

Bijlage 2b - Technische en organisatorische maatregelen behorende bij IUC25-711

Technische en organisatorische maatregelen waaronder technische en organisatorische maatregelen om de beveiliging van de gegevens te waarborgen.

Beschrijving van de technische en organisatorische maatregelen die de Opdrachtnemer heeft/hebben genomen (met inbegrip van eventuele relevante certificeringen) om een passend beveiligingsniveau te waarborgen, rekening houdend met de aard, reikwijdte, context en doeleinden van de verwerking en met de risico's voor de rechten en vrijheden van natuurlijke personen.

Beveiliging

BIO maatregelen:

Technische maatregelen

- Cryptografische toepassingen voldoen aan passende standaarden.
- Cryptografische beheersmaatregelen moeten expliciet aansluiten bij de standaarden op de 'pas toe of leg uit'-lijst van het Forum.
- Voor de beveiliging van elektronische (e-mail)berichten gelden de vastgestelde open standaarden tegen phishing en af luisteren op de 'pas toe of leg uit'-lijst van het Forum. Voor beveiliging van websiteverkeer gelden de open standaarden tegen af luisteren op de 'pas toe of leg uit'-lijst van het Forum.

Beleid voor toegangsbeveiliging

- Een beleid voor toegangsbeveiliging behoort te worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfs- en informatiebeveiligingseisen.
- Toegang tot netwerken en netwerkdiensten
Gebruikers behoren alleen toegang te krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn.

Informatiebeveiliging

BIO maatregelen:

Beleid

- Er is een informatiebeveiligingsbeleid opgesteld door de organisatie. Dit beleid is vastgesteld door de leiding van de organisatie en bevat tenminste de volgende punten:
 - a) de strategische uitgangspunten en randvoorwaarden die de organisatie hanteert voor informatiebeveiliging en in het bijzonder de inbedding in, en afstemming op het algemene beveiligingsbeleid en het informatievoorzieningsbeleid;
 - b) de organisatie van de informatiebeveiligingsfunctie, waaronder verantwoordelijkheden, taken en bevoegdheden;
 - c) de toewijzing van de verantwoordelijkheden voor ketens van informatiesystemen aan lijnmanagers;
 - d) de gemeenschappelijke betrouwbaarheidseisen en normen die op de organisatie van toepassing zijn;
 - e) de frequentie waarmee het informatiebeveiligingsbeleid wordt geëvalueerd;
 - f) de bevordering van het beveiligingsbewustzijn.Het informatiebeveiligingsbeleid wordt periodiek en in aansluiting bij de (bestaande) bestuurs- en P&C-cycli en externe ontwikkelingen beoordeeld en zo nodig bijgesteld.

Informatiebeveiligingscontinuïteit plannen

- De organisatie behoort haar eisen voor informatiebeveiliging en voor de continuïteit van het informatiebeveiligingsbeheer in ongunstige situaties, bijv. een crisis of een ramp, vast te stellen.
- Er is een back-up beleid waarin de eisen voor het bewaren en beschermen zijn gedefinieerd en vastgesteld
- Het back-up proces voorziet in opslag van de back-up op een locatie, waarbij een incident op de ene locatie niet kan leiden tot schade op de andere.

Informatie deling

- In inkoopcontracten wordt expliciet de mogelijkheid van een externe audit opgenomen waarmee de betrouwbaarheid van de geleverde dienst kan worden getoetst.

- Rapportage van zwakke plekken in de informatiebeveiliging. Van medewerkers en contractanten die gebruikmaken van de informatiesystemen en -diensten van de organisatie behoort te worden geëist dat zij de in systemen of diensten waargenomen of vermeende zwakke plekken in de informatiebeveiliging registreren en rapporteren.
- De analyses van de beveiligingsincidenten worden gedeeld met de relevante partners om herhaling en toekomstige incidenten te voorkomen. In geval van een (vermoed) informatiebeveiligingsincident is de bewaartermijn van de gelogde incidentinformatie minimaal drie jaar. Persoonsgegevens worden hiervan uitgesloten. Hiervoor geldt maximaal een bewaartermijn van 1 jaar
- Leveranciers moeten hun keten van toeleveranciers bekendmaken en transparant zijn over de maatregelen die zij genomen hebben om de aan hen opgelegde eisen ook door te vertalen naar hun toeleveranciers.

Informatiebeveiliging incidenten

- Er is een meldprocedure waarin de taken en verantwoordelijkheden van het meldloket staan beschreven.
- De proceseigenaar is verantwoordelijk voor het oplossen van informatiebeveiligingsincidenten.
- De proceseigenaar rapporteert maandelijks de opvolging van informatiebeveiligingsincidenten aan de eindverantwoordelijke voor de bedrijfsvoering.
- In de procedure voor informatiebeveiligingsincidenten is er een verwijzing gemaakt naar de procedure voor crisisbeheersing.
- Informatiebeveiligingsincidenten worden afgedaan via het incidentbeheerproces.
- In het incidentbeheerproces is opgenomen dat incidenten indien relevant gemeld worden bij de in wet- en regelgeving aangewezen toezichthouders.
- Informatiebeveiligingsincidenten worden geanalyseerd om achterliggende oorzaken vast te stellen, verbeteringen te realiseren, om zo toekomstige incidenten te voorkomen.
- Respons op informatiebeveiligingsincidenten. Op informatiebeveiligingsincidenten behoort te worden gereageerd in overeenstemming met de gedocumenteerde procedures.
- Beveiligingsincidenten worden geanalyseerd met als doel te leren en toekomstige beveiligingsincidenten te voorkomen.

Informatiebeveiliging in relatie tot personeel

- Arbeidsvoorwaarden. De contractuele overeenkomst met medewerkers en contractanten behoort hun verantwoordelijkheden voor informatiebeveiliging en die van de organisatie te vermelden.