IB-beleid 25-29:

De kernboodschappen zijn:

I. DOEL VAN ONZE INFORMATIEBEVEILIGING

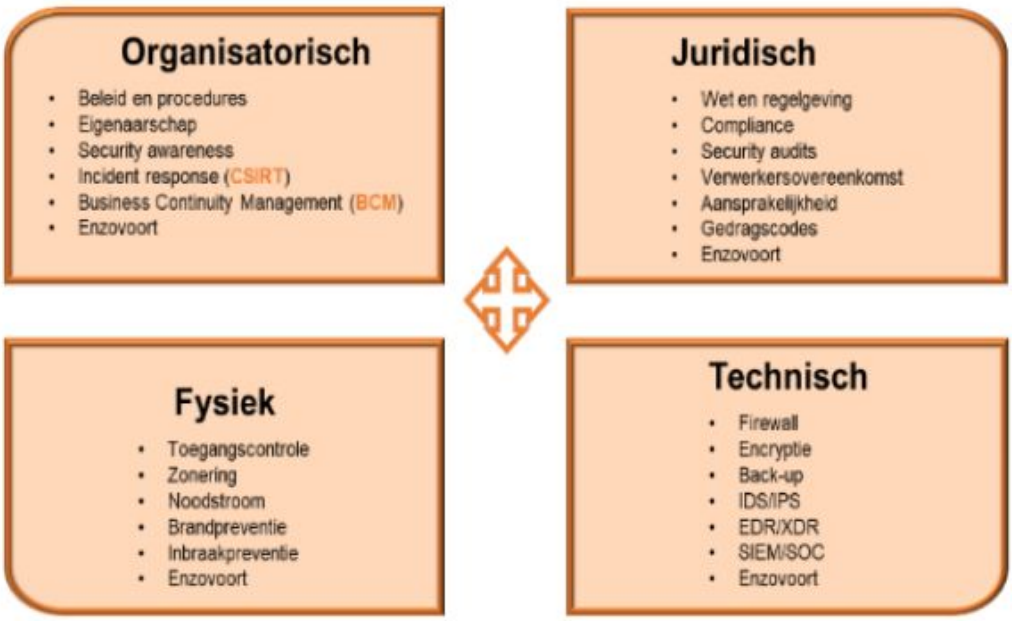
Het zorgdragen voor de beschikbaarheid, integriteit en vertrouwelijkheid van onze informatievoorziening is essentieel om de continuïteit van onze dienstverlening aan burgers, bedrijven en samenwerkingspartners te kunnen bewerkstelligen

II. DOMEINEN WAAR INFORMATIEBEVEILIGINGSMAATREGELEN WORDEN GENOMEN

Om zorg te kunnen dragen voor de beschikbaarheid, vertrouwelijkheid en integriteit van de informatievoorziening is het noodzakelijk om een samenhangend pakket van organisatorische-, juridische-, technische- en fysieke informatiebeveiligingsmaatregelen te treffen en te onderhouden.

Informatieveiligheid reikt verder dan het implementeren van technische informatiebeveiligingsmaatregelen. Het is een groot misverstand om te denken dat informatiebeveiliging iets technisch is dat centraal geregeld kan of moet worden.

Hieronder wordt schematisch weergegeven binnen welke domeinen maatregelen voor informatiebeveiliging worden getroffen en onderhouden. De beschreven maatregelen binnen deze domeinen zijn illustratief en niet limitatief.



III. Het IB-beleid 25-29 vormt de kapstok voor (de uitwerking van) aanvullend onderliggend informatiebeveiligingsbeleid, tactische en operationele richtlijnen, processen, procedures en maatregelen.

De daaruit voortkomende prioriteiten en werkzaamheden worden uitgewerkt in het jaarlijks op te stellen “Informatiebeveiligingsplan Drechtsteden 202X”

IV. VISIE OP ONZE INFORMATIEVEILIGHEID

Er is voldoende aansluiting met toekomstige wettelijke ontwikkelingen qua NIS2 en BIO.

Governance nog wel goed te regelen in de praktijk!!!

Het primaire uitgangspunt voor onze informatieveiligheid is en blijft risicomanagement. Dat vereist een integrale aanpak, goed opdrachtgeverschap, onderlinge samenwerking en risicobewustzijn, waarbij ieder organisatieonderdeel is betrokken.

De nadruk komt hierdoor te liggen op de governance rondom onze informatieveiligheid. Ook de BIO en de Network and Information Security directive3 (NIS2-richtlijn) sluiten hierop aan door de verantwoordelijkheid voor informatiebeveiliging in de organisatie(s) nadrukkelijk neer te leggen bij het bestuur en de proceseigenaren.

Deze verantwoordelijkheid brengt met zich mee dat de proceseigenaren de risico’s op het niveau van de werkprocessen/informatiesystemen in beeld hebben met als doel het implementeren en onderhouden van passende organisatorische-, juridische-, technische- en fysieke informatiebeveiligingsmaatregelen.

Overblijvende (rest)risico’s worden op het juiste bestuurs- / managementniveau geaccepteerd. Meer specifiek:

1. Relevante Europese, landelijke, sectorale wet- en regelgeving en specifieke normenkaders zijn, voor zover van toepassing op de deelnemer(s) aan het samenwerkingsverband Drechtsteden, altijd leidend. Denk bij wet- en regelgeving (niet limitatief) aan: de Baseline Informatiebeveiliging Overheid (BIO), de NEN7510, de Network and Information Security directive (NIS2-richtlijn), de Algemene Verordening Gegevensbescherming (AVG), de Wet Basisregistratie Personen (BRP), de Wet Structuur Uitvoeringsorganisatie Werk en Inkomen (SUWI), de archiefwet, enzovoort;

2. We zijn een betrouwbare partij voor onze burgers, bedrijven en samenwerkingspartners en gaan zorgvuldig en veilig om met hun én onze gegevens. We vinden een optimum tussen investeringen in informatiebeveiligingsmaatregelen en het weerstandsvermogen, zonder de organisatie(s) te verlammen met het implementeren en borgen van maatregelen om alle risico’s tot “naderend tot nul” te reduceren. Per slot van rekening, een 100% waterdichte informatiebeveiliging bestaat niet;

3. De te treffen en onderhouden organisatorische-, juridische-, technische- en fysieke informatiebeveiligingsmaatregelen zijn altijd op een risicoafweging gebaseerd en worden proportioneel getroffen.

V. Rol proceseigenaar binnen samenwerkingsverband

Binnen het samenwerkingsverband Drechtsteden is een groot deel van de ICT systemen, de ICT infrastructuur evenals het beheer regionaal (dienstenleverancier) ondergebracht. Desondanks is er ook een set lokaal te implementeren BIO maatregelen aanwezig. Op de volgende wijze geven we binnen het samenwerkingsverband Drechtsteden invulling aan de rol en verantwoordelijkheden van de proceseigenaar uit de BIO. De rol van proceseigenaar wordt onderverdeeld in een regionale systeemeigenaar (bij de dienstenleverancier) en een lokale procesverantwoordelijke (lijnmanager).

Elk hebben ze hun eigen BIO aandachtsgebieden en verantwoordelijkheden:

1. De regionale systeemeigenaar is verantwoordelijk voor de implementatie en borging van de regionale BIO beheersmaatregelen;

2. De lokale procesverantwoordelijke (lijnmanager) is verantwoordelijk voor:

a. Het toezicht houden op de naleving van de implementatie en borging van de regionale BIO beheersmaatregelen;

b. De implementatie en borging van lokale BIO beheersmaatregelen

VI. Beleidsuitgangspunten

Er worden een 11 – tal punten aangegeven waaraan voldaan moet worden bij het treffen en onderhouden van maatregelen voor de borging van de informatieveiligheid.

O.a. zijn dit:

1. relevante Europese, landelijke en sectorale wet- en regelgeving

2. BIO en IBG (informatiebeveiligingsdienst)

3. DPIA, BBN 2 etc.

4.risico-acceptatie

5. nadere uitwerking strategisch beleid naar tactisch beleid, plannen, richtlijnen etc.

6. bescherming devices

7. eigen verantwoordelijkheid medewerkers

8. algemeen directeur, lijnmanagement, CISO, lokale security officers bevorderen strategische IB-beleid 25-29 door bewustwording, communicatie etc.

VII. INRICHTING IB ORGANISATIE DRECHTSTEDEN CONFORM HET THREE LINES MODEL

De eerste lijn, het lijnmanagement (proceseigenaar), is verantwoordelijk voor het zorg dragen voor de informatiebeveiliging en privacybescherming binnen de eigen processen.

De tweede lijn (CISO, regionale ISO, lokale adviseur informatiebeveiliging, regionale ENSIA regisseur en de lokale ENSIA coördinator) ondersteunt, adviseert, coördineert en bewaakt of het lijnmanagement (proceseigenaar) zijn/haar verantwoordelijkheden ook daadwerkelijk neemt.

De derde lijn bestaat uit een interne auditor en een (externe) register EDP-auditor. De derde lijn geeft onafhankelijke en objectieve adviezen (interne auditor) en Assurance (register EDP-auditor) over de toereikendheid en effectiviteit van de informatiebeveiliging en het bijbehorende risicomanagement.

VIII. Ensia

Dat betekent dat jaarlijks door de gemeentesecretaris een gemeentelijke (lokale) ENSIA-coördinator wordt aangewezen. Deze zorgt ervoor dat de informatie die nodig is voor het beantwoorden van vragen binnen ENSIA wordt opgehaald bij de verantwoordelijke proceseigenaren (lijnmanager). De proceseigenaren (lijnmanagers) leveren alle informatie die nodig is voor het invullen van de jaarlijkse ENSIA-vragenlijsten tijdig aan. Binnen het samenwerkingsverband Drechtsteden wordt het proces regionaal gecoördineerd door een ENSIA regisseur.

IX. De 10 bestuurlijke principes voor informatiebeveiliging (behorende bij BIO)

1. Bestuurders bevorderen een veilige cultuur
2. Informatieveiligheid is van iedereen
3. Informatieveiligheid is risicomanagement
4. Risicomanagement is onderdeel van de besluitvorming
5. Informatiebeveiliging behoeft aandacht in (keten)samenwerking
6. Informatiebeveiliging is een proces
7. Informatiebeveiliging kost geld
8. Onzekerheid dient te worden ingecalculeerd
9. Verbetering komt voort uit leveren en ervaring
10. Het bestuur controleert en evalueert