

Doelstellingen BIO

Nummer Onderwerp	Onderwerp	Nummer Hoofdstuk	Hoofdstuk
6	Organiseren van informatiebeveiliging	6.1	Interne organisatie
		6.2	Mobiele apparatuur en telewerken
7	Veilig personeel	7.1	Voorafgaand aan het dienstverband
		7.2	Tijdens het dienstverband
		7.3	Beëindiging en wijziging van dienstverband
8	Beheer van bedrijfsmiddelen	8.1	Verantwoordelijkheid voor bedrijfsmiddelen
		8.2	Informatieclassificatie
		8.3	Behandelen van media
9	Toegangsbeveiliging	9.1	Bedrijfseisen voor toegangsbeveiliging
		9.2	Beheer van toegangsrechten van gebruikers
		9.3	Verantwoordelijkheden van gebruikers
		9.4	Toegangsbeveiliging van systeem en toepassing
10	Cryptografie	10.1	Cryptografische beheersmaatregelen
11	Fysieke beveiliging en beveiliging van de omgeving	11.1	Beveiligde gebieden
		11.2	Apparatuur
12	Beveiliging bedrijfsvoering	12.1	Bedieningsprocedures en verantwoordelijkheden
		12.2	Bescherming tegen malware
		12.3	Back-up
		12.4	Verslaglegging en monitoren
		12.5	Beheersing van operationele software
		12.6	Beheer van technische kwetsbaarheden
		12.7	Overwegingen betreffende audits van informatiesystemen

13	Communicatiebeveiliging	13.1	Beheer van netwerkbeveiliging
		13.2	Informatietransport
14	Acquisitie, ontwikkeling en onderhoud van informatiesystemen	14.1	Beveiligingseisen voor informatiesystemen
		14.2	Beveiliging in ontwikkelings- en ondersteunende processen
		14.3	Testgegevens
15	Leveranciersrelaties	15.1	Informatiebeveiliging in leveranciersrelaties
		15.2	Beheer van dienstverlening van leveranciers
16	Beheer van informatiebeveiligingsincidenten	16.1	Beheer van informatiebeveiligingsincidenten en -verbeteringen
17	Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer	17.1	Informatiebeveiligingscontinuïteit
		17.2	Redundante componenten
18	Naleving	18.1	Naleving van wettelijke en contractuele eisen
		18.2	Informatiebeveiligingsbeoordelingen

Doelstelling
Een beheerkader vaststellen om de implementatie en uitvoering van de informatiebeveiliging binnen de organisatie te initiëren en te beheersen.
Het waarborgen van de veiligheid van telewerken en het gebruik van mobiele apparatuur.
Waarborgen dat medewerkers en contractanten hun verantwoordelijkheden begrijpen en geschikt zijn voor de rollen waarvoor zij in aanmerking komen.
Ervoor zorgen dat medewerkers en contractanten zich bewust zijn van hun verantwoordelijkheden op het gebied van informatiebeveiliging en deze nakomen.
Het beschermen van de belangen van de organisatie als onderdeel van de wijzigings- of beëindigingsprocedure van het dienstverband.
Bedrijfsmiddelen van de organisatie identificeren en passende verantwoordelijkheden ter bescherming definiëren.
Bewerkstelligen dat informatie een passend beschermingsniveau krijgt dat in overeenstemming is met het belang ervan voor de organisatie.
Onbevoegde openbaarmaking, wijziging, verwijdering of vernietiging van informatie die op media is opgeslagen voorkomen.
Toegang tot informatie en informatie verwerkende faciliteiten beperken.
Toegang voor bevoegde gebruikers bewerkstelligen en onbevoegde toegang tot systemen en diensten voorkomen.
Gebruikers verantwoordelijk maken voor het beschermen van hun authenticatie-informatie.
Onbevoegde toegang tot systemen en toepassingen voorkomen.
Zorgen voor correct en doeltreffend gebruik van cryptografie om de vertrouwelijkheid, authenticiteit en/of integriteit van informatie te beschermen.
Onbevoegde fysieke toegang tot, schade aan en interferentie met informatie en informatieverwerkende faciliteiten van de organisatie voorkomen.
Verlies, schade, diefstal of compromittering van bedrijfsmiddelen en onderbreking van de bedrijfsvoering van de organisatie voorkomen.
Correcte en veilige bediening van informatie verwerkende faciliteiten waarborgen.
Waarborgen dat informatie en informatie verwerkende faciliteiten beschermd zijn tegen malware.
Beschermen tegen het verlies van gegevens.
Gebeurtenissen vastleggen en bewijs verzamelen.
De integriteit van operationele systemen waarborgen.
Benutting van technische kwetsbaarheden voorkomen.
De impact van auditactiviteiten op uitvoeringssystemen zo gering mogelijk maken.

De bescherming van informatie in netwerken en de ondersteunende informatie verwerkende faciliteiten waarborgen.
Handhaven van de beveiliging van informatie die wordt uitgewisseld binnen een organisatie en met een externe entiteit.
Waarborgen dat informatiebeveiliging integraal deel uitmaakt van informatiesystemen in de gehele levenscyclus. Hiertoe behoren ook de eisen voor informatiesystemen die diensten verlenen via openbare netwerken.
Bewerkstelligen dat informatiebeveiliging wordt ontworpen en geïmplementeerd binnen de ontwikkelingslevenscyclus van informatiesystemen.
Bescherming waarborgen van gegevens die voor het testen zijn gebruikt.
De bescherming waarborgen van bedrijfsmiddelen van de organisatie die toegankelijk zijn voor leveranciers.
Een overeengekomen niveau van informatiebeveiliging en dienstverlening in overeenstemming met de leveranciersovereenkomsten handhaven.
Een consistente en doeltreffende aanpak bewerkstelligen van het beheer van informatiebeveiligingsincidenten, met inbegrip van communicatie over beveiligingsgebeurtenissen en zwakke plekken in de beveiliging.
Informatiebeveiligingscontinuïteit behoort te worden ingebed in de systemen van het bedrijfscontinuïteitsbeheer van de organisatie.
Beschikbaarheid van informatie verwerkende faciliteiten bewerkstelligen.
Voorkomen van schendingen van wettelijke, statutaire, regelgevende of contractuele verplichtingen betreffende informatiebeveiliging en beveiligingseisen.
Verzekeren dat informatiebeveiliging wordt geïmplementeerd en uitgevoerd in overeenstemming met de beleidsregels en procedures van de organisatie.