Europese aanbesteding Communicatieverbindingen

Bijlage 16 PvE.02
Informatiebeveiligingsbeleid

Skal BIOCONTROLE

1 Doelstelling

Dit beleid beschrijft hoe Skal Biocontrole de vertrouwelijkheid, integriteit en beschikbaarheid van haar informatie en systemen borgt. Het beleid is van toepassing op alle medewerkers, externen, systemen, applicaties en cloudomgevingen die onder verantwoordelijkheid van Skal Biocontrole vallen. Skal Biocontrole handelt binnen het normenkader van de Baseline Informatiebeveiliging Overheid (BIO), de Algemene Verordening Gegevensbescherming (AVG), de NIS2-richtlijn en de best practices van ISO 27001/27002. Met als doelstelling, zorgen voor betrouwbare/veilige informatievoorziening en bescherming van persoonsgegevens tegen verlies of onbevoegde toegang.

2 Governance en verantwoordelijkheden

Directie	Eindverantwoordelijk voor het informatiebeveiligingsbeleid en stelt de benodigde middelen beschikbaar.
Chief Information Security Officer (CISO)	Verantwoordelijk voor het beheer, de uitvoering en de periodieke evaluatie van het beleid.
Security Officer (SO)	Ondersteunt de CISO, adviseert over risico's en bewaakt de naleving.
Privacy Officer (PO)	Ziet toe op naleving van de AVG en coördineert datalekmeldingen.
ICT-organisatie	Voert de technische beveiligingsmaatregelen uit, registreert incidenten en verzorgt hersteltaken.
Leidinggevenden	Zijn verantwoordelijk voor het juist autoriseren van medewerkers en het melden van afwijkingen of incidenten.
Alle medewerkers	Zijn verplicht zorgvuldig om te gaan met informatie en beveiligingsincidenten direct te melden.

3 Risicomanagement

Skal Biocontrole voert periodiek een risicoanalyse uit om bedreigingen, kwetsbaarheden en gevolgen voor bedrijfsprocessen te identificeren. De resultaten worden vastgelegd in een risicoregister en beoordeeld door de CISO. Op basis hiervan worden passende maatregelen getroffen of risico's formeel geaccepteerd. Bij significante veranderingen of incidenten wordt een tussentijdse evaluatie uitgevoerd. De directie wordt periodiek geïnformeerd over de belangrijkste risico's en genomen beheersmaatregelen.

4 Beheer van informatie en middelen

Alle informatiemiddelen worden geregistreerd in een Configuration Management Database (CMDB) en zijn voorzien van een aangewezen eigenaar. Onder informatiemiddelen worden in dit kader onder meer verstaan: systemen, applicaties, data(verzamelingen), infrastructuurcomponenten en overige bedrijfskritische middelen. Informatie wordt geclassificeerd als openbaar, intern, vertrouwelijk of zeer vertrouwelijk, met bijpassende beveiligingsmaatregelen, in lijn met de Baseline Informatiebeveiliging Overheid (BIO). Back-ups worden dagelijks uitgevoerd, dertig dagen bewaard en gerepliceerd naar een externe locatie om dataverlies te voorkomen. De hersteltijd (RTO) voor kritieke processen is maximaal 48 uur, de

maximale dataverliesduur (RPO) bedraagt 24 uur. Het testen van bijbehorende herstelprocedures vinden periodiek plaats.
Apparatuur met opslagmedia wordt bij buitengebruikstelling of defect door de beheersorganisatie veilig gewist of fysiek vernietigd. Hergebruik buiten de organisatie is alleen toegestaan na volledige gegevensverwijdering via Secure Erase of een gelijkwaardige methode.

5 Toegangsbeheer

a) Toegang tot systemen wordt verleend volgens het need-to-know-principe en least-privilege-principe gebaseerd op functierollen.
b) Autorisaties worden verstrekt na goedkeuring door de leidinggevende en geregistreerd in de autorisatiematrix.
c) De Security Officer voert minimaal periodiek een review uit op alle rechten. Bij indiensttreding, functiewijziging of uitdiensttreding worden autorisaties direct aangepast of beëindigd.
d) Authenticatie vindt plaats met multi-factor authenticatie (MFA) waar dit technisch mogelijk is.
e) Het wachtwoordbeleid vereist sterke, unieke wachtwoorden met een minimale lengte van twaalf tekens en periodieke vernieuwing.
f) Gebruik van een wachtwoordmanager wordt aangemoedigd om hergebruik te voorkomen.

6 Technische/organisatorische beveiliging

a) Systemen en applicaties worden onderhouden en tijdig voorzien van updates en beveiligingspatches.
b) Netwerken zijn gesegmenteerd en beschermd met firewalls en monitoring door een Security Operations Center (SOC).
c) De kroonjuwelen van Skal Biocontrole, essentieel voor de bedrijfsvoering, worden 24/7 gemonitord door het Security Operations Center (SOC). Alle Microsoft-licenties (gebruikers) worden 24/7 gemonitord door het Security Operations Center (SOC).
d) Alle loggegevens van kritieke systemen worden centraal opgeslagen en minimaal twaalf maanden bewaard voor analyse en auditing.
e) Versleuteling wordt toegepast op alle vertrouwelijke gegevens, zowel tijdens opslag als tijdens overdracht.
f) Wijzigingen in systemen worden uitgevoerd via een gecontroleerd wijzigingsproces, inclusief goedkeuring en terugvalplan.
g) Kwetsbaarheden worden periodiek opgespoord via scans en penetratietesten, waarna verbetermaatregelen worden ingevoerd.
h) Medewerkers ontvangen structureel training en bewustwordingssessies over informatiebeveiliging en privacy.
i) Skal Biocontrole heeft een gebruikersovereenkomst om de privacy en veiligheid van gegevens te waarborgen, deze bestaat uit: Non-Disclosure Agreement (NDA), verwerkingsovereenkomst en Verklaring Omtrent het Gedrag (VOG).
j) Skal Biocontrole hanteert het redundantieprincipe op het gebied van informatiebeveiliging.
k) Skal Biocontrole beschikt over een uitwijkprocedure voor de private Cloud omgeving.

7 Back-up & Recovery

Skal Biocontrole stelt de volgende eisen aan back-up en recovery:

ID	Requirement	Type	MoSCoW	Rationele
R.0	Skal Biocontrole hanteert het Security by Design-principe.	Principieel	Must have	De gangbare principes rondom 'security by design' zijn uitgangspunt voor de ontwikkeling van software en systemen.
R.1	Skal Biocontrole hanteert een Recovery Time Objective (RTO) van maximaal 48 uur.	Principieel	Must have	Hersteltijd in geval van incidenten is maximaal 48 uur
R.2	Skal Biocontrole hanteert een Recovery Point Objective (RPO) van maximaal 24 uur.	Principieel	Must have	Dataverlies bedraagt maximaal 24 uur.
R.3	Er dient iedere 24 uur een volledige back-up uitgevoerd te worden.	Organisatorisch	Must have	
R.4	Skal Biocontrole hanteert een retentieperiode van 30 dagen voor de gemaakte back-up.	Organisatorisch	Must have	
R.5	Skal dient een back-up en herstelplan te ontvangen.	Organisatorisch	Must have	Een stappenplan waarin helder wordt toegelicht hoe het herstelproces en de implementatie van back-up worden uitgevoerd.
R.6	Skal Biocontrole dient het back-up en herstelplan jaarlijks te testen.	Organisatorisch	Must have	Back-up van informatie, software en systemen behoren te worden bewaard en regelmatig te worden getest overeenkomstig het overeengekomen onderwerp specifieke beleid inzake back-up.
R.7	Skal Biocontrole hanteert het principe van redundantie.	Principieel	Must have	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. Skal Biocontrole secundaire cloud provider is Previder.
R.8	Skal Biocontrole dient een unmutable back-up te hebben.	Organisatorisch	Must have	Zorg dat ten minste één back-up niet online benaderbaar is en beschermd wordt tegen veranderingen.

8 Incident beheer

Alle beveiligingsincidenten, storingen en datalekken worden direct geregistreerd in het incidentmanagementsysteem. Wanneer nodig zal de CISO het Incident Response Plan (IRP) activeren, waarin rollen, communicatielijnen en draaiboeken zijn vastgelegd. Datalekken met mogelijke impact op persoonsgegevens worden binnen 72 uur gemeld aan de Autoriteit Persoonsgegevens door de Privacy Officer. Mocht herstel van systemen nodig zijn dan: op basis van gevalideerde back-ups, de root-cause wordt vastgesteld en de bijbehorende structurele maatregelen worden vastgelegd.

9 Leveranciers

Bij uitbesteding van ICT-diensten worden beveiligingseisen opgenomen in contracten en service-level-afspraken. Leveranciers dienen aantoonbaar te voldoen aan relevante normen op het gebied van informatiebeveiliging, waaronder minimaal ISO 27001 of een aantoonbaar gelijkwaardig normenkader. Indien van toepassing wordt daarnaast aansluiting verwacht op sectorspecifieke of wettelijke kaders, zoals de BIO en NIS2. Skal Biocontrole controleert periodiek de naleving hiervan via rapportages, audits of/en penetratietesten. Back-up, herstel en beschikbaarheid van omgevingen worden geborgd via formele afspraken over RPO en RTO.

10 Privacy

a) Persoonsgegevens worden uitsluitend verwerkt voor gerechtvaardigde doeleinden en in overeenstemming met de AVG.
b) Nieuwe of gewijzigde verwerkingen worden vooraf door Skal Biocontrole getoetst op risico's door middel van een Data Protection Impact Assessment (DPIA), onder regie van de Privacy Officer.
c) Verwerkersovereenkomsten worden afgesloten met alle externe partijen die persoonsgegevens verwerken.
d) Gegevens worden niet langer bewaard dan noodzakelijk en worden veilig vernietigd na afloop van de bewaartermijn.
e) Betrokkenen kunnen gebruikmaken van hun rechten op inzage, correctie en verwijdering via de Privacy Officer.

11 Onderhoud

De werking van dit beleid wordt periodiek geëvalueerd binnen het Information Security Management System (ISMS). Interne audits en managementreviews beoordelen de effectiviteit van maatregelen en leiden tot een verbeterplan waar nodig. Afwijkingen op het beleid zijn slechts toegestaan na goedkeuring door de CISO en worden tijdelijk vastgelegd met een einddatum. Het beleid wordt herzien bij significante organisatorische of wettelijke wijzigingen en minimaal één keer per jaar ter goedkeuring voorgelegd aan de directie.

Einde document.