Autorisatiebeleid Sabewa Zeeland

Januari 2024

A. Verhage/ S. Boudens

Versiebeheer

Versie	Datum	Door	Wijzigingen
0.1	27-03-2023	Astrid Verhage	
0.2	23-12-2023	Saskia Boudens/ Astrid Verhage	
0.3	25-01-2024	Astrid Verhage	Toevoegen autorisatiematrix
0.4	30-01-2024	Saskia Boudens/ Astrid Verhage	Definitief concept

Relatie met overige documenten

- Baseline Informatiebeveiliging Overheid (BIO)
- Strategisch Informatiebeveiligingsbeleid Sabewa Zeeland 2023 - 2027
- Beleid medewerker in- en uit dienst Sabewa Zeeland
- Beleid voor toegangsbeveiliging Sabewa Zeeland

Verwijzingen naar de Baseline Informatiebeveiliging voor de Overheid (BIO)

9.2.1 Registratie en afmelden van gebruikers

9.2.2 Gebruikers toegang verlenen

9.2.3 Beheren van speciale toegangsrechten

9.2.5 Beoordeling van toegangsrechten van gebruikers

9.2.6 Toegangsrechten intrekken of aanpassen

1. Inleiding

De beleidsuitgangspunten in dit autorisatiebeleid 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.
- Basisbeveiligingsniveau(BNN)
  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/algemeendirecteur
    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. Beheer en verlenen van toegangsrechten van gebruikers

9.2.1	**1**	**Registratie en afmelden van gebruikers** Een formele registratie- en afmeldingsprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.	Proceseigenaar Dienstenleverancier
9.2.1.1	1	Er is een sluitende formele registratie- en afmeldprocedure voor het beheren van gebruikersidentificaties.	

9.2.2	**1**	**Gebruikers toegang verlenen** Een formele gebruikerstoegangsverleningsprocedure behoort te worden geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken.	Proceseigenaar Dienstenleverancier
9.2.2.1	1	Er is uitsluitend toegang verleend tot informatiesystemen na autorisatie door een bevoegde functionaris.	
9.2.2.2	1	Op basis van een risicoafweging is bepaald waar en op welke wijze functiescheiding wordt toegepast en welke toegangsrechten worden gegeven.	

9.2.3	**1**	**Beheren van speciale toegangsrechten** Het toewijzen en gebruik van speciale toegangsrechten behoren te worden beperkt en beheerst.	Proceseigenaar Dienstenleverancier

9.2.6	**1**	**Toegangsrechten intrekken of aanpassen** De toegangsrechten van alle medewerkers en externe gebruikers voor informatie en informatie verwerkende faciliteiten behoren bij beëindiging van hun dienstverband, contract of overeenkomst te worden verwijderd, en bij wijzigingen behoren ze te worden aangepast.	Proceseigenaar Dienstenleverancier

Toegangsrechten worden verleend wanneer een medewerker in dienst komt of er een wijziging is in het dienstverband. Daarnaast kan de leidinggevende (extra) speciale toegangsrechten toewijzen aan een medewerker.

De verantwoordelijk leidinggevende geeft opdracht aan Bestuursondersteuning door middel van een ondertekend autorisatieformulier welke toegangsrechten een medewerker krijgt. Mocht een medewerker speciale toegangsrechten toegewezen krijgen, dan licht de verantwoordelijk leidinggevende dit beargumenteerd toe in het autorisatieformulier te vinden op K:\Directie\Personeel. Bestuursondersteuning geeft de betreffende autorisaties door aan de functioneel applicatiebeheerder van het team waar de medewerker in dienst treedt. De functioneel applicatiebeheerder vraagt de autorisaties aan, vult de autorisatiematrix en houdt de regie op de uitvoering hiervan.

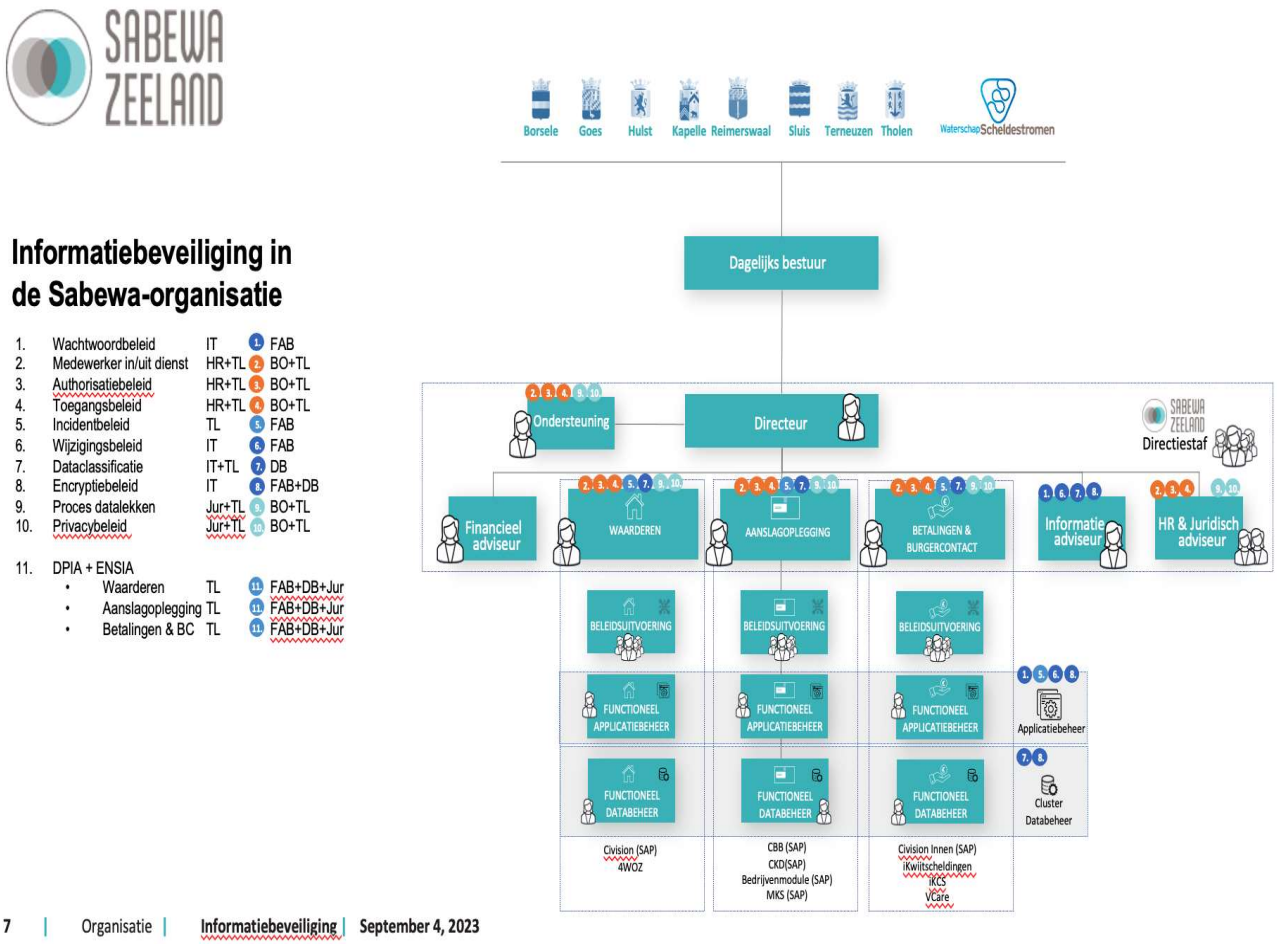
Bij uitdiensttreding van een medewerker geeft de verantwoordelijk leidinggevende opdracht aan Bestuursondersteuning om alle toegangsrechten (gebouw, apparatuur en systemen/autorisaties) van de betrokken medewerker in te trekken. De checklist “offboarding” wordt hiervoor als hulpmiddel gebruikt. Bestuursondersteuning geeft de intrekkingen van de autorisaties door aan de functioneel applicatiebeheerder van het team waar de medewerker uit dienst treedt. De functioneel applicatiebeheerder trekt de autorisaties in en verwijdert de medewerker uit de autorisatielijst van de betrokken systemen.

Autorisatiematrix
Een autorisatiematrix is voor Sabewa Zeeland een hulpmiddel om inzicht te krijgen in de toegangsrechten van medewerkers. In de autorisatiematrix is te zien wie binnen Sabewa Zeeland welke rechten heeft (raadplegen, muteren etc.). Ook zie je direct voor welke functies die rechten gelden. De matrix legt dus vast wie bij welke gegevens kan en waarom.

<u>Randvoorwaarden autorisatiematrix</u>

Onderstaande randvoorwaarden zijn van toepassing met betrekking tot autorisatiematrix:

- Er is een actueel overzicht van de bij Sabewa Zeeland in gebruik zijnde informatiesystemen beschikbaar:
  Er dient een matrix beschikbaar te zijn waarin medewerkers en organieke functies en rollen met elkaar gekoppeld worden:
- Voor elk systeem dient een actuele autorisatiematrix beschikbaar zijn waarin vastgelegd is welke autorisaties aan een specifieke functie/rol gekoppeld is;
- De autorisatiematrices worden actueel gehouden door de via de betreffende procedures aangevraagde functie of autorisatiewijzingen hierin te verwerken;
- Het toekennen van speciale bevoegdheden aan medewerkers vindt beperkt plaats.



3. Jaarlijkse beoordeling van de toegangsrechten

Control	BNN	Gedrag / procedure	Verantwoordelijke
9.2.5	**1**	**Beoordeling van toegangsrechten van gebruikers** Eigenaren van bedrijfsmiddelen behoren toegangsrechten van gebruikers regelmatig te beoordelen.	Proceseigenaar Dienstenleverancier
9.2.5.1	1	Alle uitgegeven toegangsrechten worden minimaal eenmaal per jaar beoordeeld.	
9.2.5.2	1	De opvolging van bevindingen is gedocumenteerd en wordt behandeld als beveiligingsincident.	

Het functioneel applicatiebeheer team controleert en beoordeelt minimaal eenmaal per jaar alle uitgegeven toegangsrechten van de systemen. De jaarlijkse controle is opgenomen in het intern controleplan van Sabewa Zeeland. De bevindingen worden vastgelegd in de map G:\SaBeWa Zeeland\Interne Controle. Indien de bevindingen daartoe aanleiding geven, worden vervolgacties uitgezet.

Aldus vastgesteld door het MT van Sabewa Zeeland op 30 januari 2024.

Aldus vastgesteld door het Dagelijks Bestuur van Sabewa Zeeland op 8 februari 2024.