebeveiligingseisen om risico's te verlagen die verband houden met de toegang van de leverancier tot de bedrijfsmiddelen van de organisatie, te worden overeengekomen en gedocumenteerd.	Bij offerte aanvragen waar informatie (-voorziening) een rol speelt, dienen **eisen t.a.v. informatiebeveili-ging** (beschikbaarheid, integriteit en vertrouwelijkheid) te worden benoemd. Deze eisen zijn gebaseerd op een **expliciete risicoafweging**. Op basis van een expliciete risicoafweging worden de **beheersmaatregelen** met betrekking tot leverancierstoegang tot bedrijfsinformatie vastgesteld. **Bestaande contracten** van leveranciers dienen op dit onderdeel **herzien** te worden. Jaarlijks wordt daarbij de **prestatie van leveranciers** op het gebied van informatiebeveili-	Met leveranciers die tevens verwerker of joint controller zijn, is informatiebeveiliging verplicht onderdeel van respectievelijk de verwerkersovereenkomst danwel van de verplichte onderlinge overeenkomst.

			ging beoordeeld op vooraf vastgestelde **prestatie indicatoren**, zoals in het contract opgenomen is.	
5	Acquisitie, ontwikkeling en onderhoud van informatiesystemen *BIO 14.1.1; 14.1.1.1*	De eisen die verband houden met informatiebeveiliging behoren te worden opgenomen in de eisen voor nieuwe informatiesystemen of voor uitbreidingen van bestaande informatiesystemen.	Bij nieuwe informatiesystemen en bij wijzigingen op bestaande informatiesystemen moet een **expliciete risicoafweging** worden uitgevoerd ten behoeve van het **vaststellen van de beveiligingseisen**, uitgaande van de BIO.	
6	Toegangsbeleid en autorisatiematrix *BIO 6.1.2.1; 9.2.3.1; 9.2.5.2; 9.2.5.3; 9.4.1.1; 9.4.1.2*	Opstellen van een toegangsbeleid en autorisatiematrix document + een procedure voor periodieke review.	**Autorisatiematrix** voor alle applicaties opstellen, en deze periodiek beoordelen	Er is een autorisatiematrix voor enkele applicaties: bijvoorbeeld voor de ***Suite*** (beheer bij functioneel applicatiebeheerder), voor ***E-Beheer/InForm*** (deze autorisatiematrix wordt jaarlijks aangepast en vastgesteld i.h.k.v. de DigiD-audit) en voor ***SIM*** (eveneens jaarlijks aangepast en vastgesteld i.h.k.v. de DigiD-audit). Applicatiebeheer beschikt over overzichten van geautoriseerde gebruikers (dus gebruikers die toegang hebben tot) ***Corsa***, ***ProfPortaal***, ***Liaan***, ***Cognos*** en ***Key2-applicaties***.
7	Beveiliging bedrijfsvoering *BIO 12.4.1.3*	De informatie verwerkende omgeving wordt gemonitord via detectie-voorzieningen, die worden ingezet op	Geen **SIEM en/of SOC** via detectievoorziening en aanwezig. Meenemen in	SIEM en SOC is verantwoordelijkheid van PIT.

		basis van een risico-inschatting zodat aanvallen kunnen worden gedetecteerd.	evaluatie DVO gemeente Landgraaf.	
8	Naleving *BIO 18.2.1; 18.2.1.2; 18.2.2.1; 18.2.3.1*	De aanpak van de organisatie ten aanzien van het beheer van informatiebeveiliging en de implementatie ervan (bijv. beheerdoelstellingen, beheersmaatregelen, beleidsregels, processen en procedures voor informatiebeveiliging), behoren onafhankelijk en met geplande tussenpozen of zodra zich belangrijke veranderingen voordoen te worden beoordeeld.	Er dient een ***Information Security Management System*** **(ISMS)** aanwezig te zijn waarmee aantoonbaar de gehele plan-do-check-act cyclus op gestructureerde wijze afgedekt wordt. Daarnaast is er een vastgesteld **auditplan** waarin jaarlijks keuzes worden gemaakt voor welke systemen welk soort beveiligingsaudits worden uitgevoerd.	***ISMS*** is in concept opgeleverd, maar nog niet operationeel. ***Auditplan:*** voor die applicaties waarvan het beheer ligt bij PIT, bijvoorbeeld Suite, Key2-applicaties, RPA etc… is ook het auditplan de verantwoordelijkheid van PIT. ISD BOL krijgt jaarlijks *'Third Party Memoranda'* (TPM's) van PIT. In de loop van 2022 is ISD BOL voor het DMS overgestapt op Corsa Cloud. Dat wordt gehost door de leverancier. ISD BOL zal de vereisten t.a.v. audits afstemmen met de leverancier BCT.
9	BCM/BCP *BIO 17.1.3.1; 17.1.3.2; 17.1.3.3*	Vaststellen kritieke processen voor bedrijfscontinuïteit. Vaststellen bedrijfscontinuïteitplan. Afspraken maken over redundantie met gemeente Brunssum.	Geen **calamiteitenplan** en geen beheerst proces voor een calamiteit.	In november 2021 hebben de gemeente Landgraaf en de gemeente Brunssum elk een ***bedrijfscontinuïteitsplan*** vastgesteld waarvan ook *'gezamenlijke dochter'* ISD BOL onderdeel uitmaakt. ISD BOL beschikt niet over een eigen bedrijfscontinuiteitsplan. Het bedrijfscontinuïteitsplan dient jaarlijks beoordeeld te worden en indien nodig geactualiseerd te worden. 1 x per jaar voeren de gemeente Brunssum en Landgraaf

				een test uit inzake het BCP. De bevindingen uit de test worden besproken met de directie en dienen te leiden tot eventuele aanpassingen van het BCP alsook tot eventuele aanpassingen in het nog te ontwikkelen BCP ISD BOL.
10	Fysieke beveiliging *BIO 11.1.1.1; 11.1.2.1; 11.1.3.1; 11.1.4.1; 11.1.4.2; 11.2.9.1; 11.2.9.3; 11.2.9.4*	Voor kantoren, ruimten en faciliteiten behoort fysieke beveiliging te worden ontworpen en toegepast	Alle aanwezigen in gebouw van gemeente Brunssum hebben **toegang tot bedrijfsruimte ISD BOL**. Beveilig toegang tot bedrijfsruimte ISD BOL (in overeenstemming met het informatiebeveiligingsbeleid) binnen het gebouw van de gemeente Brunssum.	***Quick win:*** toegangsbeveiliging (badgelezer) bij het kantoor van de directeur van ISD BOL en de bedrijfsruimte van ISD BOL, beide ter hoogte van de liften op de begane grond.
11	Beleid voor mobiele apparatuur *BIO 6.2.1; 6.2.1.1; 6.2.1.2; 6.2.2*	Beleid en ondersteunende beveiligingsmaatregelen behoren te worden vastgesteld om de risico's die het gebruik van mobiele apparatuur met zich meebrengt te beheren.	Mobiele apparatuur is zo ingericht dat geen bedrijfsinformatie onbewust wordt opgeslagen **('zero footprint')**. Als zero footprint (nog) niet realiseerbaar is, biedt een mobiel apparaat de mogelijkheid om de gegevens te versleutelen en moet 'wissen op afstand' mogelijk zijn d.m.v. een **Mobile Device Management (MDM)**-oplossing.	***Quick win:*** De medewerker dient een verklaring mobiel en/of thuiswerken te tekenen waardoor de medewerker zich bewust wordt van de geldende regels en de risico's die kleven aan mobiel werken. ICT-leverancier PIT maakt via leverancier Fondo gebruik van een ***Mobile Device Management (MDM)*** beheeromgeving (in de vorm van een SAAS-oplossing). Zie Werkzaamheden MDM • Parkstad-IT Parkstad IT draagt zorg voor het beheer van de

				mobiele apparaten (tablets, smartphones) inclusief bijbehorende abonnementen. Tot het beheer hoort onder andere dat PIT: • mobiele apparaten inricht volgens de PIT-standaard • zorgdraagt voor ***Mobile device management***, e-mail en internetinstellingen, security instellingen. Zie Beheer mobiele apparaten • Parkstad-IT *"Met het implementeren van het **MDM (Mobile Device Management)** is er voor Boxer gekozen doordat deze samen met dit systeem geïntegreerd kon worden."* Zie Boxer App voor Android toestellen – Handleiding • Parkstad-IT
12	Informatiebeveiligingsbeleid *BIO 5.1.1.1; 5.1.2.1*	Informatiebeveiligingsbeleid met periodieke herziening.	3-jaarlijks herzien en vaststellen voor de volgende 3-jaarlijkse periode.	Informatiebeveiligingsbeleid is er inmiddels. Vanaf nu 3-jaarlijkse herziening en hernieuwde vaststelling.

Planning

	2023				2024				2025			
	1	2	3	4	1	2	3	4	1	2	3	4
Rollen en verantwoordelijkheden bij informatiebeveiliging												
Privacy en bescherming van persoonsgegevens												
Arbeidsvoorwaarden												
Leveranciersrelaties												
Acquisitie, ontwikkeling en onderhoud van informatiesystemen												

Toegangsbeleid en autorisatiematrix												
Beveiliging bedrijfsvoering												
Informatiebeveiligingsbeleid												

4 Stappenplan BIO informatiesystemen

Zoals aangegeven (zie figuur 1) is een informatiesysteem een samenhangend geheel van gegevensverzamelingen, en de daarbij behorende personen, procedures, processen en programmatuur en ook de voor het informatiesysteem getroffen voorzieningen voor opslag, verwerking en communicatie. Om de risico's rondom informatieveiligheid te beheersen zal hier een *methodiek voor eigenaarschap, implementatie, rapportage en sturing* op moeten worden toegepast. Dit geldt voor informatiesystemen die *organisatiebreed* voor beveiliging zorgen (zie hoofdstuk 3), maar ook voor informatiesystemen waarbij *specifieke* maatregelen getroffen moeten worden. In ***dit hoofdstuk*** ligt de focus op het implementeren van de BIO voor ***informatiesystemen met specifieke maatregelen***. Het stappenplan dient echter ook toegepast te worden op de *organisatiebrede* informatiesystemen.

Onderstaand overzicht geeft de stappen weer die gevolgd moeten worden voor het uitvoeren van een gedegen implementatie van de BIO.

1. Informatiesystemen bekend en eigenaarschap vastgelegd
2. Baselinetoets en niveau vastleggen (BBN-analyse)
3. GAP-analyse maatregelen door proceseigenaar
4. Selectie en toewijzing van controls & maatregelen aan eigenaar
5. Implementatie en borging maatregelen door proceseigenaar
6. Monitoring status via ISMS en periodieke rapportage en sturing

In de volgende alinea's zullen deze stappen concreet toegelicht worden.

4.1.1 Vaststellen informatiesystemen en eigenaarschap

Het belangrijkste informatiesysteem binnen ISD BOL is de *participatie-opdracht*. Voor dit informatiesysteem dient een *eigenaar* vastgesteld te worden door het dagelijks bestuur. Daarnaast zal de CISO moeten onderzoeken of er *meer informatiesystemen* binnen ISD BOL afgebakend moeten worden. Uiteindelijk bepalen de eigenaren van de informatiesystemen wat binnen de scope van die informatiesystemen valt.

4.1.2 Vaststellen basisbeveiligingsniveaus

In de BIO zijn op basis van de generieke schades en dreigingen voor de overheid standaard Basis Beveiligings Niveaus (BBN's) gedefinieerd met bijbehorende beveiligingseisen die moeten worden ingevuld. Per informatiesysteem bepaalt het lijnmanagement het basis beveiligingsniveau (BBN). Een BBN is het niveau dat aangeeft

welke maatregelen er aanwezig moeten zijn op het gebied van informatiebeveiliging. Om te bepalen of een informatiesysteem al een bepaald basis beveiligingsniveau heeft, of dat er méér maatregelen nodig zijn, wordt een ***BBN-toets*** uitgevoerd. De uitkomsten kunnen worden gebruikt om te bepalen welke maatregelen nodig zijn voor een proces en onderliggende informatiesystemen. Deze maatregelen kunnen worden verkregen uit een voorgedefinieerde lijst met maatregelen bovenop de baseline, of door een aanvullende diepgaande risicoanalyse. Voor ieder informatiesysteem binnen ISD BOL moet het basis beveiligingsniveau worden vastgesteld om inzicht te krijgen welk informatiesysteem het meest kritiek is en dus de meeste aandacht verdient rondom beveiligingsmaatregelen. Gemeenten hanteren hiervoor drie verschillende niveaus welke in onderstaande tabel zijn weergegeven. De CISO begeleidt dit proces waarbij de eigenaar van het informatiesysteem de uiteindelijke keuze maakt welk BBN van toepassing is.

BBN	Omschrijving	Toelichting
BBN1	Basisniveau	Basisniveau Informatiesystemen op BBN1 zijn systemen waar BBN2 te zwaar voor is. Overheidssystemen moeten als minimum aan BBN1 voldoen. Controls en overheidsmaatregelen komen voort uit wet- en regelgeving en algemene beveiligingsprincipes.
BBN2	Niveau (bijna) alle	BBN2 vormt voor informatiesystemen binnen de overheid het uitgangspunt. BBN2 is van toepassing ▪ indien er vertrouwelijke informatie wordt verwerkt ▪ mogelijke incidenten leiden tot bestuurlijke commotie of ▪ de veiligheid van andere systemen afhankelijk is van de veiligheid van het eigen systeem. Controls en maatregelen van BBN2 bevatten de controls gemeentelijke processen en maatregelen van BBN1. Daarnaast komen controls en maatregelen voor BBN2 voort uit: ▪ Wet- en regelgeving; ▪ Aansluitvoorwaarden van gemeentelijke diensten; ▪ Afhankelijkheden in ketens en netwerken; ▪ Minimale eisen ten behoeve van een efficiënte beveiliging van BBN3
BBN3	Niveau AIVD, kritieke, infrastructuur, staatsgeheimen	BBN3 is van toepassing op departementaal vertrouwelijke informatie waarbij weerstand tegen dreigingen van statelijke actoren en beroepscriminelen. BBN3 is van toepassing indien verlies van informatie een grote impact heeft, waarvan niet uit te leggen is als deze niet gerubriceerd is en beschermd wordt op het niveau van BBN3.

Bron I Baseline Informatiebeveiliging Overheid, v1.04.

4.1.3 GAP-analyse maatregelen door proceseigenaar

De GAP-analyse is een methode om een vergelijking te maken tussen de ***huidige situatie*** en ***gewenste situatie*** met hierin de controls en overheidsmaatregelen uit de BIO. De

organisatiebrede GAP-analyse is gemaakt in het vierde kwartaal 2019. In deze stap wordt een GAP-analyse gemaakt voor *individuele informatiesystemen*. Dit wordt uitgevoerd door de verantwoordelijke manager, waarbij deze ondersteund en geadviseerd wordt door de CISO.

4.1.4 Selectie en toewijzing van controls & maatregelen aan eigenaar

Nadat helder is hoe de huidige situatie eruit ziet, worden controls en overheidsmaatregelen geselecteerd waarmee de 'GAP' ***overbrugd*** kan worden naar de gewenste situatie. Voor een succesvolle implementatie is het van groot belang dat voor elke control en maatregel een *eigenaar* wordt toewezen en er een *planning* aan wordt gekoppeld. De CISO begeleidt dit proces waarbij de eigenaar van het informatiesysteem de uiteindelijke keuze maakt welke controls en overheidsmaatregelen in welke volgorde toegevoegd moeten worden. De overheidsmaatregelen zijn ***verplicht***.

4.1.5 Implementatie en borging maatregelen door proceseigenaar

Als de geselecteerde controls en maatregelen een eigenaar hebben en er een heldere planning aan ten grondslag ligt, kan aan de ***implementatie*** begonnen worden. Hierbij dient op basis van risicomanagement een afweging gemaakt te worden in prioriteit. Hoofdstuk 4 van dit plan geeft al richting wat prioriteit heeft op organisatiebreed gebied binnen ISD BOL. Daarnaast kan er ook kritisch gekeken worden welke *'quick-wins'* te behalen zijn. De PDCA-cyclus moet zijn opgenomen in het ontwerp van de maatregel zoals beschreven in het beleid.

4.1.6 Monitoring, periodieke rapportage en sturing

Wanneer de controls en overheidsmaatregelen worden uitgevoerd dienen deze ***gemonitord*** te worden. Het ISMS speelt hierin een sleutelrol als beheersingsmethodiek. Het gaat om controlecyclus die toegepast moet worden op afzonderlijke controls en overheidsmaatregelen. ISMS-tooling biedt hierbij een ondersteunende rol. Hierbij wordt telkens het risico tegenover de uitvoering en kwaliteit gezet. De proceseigenaar is verantwoordelijk dat de control of overheidsmaatregel goed wordt geïmplementeerd, uitgevoerd en eventueel bijgesteld.

Tussentijds moet de proceseigenaar telkens de afweging maken of tijd, middelen en budget afdoende zijn, of dat er ***bijgestuurd*** moet worden. Risico's met een kleine impact kunnen op een lager niveau in de organisatie geaccepteerd worden. Echter, wanneer het risico een significante invloed heeft op de *beschikbaarheid*, *integriteit* en/of *vertrouwelijkheid* van de informatie en de bedrijfsvoering van de organisatie beslist het dagelijks bestuur of het risico acceptabel is of dat (extra) maatregelen getroffen moeten worden. De CISO ondersteunt bij dit proces en geeft advies.

Naast de cyclus voor specifieke controls en overheidsmaatregelen volgt er ook ***elk jaar een rapportage***. De CISO heeft hierin een coördinerende rol. Jaarlijks voorziet de CISO het management en het Dagelijks Bestuur van een rapport met een beschrijving van de *huidige situatie*, de *gewenste situatie*, de *voortgang* die gemaakt is, en de *planning* voor het komend jaar. Verder bevat dit rapport ook een *advies* over mogelijke bijstelling van deze planning. Zo blijft zowel het management als het Dagelijks Bestuur op de hoogte en kunnen zij indien nodig sturing geven.

Naast het jaarlijkse rapport wordt er **per kwartaal een status-update** afgegeven. Daarmee kan op hoger niveau de voortgang in grote lijnen gemonitord worden. Dienen zich nieuwe risico's aan? Of zijn risico's onvoldoende afgedekt? Dan kan het Dagelijks Bestuur besluiten om risico's te accepteren of bij te sturen. De CISO kan het Dagelijks Bestuur hierbij ondersteunen en adviseren.

#	Actie	Verwachte tijdsbesteding (*)	Verantwoordelijke
1	Informatiesystemen bekend en eigenaarschap vastgelegd	5-8 uur	CISO/leidinggevenden
2	Baselinetoets en niveau vastleggen (BBN-analyse)	4 uur	CISO/proceseigenaren
3	GAP-analyse maatregelen door proceseigenaar	4-8 uur	CISO/proceseigenaren
4	Selectie en toewijzing van controls & maatregelen aan eigenaar	2-4 uur	CISO/proceseigenaren
5	Implementatie en borging maatregelen door proceseigenaar	Afhankelijk van de te treffen maatregelen	CISO, proceseigenaren, procesdeskundigen, applicatiebeheerders
6	Monitoring status via ISMS en periodieke rapportage en sturing	4 uur	CISO/Dagelijks Bestuur

(*) Tijdsindicatie is per proceseigenaar.

Planning

	2023				2024				2025			
	1	2	3	4	1	2	3	4	1	2	3	4
Informatiesystemen bekend en eigenaarschap vastgelegd												
Baselinetoets en niveau vastleggen (BBN-analyse)												
GAP-analyse maatregelen door proceseigenaar												

Selectie en toewijzing van controls & maatregelen aan eigenaar												
Implementatie en borging maatregelen door proceseigenaar												
Monitoring status via ISMS en periodieke rapportage en sturing												