Wat moet er in het informatiebeveiligingsbeleid (uitwerking) 2021

In 2020 is het Informatiebeveiligingsbeleid niet herzien, hangende een evaluatie van het beleid. De manier van het evalueren van het beleid wordt ontwikkeld maar is nog niet bruikbaar. Ondertussen zijn er de nodige ontwikkelingen geweest die hun weerslag moeten vinden in het informatiebeveiligingsbeleid en zal een herziening dit jaar moeten plaatsvinden. Dit jaar betekent dat de nieuwe tekst voor de zomer af zou moeten zijn.

Uit verschillende bronnen heb ik in de loop van het jaar punten verzameld die verwerkt zouden moeten worden in het nieuwe beleid.

Het verzoek is of wij het herzien van het informatiebeveiligingsbeleid gezamenlijk op kunnen pakken op een manier die voorkomt dat een persoon onevenredig belast wordt en toch een product oplevert waar wij achter kunnen staan.

Accountant

Wachtwoordbeleid
Wachtwoordbeleid in lijn met best practices en praktijk:

Op basis van document inspectie is vastgesteld dat Nijmegen in het informatiebeveiligingsbeleid de wachtwoordvereisten heeft opgenomen, echter zijn de volgende wachtwoord configuratie instellingen (nog) niet opgenomen:
•Accountlock-out(bestaande uit het aantal minuten, aantal pogingen, en de reset van de lock-out pogingen);

•Wachtwoordhistorie;

•Minimale wachtwoord lengte.

Het verdient aanbeveling om het informatiebeveiligingsbeleid 2019 te updaten en hierbij het wachtwoordbeleid aan te scherpen naar de Deloitte good-practice richtlijnen:
•Wachtwoordhistorie: 14-24 of meer wachtwoorden (afhankelijk van normale eindgebruiker of beheeraccount);

•Minimum wachtwoordlengte: 8-14 karakters (afhankelijk van normale eindgebruiker of beheeraccount);

•Duurlock-out: 30 minuten;

•Aantal pogingen alvorens lock-out: 3;

•Reset aantal pogingen lock-out: 1440 minuten.

In aanvulling op bovenstaande wachtwoord configuratie instellingen adviseren wij om de two-factor authentication (2FA) onderdeel uit te laten maken van het ‘onderzoekwachtwoorden’ van de gemeente zodat de implementatie hiervan gerealiseerd kan worden.

MDM en nieuwe werkplek.
Wat kan wel en wat kan niet met de nieuwe inrichting. Hoe werkt de medewerker op welke locatie (gerelateerd aan corona).

Opleiding en afspraken met medewerkers
Continue opleiding en bijscholing. Overleggen bewijs. Binnen 3 maanden na in dienst de eerste module afgerond. Communicatie naar medewerker over wat van hem/haar verwacht wordt in functie.

Gebruik social media
Zie Z&I afspraken die voorstelde

Rollen en taken
iRvN, hoe houden we contact, ook bij een crisis (koppeling met crisis proces). Hoe werken we samen. Wat is de verantwoordelijkheid van de gemeente/ proceseigenaren. Zie ook de opmerkingen van de accountant over het afronden van processen.

De iRvN heeft een belangrijke rol in het realiseren van de doelstellingen in het informatiebeveiligingsbeleid. Deze rol is echter minimaal beschreven in het uitwerkingsdocument, alsmede is er een minimale beschrijving van de verantwoording van de taken en verantwoordelijkheden door de iRvN

informatiebeveiligingsbeleid organisatie breed toe te passen. Advies is om het informatiebeveiligingsbeleid te verbreiden naar het volledige aspect van informatieveiligheid in plaats de focus op de AVG.

Beschrijving vernieuwde privacy ambassadeurs, SO?

Logging en rapportage
SIEM-EWS en applicaties: wat willen we voor de verschillende soorten logging, wat willen we kunnen zien per soort (voor auditor, accountant, maar ook dreiging, inzage)

Crisisteam
Gerelateerd aan het crisisproces: taken in vredestijd, oefenen, casusbespreking

ENSIA Audit:
Suwinet RMC en DKD inlezen toevoegen.

Documentatie op orde voor de audit. Controle door het jaar heen inplannen en uitvoeren. Incidentmanagement proces gemeente intern, aansluitend op de incidentmanagement processen van de iRvN, maken en naar verwijzen.

Informatiebeveiligingsplan
Beleid + cybermanager => informatiebeveiligingsplan
Welke vorm heeft dit plan? Is hier een apart plan voor nodig. Hoe verhoudt zich dit tot het controle plan van de FG.

Evaluatie beleid (en plannen)
Proces wanneer en op basis van welke informatie. In samenhang met andere

Input vanuit direct betrokkenen
Ontwikkel I&A
AVG proof project
FG/PO/SO/CISO en privacy ambassadeurs
Evaluatie IB (als dat lukt)
Kwaliteitsmedewerkers stelsels (BRP, SUWI, BAG/BGT/BRO, DigiD)