Classificatiebeleid Sabewa Zeeland

16 januari 2024
Mirjam van Delft - Kaijser

Versiebeheer

Versie	Datum	Door	Wijzigingen
0.1	14-12-2023	Mirjam van Delft - Kaijser	
1.0	16-01-2024	Mirjam van Delft – Kaijser	Beleid vastgesteld door MT Sabewa Zeeland

1.1 Relatie met overige documenten

- Baseline Informatiebeveiliging Overheid (BIO)
- Strategisch Informatiebeveiligingsbeleid Sabewa Zeeland 2023 - 2027
- Wijzigingsbeleid Sabewa Zeeland
- Encryptiebeleid Sabewa Zeeland

1.2 Verwijzingen naar de Baseline Informatiebeveiliging voor de Overheid (BIO)

8.2.1 Informatie Classificatie

Inleiding

Dit classificatiebeleid is een essentieel onderdeel van onze inzet voor een effectieve informatiebeveiliging binnen Sabewa Zeeland. Het zorgt voor een gestructureerde aanpak om de vertrouwelijkheid van informatie te waarborgen en de risico's voor de organisatie te minimaliseren.

De beleidsuitgangspunten in dit Classificatiebeleid zijn ontleend aan de Baseline Informatiebeveiliging Overheid (BIO). Bij elk beleidsuitgangspunt zijn de bijbehorende doelstelling en het kader uit de BIO opgenomen. Hierin zijn opgenomen:

- Control
  Dit is het nummer van de in die BIO beschreven control die voor dit onderwerp van toepassing is. Dit kan een Controle nummer zijn. overeenkomstig met ISO 27002 (blauwe tekst), of een O-maatregelnummer[1] (groene tekst). Op basis van een risicoafweging wordt door het management bepaald hoe moet worden voldaan aan de gestelde beveiligingsdoelstellingen van de controls. Voor het voldoen aan deze doelstellingen kunnen implementatierichtlijnen uit de ISO 27002, overheidsmaatregelen en/of operationaliseringen in handreikingen worden gebruikt.
- BBN – Basisbeveiligingsniveau.
  De BIO onderscheidt drie niveaus:
  - Voor BBN1 ligt de nadruk op 'wat mag minimaal verwacht worden?'.
  - Voor BBN2 ligt de nadruk op de bescherming van de meest voorkomende categorieën informatie volgens het principe 'valt de maatregel onder goed huisvaderschap; toont deze beveiliging de betrouwbare overheid?'
  - BBN3 is van toepassing op gerubriceerde informatie Departementaal Vertrouwelijk dan wel vergelijkbaar vertrouwelijk bij andere overheidslagen, waarbij weerstand tegen statelijke actoren of vergelijkbare dreigers nodig is.
- Verantwoordelijke
  In het algemeen geldt dat onderdelen van de BIO op verschillende plaatsen in de organisatie worden toegepast op grond van verschillende verantwoordelijkheden en gezagsverhoudingen. De BIO onderscheidt drie (hoofd)rollen:
  - Secretaris/algemeen directeur
    Als eindverantwoordelijke voor het beveiligingsbeleid in de organisatie is de secretaris/algemeen directeur verantwoordelijk voor de uitvoering van organisatiebrede vraagstukken ten aanzien van informatiebeveiliging.
  - Proceseigenaar
    Onder de proceseigenaar wordt de lijnmanager verstaan die verantwoordelijk is voor de beveiliging van het betreffende proces / informatiesysteem.
  - Dienstenleverancier
    Bedoeld wordt de dienstenleverancier (bijvoorbeeld SSO) binnen de overheid of organisaties in de markt waaraan de secretaris/algemeen directeur of proceseigenaar (een deel van) de beveiligingstaak inbesteedt respectievelijk uitbesteedt.

[1] *O-maatregel is de overheidsmaatregel gebaseerd op een ISO 27002 control*

2. Informatie classificatie

Doelstelling: Bewerkstelligen dat informatie een passend beschermingsniveau krijgt dat in overeenstemming is met het belang ervan voor de organisatie.

Control	BBN	Gedrag / procedure	Verantwoordelijke
8.2.1	**1**	**Classificatie van informatie** Informatie behoort te worden geclassificeerd met betrekking tot wettelijke eisen, waarde, belang en gevoeligheid voor onbevoegde bekendmaking of wijziging.	Proceseigenaar
8.2.1.1	1	De informatie in alle informatiesystemen is door middel van een expliciete risicoafweging geclassificeerd, zodat duidelijk is welke bescherming nodig is.	

2.1 Classificatie criteria

Het belang van classificeren is een inzicht krijgen in de waarde van informatie over de assen Beschikbaarheid, Integriteit en Vertrouwelijkheid. Met dit inzicht kan Sabewa Zeeland passende maatregelen nemen om die informatie te beschermen. Dit zijn de BIO maatregelen, aangevuld met de aanvullende set van BBN2+ maatregelen.

We onderkennen drie assen, met elk vier niveaus

Essentieel	Desastreus	Geheim
Noodzakelijk	Ernstig	Vertrouwelijk
Belangrijk	Gering	Intern
Niet Zeker	Verwaarloosbaar	Openbaar
Beschikbaarheid	**Integriteit**	**Vertrouwelijkheid**

2.1.1 Beschikbaarheid

De as beschikbaarheid beschrijft hoeveel en wanneer data toegankelijk is en gebruikt kan worden.

De niveaus zijn:

- **Niet zeker (B0)**: De gegevens kunnen zonder gevolgen langere tijd niet beschikbaar zijn. Schending van beschikbaarheid heeft geen gevolgschade.
- **Belangrijk (B1)**: De informatie of service mag incidenteel uitvallen, het bedrijfsproces staat incidentele uitval toe. De continuïteit zal op redelijke termijn moeten worden hervat. Schending van beschikbaarheid kan enige (in)directe schade toebrengen
- **Noodzakelijk (B2)**: De informatie of service mag bijna nooit uitvallen, het bedrijfsproces staat nauwelijks uitval toe. De continuïteit zal snel moeten worden hervat. Schending van beschikbaarheid kan serieuze (in)directe schade toebrengen.
- **Essentieel (B3)**: De informatie of dienst mag alleen in zeer uitzonderlijke situaties uitvallen, bijvoorbeeld als gevolg van een calamiteit, het bedrijf kritische bedrijfsproces staat eigenlijk geen uitval toe. De continuïteit zal zeer snel moeten worden hervat.

2.1.2 Integriteit

De as integriteit beschrijft het in overeenstemming zijn van informatie met de werkelijkheid en dat niets ten onrechte is achtergehouden of verdwenen (juistheid, volledigheid en tijdigheid).

De niveaus zijn:

- **Verwaarloosbaar (I0)**: Deze informatie mag worden veranderd. Geen extra bescherming van integriteit noodzakelijk. Schending van integriteit heeft geen gevolgschade.
- **Gering (I1):** Het bedrijfsproces dat gebruik maakt van deze informatie staat enkele (integriteits-) fouten toe. Een basisniveau van beveiliging is noodzakelijk. Schending van integriteit kan enige (in-)directe schade toebrengen.
- **Ernstig (I2)**: Het bedrijfsproces dat gebruik maakt van deze informatie staat zeer weinig (integriteits-)fouten toe. Bescherming van integriteit is absoluut noodzakelijk. Schending van integriteit kan serieuze (in)directe schade toebrengen.
- **Desastreus (I3 met aanvullende risicoanalyse)**: Het bedrijfsproces dat gebruik maakt van deze informatie staat geen (integriteits-) fouten toe. Schending van integriteit kan (zeer) grote schade toebrengen.

2.1.3 Vertrouwelijkheid

De as vertrouwelijkheid beschrijft de bevoegdheden en de mogelijkheden tot muteren, kopiëren, toevoegen, vernietigen of kennisnemen van informatie voor een gedefinieerde groep van gerechtigden.

Het vertrouwelijkheidsniveau is in dit geval wel gekoppeld aan het BBN niveau omdat dit ook de bepalende factor is voor de BIO.

De niveaus zijn:

- **Openbaar (0)**: Alle informatie die algemeen toegankelijk is voor iedereen. Er is geen schending van vertrouwelijkheid mogelijk.
- **Intern (BBN1)**: Informatie die toegankelijk mag of moet zijn voor alle medewerkers van de eigen organisatie(s). Vertrouwelijkheid is gering. Schending van vertrouwelijkheid kan enige (in)directe schade toebrengen.
- **Vertrouwelijk (BBN2)**: Informatie die alleen toegankelijk mag zijn voor een beperkte groep gebruikers . De informatie wordt ter beschikking gesteld op basis van vertrouwen. Schending van vertrouwelijkheid kan serieuze (in)directe schade toebrengen.
- **Geheim (BBN2+)**: Dit betreft gevoelige informatie die alleen toegankelijk mag zijn voor de direct geadresseerde. Schending van vertrouwelijkheid kan zeer grote schade toebrengen. Weerstand tegen statelijke actoren noodzakelijk. Let wel: statelijke actoren kan binnen de gemeentelijke context vertaald worden naar georganiseerde misdaad en ondermijning.

2.2 Classificatieproces

1. **Identificatie van Informatie**
   De proces- en informatie eigenaren identificeren en documenteren de informatiebronnen.
2. **Classificatie van informatie**
   Voor de classificatie van de informatie voeren de proces- en informatie eigenaren de Classificatietoets in. Hiervoor wordt de handreiking BIO-Dataclassificaties gebruikt.

   De voorgestelde classificatiemethodiek geeft een snelle indicatie van het belang van de informatie die verwerkt wordt in informatiesystemen en is daarmee een basis voor de maatregelselectie of een aanvullende risicoanalyse.

   De ingevulde classificatie toets wordt bewaart in het systeemdossier van het betreffende informatiesysteem.

3. **Beschermingsmaatregelen:**
   Op basis van de ingevulde classificatietoets worden passende beschermingsmaatregelen genomen. Deze zijn beschreven in het encryptiebeled, authorisatiebeleid en wijzigingsbeleid van Sabewa Zeeland.

2.2.2 Standaard classificatie

Gegevens die niet expliciet zijn geclassificeerd, worden behandeld als gegevens van het tweede niveau: Beschikbaarheid – Belangrijk, Integriteit – Gering, Vertrouwelijkheid – Intern. Hiervoor geldt minimaal beveiligingsniveau BBN1.

2.3 Classificatie cyclus

Classificatie van informatie vindt plaats op de volgende momenten:

- Bij de start van een project of implementatie van een nieuw informatiesysteem
- Bij wijzigingen:
    - Nieuwe wet- of regelgeving
    - Meer aangesloten (keten)partners
    - Voor het zelfde doel worden meer (persoons)gegevens verzameld
    - Grote proces of systeemwijzigingen
- Periodieke Herziening (jaarlijks)

2.3.1 Periodieke herziening

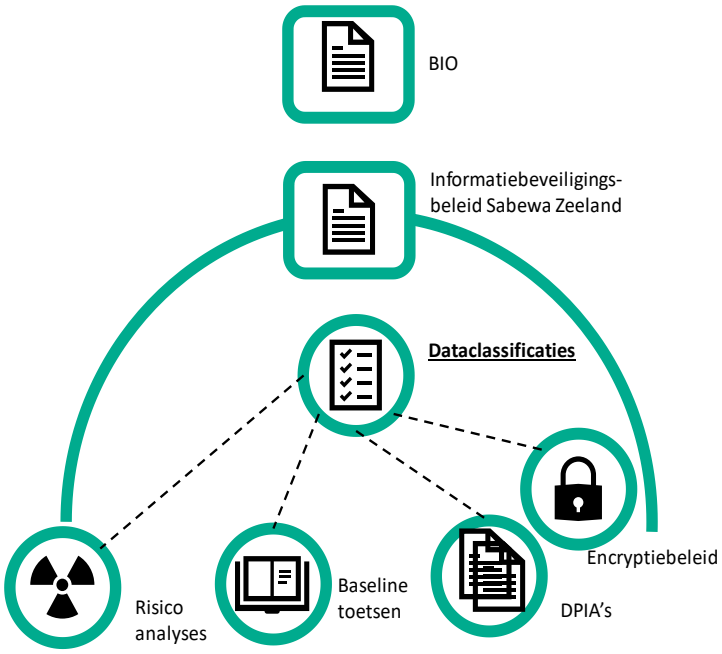
Jaarlijks vindt een evaluatie en her-classificatie van informatie plaats om ervoor te zorgen dat de classificatie up-to-date blijft. Proces- en informatie eigenaren stellen hiervoor een jaarcyclus op, zodat voor alle informatie systemen welke onder hun verantwoording vallen de jaarlijkse herziening plaatsvindt.

2.4 Communicatie en bewustwording

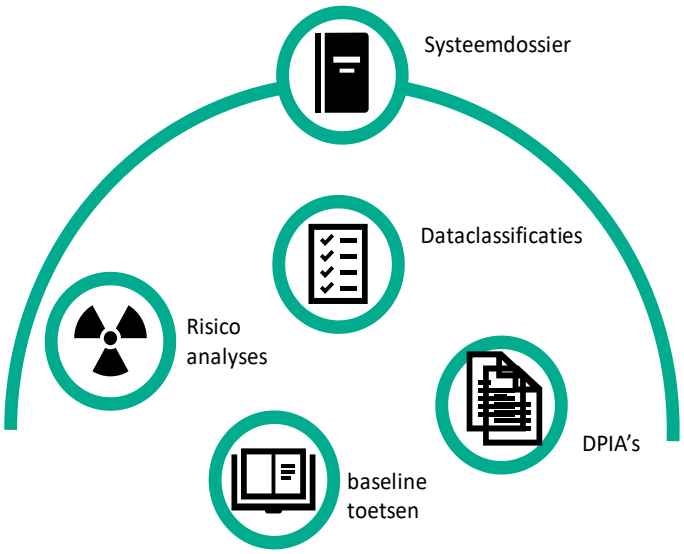
Proces- en informatie eigenaren worden getraind in het classificatieproces. Zij en de overige medewerkers worden bewust gemaakt van de implicaties. Dit is onderdeel van het cyber security awareness programma.

De classificatiecriteria en verantwoordelijkheden worden duidelijk binnen de organisatie gecommuniceerd.

2.5 Positie informatie classificatie



De classificatietoetsen zijn onderdeel van het Informatiebeveiligingsbeleid van Sabewa Zeeland. Classificatietoetsen worden opgenomen in de bijbehorende DPIA'S. De output van de classificatietoetsen bepaalt het benodigde encryptieniveau en of het nodig is een verdere risicoanalyse of baseline toets uit te voeren.



Classificatietoetsen zijn, samen met de DPIA's, Risico analyses en baselinetoetsen onderdeel van het systeemdossier van de informatie systemen binnen Sabewa Zeeland.

3. Rapportage en controle

- Het management controleert minimaal eens per kwartaal in een management rapportage de uitvoering van het beleid. Bij incidenten wordt de zwaarte van het incident bepaald op basis van het classificatieniveau.
- Continue monitoring van informatiestromen zorgt voor het tijdig identificeren van ongeautoriseerde classificatie-afwijkingen.

Aldus vastgesteld door het MT van Sabewa Zeeland op 16 januari 2024

Aldus vastgesteld door het Dagelijks Bestuur van Sabewa Zeeland op *[datum]*