



Adviesmemo Informatiebeveiliging & Privacy Beleid 2023

Te besluiten om

Het Informatiebeveiliging en Privacybeleid 2023 vaststellen.

Inleiding/ probleemstelling

De vigerende beleidsdocumenten zijn in 2018 vastgesteld en vragen actualisatie met behulp van de handreiking van de VNG. Tevens is op advies van de VNG het beleid voor informatiebeveiliging en privacy (IB&P) geïntegreerd in één document vanwege dat twee onderwerpen elkaar versterken voor BghU.

Beoogd effect

- Heldere ambitie te hebben voor BghU op het gebied van informatiebeveiliging en privacy;
- Dat informatiebeveiliging en voldoen aan de AVG complementair aan elkaar zijn;
- De verantwoordelijkheden helder zijn omschreven in eind- en uitvoerende verantwoordelijkheid en bijdragen aan eigenaarschap om conform het IB&P beleid daar uitvoering aan te geven.
- Dat het voorgestelde beleid bijdraagt om qua volwassenheidsniveau komende jaren te groeien als organisatie in professionaliteit en ontwikkelingsmogelijkheden biedt voor medewerkers;
- Het beleid bijdraagt om te voldoen aan de BIO en het naleven van de AVG en overige relevante wet- en regelgeving voor BghU;

Argumenten

Met behulp van dit voorgestelde beleid wil BghU een verdere professionaliseringslag maken op het gebied van Informatiebeveiliging en naleving van de AVG. Door toename van risico's op het gebied van IB&P, regelgeving en methode van technische-, organisatorische- en contractuele maatregelen is bijsturing op beleid en uitvoering met behulp van (deel)processen noodzakelijk.

Het belang van beheersing van de informatiebeveiliging en privacy ter voorkoming van reputatie- en financiële risico's neemt toe. Een actualisering van het IB&P beleid is noodzakelijk om qua volwassenheidsniveau te kunnen groeien als BghU.

Kanttekeningen

Geen

Financiën

De capaciteit voor informatiebeveiliging- en privacytaken zijn voor BghU nooit begroot en geformaliseerd. De CISO wordt al geruime tijd ingehuurd. Hierdoor krijgen we steeds meer zicht op de inhoud van functie en aanverwante taken (FG en PO). Daarnaast is de regelgeving in de loop der tijd aangescherpt en wordt reeds uitvoering gegeven aan de activiteiten vanuit de top 10 risico analyse van de BIO.

De omvang van de benodigde uitvoering is geïnventariseerd. Verwacht wordt dat we 1,2 Fte nodig hebben voor deze drie functies. De capaciteitsaanvraag wordt verwerkt in de begrotingswijziging 2024 e.v.

Het voorstel is in de vergadering van december 2023 aangehouden vanwege mogelijke vragen. Deze zijn niet meer ontvangen. Daarom is besloten om het voorstel nu opnieuw voor te leggen.

In de tussentijd is er berichtgeving dat de huidige BIO 1.04 medio 2025 wordt vervangen door de ISO27001 norm. De aanleiding hiertoe is de NIS2 regelgeving (Network and Information Security van de Europese Unie), waarin staat opgenomen de aantoonbaarheid van de genomen informatiebeveiligingsmaatregelen. Deze aanstaande wijziging heeft verzwarende consequenties voor de bijbehorende rollen. Hierdoor is de verwachting dat de ingeschatte benodigde capaciteit minimaal benodigd blijft.

Risico's

Met de voorgestelde governance heeft dit impact op huidige werkwijze van eigenaarschap, te maken werkafspraken en elkaar daar op aanspreken. Om in volwassenheidsniveau als organisatie te kunnen groeien draagt het 3-lines model bij in de rolverdeling van operationele verantwoordelijkheid en deskundige/onafhankelijke ondersteuning vanuit de 2^e lijn. De 3^e lijn zal vervolgens onafhankelijk monitoren op de realisatie van de doelstellingen van BghU.

Zienswijze (ja/nee)

nvt

Communicatie

- Na vaststelling van het beleidsdocument worden teamcoördinatoren in een bijeenkomst hierover geïnformeerd en vervolgens de vertaling naar uitvoering van het beleid;
- Medewerkers ontvangen video presentatie waarin het nieuwe IB&P beleid door de Privacy Officer en CISO wordt toegelicht.

Vervolg

Naast het IB&P Beleid 2023 is er een strategisch Informatiebeveiligingsbeleid wat is vastgesteld tot en met 2023. In maanden november en december 2023 is tijd gereserveerd om het strategische informatiebeveiligingsbeleid te herijken op basis van het strategisch beleid van BghU.

Verder zijn er beheerregels voor Informatiebeveiliging Beheer vastgesteld voor de archivering van de documenten volgens de Archiefwet 1995 en de Selectielijst 2020.

Bijlagen

1. Informatiebeveiliging & Privacy Beleid BghU 2023

Aldus vastgesteld in de bestuursvergadering van 3 april 2024,

De voorzitter,
J.C.H. Haan

De secretaris,
M. Vrisou van Eck