Bexter B.V.

Versie: 31 maart 2023 Norm: ISO 27001:2017

	Beheersaspect	van Toepassing	Geïmplementeerd	Rechtvaardiging			
		Ja / Nee	Ja / Deels / Niet	WE	CE	BR	RA
A.5	Informatiebeveiligingsbeleid						
A.5.1	Aansturing door de directie van de informatiebeveiliging						
	Doelstelling: Het verschaffen van directieaansturing van en -steun voor informatiebeveiliging in overeenstemming met bedrijfseisen en relevante wet- en regelgeving.						
A.5.1.1	Beleidsregels voor informatiebeveiliging	Ja	Ja			V	V
A.5.1.2	Beoordelen van het informatiebeveiligingsbeleid	Ja	Ja			V	V
A.6	Organiseren van informatiebeveiliging						
A.6.1	Interne organisatie						
	Doelstelling: Een beheerkader vaststellen om de implementatie en uitvoering van de informatiebeveiliging binnen de organisatie te initiëren en te beheersen.						
A.6.1.1	Rollen en verantwoordelijkheden bij informatiebeveiliging	Ja	Ja			V	V
A.6.1.2	Scheiding van taken	Ja	Ja			V	V
A.6.1.3	Contact met overheidsinstanties	Ja	Ja	V			V
A.6.1.4	Contact met speciale belangengroepen	Ja	Ja			V	V
A.6.1.5	Informatiebeveiliging in projectbeheer	Ja	Ja		V		V
A.6.2	Mobiele apparatuur en telewerken						
	Doelstelling: Het waarborgen van de veiligheid van telewerken en het gebruik van mobiele apparatuur.						
A.6.2.1	Beleid voor mobiele apparatuur	Ja	Ja			V	V
A.6.2.2	Telewerken	Ja	Ja			V	V
A.7	Veilig personeel						
A.7.1	Voorafgaand aan het dienstverband						
	Doelstelling: Waarborgen dat medewerkers en contractanten hun verantwoordelijkheden begrijpen en geschikt zijn voor de functies waarvoor zij in aanmerking komen.						
A.7.1.1	Screening	Ja	Ja				V
A.7.1.2	Arbeidsvoorwaarden	Ja	Ja				V
A.7.2	Tijdens het dienstverband						
	Doelstelling: Ervoor zorgen dat medewerkers en contractanten zich bewust zijn van hun verantwoordelijkheden op het gebied van informatiebeveiliging en deze nakomen.						
A.7.2.1	Directieverantwoordelijkheden	Ja	Ja			V	
A.7.2.2	Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	Ja	Ja			V	V
A.7.2.3	Disciplinaire procedure	Ja	Ja			V	V
A.7.3	Beëindiging en wijziging van dienstverband						
	Doelstelling: Het beschermen van de belangen van de organisatie als onderdeel van de wijzigings- of beëindigingsprocedure van het dienstverband.						
A.7.3.1	Beëindiging of wijziging van verantwoordelijkheden van het dienstverband	Ja	Ja			V	V
A.8	Beheer van bedrijfsmiddelen						
A.8.1	Verantwoordelijkheid voor bedrijfsmiddelen						
	Doelstelling: Bedrijfsmiddelen van de organisatie identificeren en passende verantwoordelijkheden ter bescherming definiëren.						
A.8.1.1	Inventariseren van bedrijfsmiddelen	Ja	Ja			V	V
A.8.1.2	Eigendom van bedrijfsmiddelen	Ja	Ja			V	V
A.8.1.3	Aanvaardbaar gebruik van bedrijfsmiddelen	Ja	Ja			V	V
A.8.1.4	Teruggeven van bedrijfsmiddelen	Ja	Ja			V	V
A.8.2	Informatieclassificatie						
	Doelstelling: Bewerkstelligen dat informatie een passend beschermingsniveau krijgt dat in overeenstemming is met het belang ervan voor de organisatie.						
A.8.2.1	Classificatie van informatie	Ja	Ja			V	V
A.8.2.2	Informatie labelen	Ja	Ja			V	V
A.8.2.3	Behandelen van bedrijfsmiddelen	Ja	Ja			V	V
A.8.3	Behandelen van media						
	Doelstelling: Onbevoegde openbaarmaking, wijziging, verwijdering of vernietiging van informatie die op media is opgeslagen voorkomen.						
A.8.3.1	Beheer van verwijderbare media	Ja	Ja			V	V
A.8.3.2	Verwijderen van media	Ja	Ja			V	V
A.8.3.3	Media fysiek overdragen	Nee	**Informatie wordt niet fysiek overgedragen, paperless beleid**				
A.9	Toegangsbeveiliging						
A.9.1	Bedrijfseisen voor toegangsbeveiliging						
	Doelstelling: Toegang tot informatie en informatieverwerkende faciliteiten beperken.						
A.9.1.1	Beleid voor toegangsbeveiliging	Ja	Ja			V	V
A.9.1.2	Toegang tot netwerken en netwerkdiensten	Ja	Ja			V	V
A.9.2	Beheer van toegangsrechten van gebruikers						
	Doelstelling: Toegang voor bevoegde gebruikers bewerkstelligen en onbevoegde toegang tot systemen en diensten voorkomen.						
A.9.2.1	Registratie en uitschrijving van gebruikers	Ja	Ja			V	V
A.9.2.2	Gebruikers toegang verlenen	Ja	Ja			V	V
A.9.2.3	Beheren van speciale toegangsrechten	Ja	Ja			V	V
A.9.2.4	Beheer van geheime authenticatieinformatie van gebruikers	Ja	Ja			V	V
A.9.2.5	Beoordeling van toegangsrechten van gebruikers	Ja	Ja			V	V
A.9.2.6	Toegangsrechten intrekken of aanpassen	Ja	Ja			V	V
A.9.3	Gebruikersverantwoordelijkheden						
	Doelstelling: Gebruikers verantwoordelijk maken voor het beschermen van hun authenticatie-informatie.						
A.9.3.1	Geheime authenticatie-informatie gebruiken	Ja	Ja			V	V
A.9.4	Toegangsbeveiliging van systeem en toepassing						
	Doelstelling: Onbevoegde toegang tot systemen en toepassingen voorkomen.						
A.9.4.1	Beperking toegang tot informatie	Ja	Ja			V	V
A.9.4.2	Beveiligde inlogprocedures	Ja	Ja			V	V
A.9.4.3	Systeem voor wachtwoordbeheer	Ja	Ja			V	V
A.9.4.4	Speciale systeemhulpmiddelen gebruiken	Ja	**Ja**			V	V
A.9.4.5	Toegangsbeveiliging op programmabroncode	Ja	Ja			V	V
A.10	Cryptografie						
A.10.1	Cryptografische beheersmaatregelen						
	Doelstelling: Zorgen voor correct en doeltreffend gebruik van cryptografie om de vertrouwelijkheid, authenticiteit en/of integriteit van informatie te beschermen.						
A.10.1.1	Beleid inzake het gebruik van cryptografische beheersmaatregelen	Ja	Ja			V	V
A.10.1.2	Sleutelbeheer	Ja	Ja			V	V
A.11	Fysieke beveiliging en beveiliging van de omgeving						
A.11.1	Beveiligde gebieden						
	Doelstelling: Onbevoegde fysieke toegang tot, schade aan en interferentie met informatie en informatieverwerkende faciliteiten van de organisatie voorkomen.						
A.11.1.1	Fysieke beveiligingszone	Ja	Ja			V	V
A.11.1.2	Fysieke toegangsbeveiliging	Ja	Ja			V	V
A.11.1.3	Kantoren, ruimten en faciliteiten beveiligen	Ja	Ja			V	V
A.11.1.4	Beschermen tegen bedreigingen van buitenaf	Ja	Ja			V	V
A.11.1.5	Werken in beveiligde gebieden	Ja	Ja			V	V
A.11.1.6	Laad- en loslocatie	Ja	Ja			V	V
A.11.2	Apparatuur						
	Doelstelling: Verlies, schade, diefstal of compromittering van bedrijfsmiddelen en onderbreking van de bedrijfsvoering van de organisatie voorkomen.						

	Beheersaspect	van Toepassing	Geïmplementeerd	Rechtvaardiging			
		Ja / Nee	Ja / Deels / Niet	WE	CE	BR	RA
A.11.2.1	Plaatsing en bescherming van apparatuur	Ja	Ja			V	V
A.11.2.2	Nutsvoorzieningen	Ja	Ja			V	V
A.11.2.3	Beveiliging van bekabeling	Ja	Ja			V	V
A.11.2.4	Onderhoud van apparatuur	Ja	Ja			V	V
A.11.2.5	Verwijdering van bedrijfsmiddelen	Ja	Ja			V	V
A.11.2.6	Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein	Ja	Ja			V	V
A.11.2.7	Veilig verwijderen of hergebruiken van apparatuur	Ja	Ja			V	V
A.11.2.8	Onbeheerde gebruikersapparatuur	Ja	Ja			V	V
A.11.2.9	'Clear desk'- en 'clear screen'-beleid	Ja	Ja			V	V
A.12	**Beveiliging bedrijfsvoering**						
A.12.1	**Bedieningsprocedures en verantwoordelijkheden**						
	Doelstelling: Correcte en veilige bediening van informatieverwerkende faciliteiten waarborgen.						
A.12.1.1	Gedocumenteerde bedieningsprocedures	Ja	Ja			V	V
A.12.1.2	Wijzigingsbeheer	Ja	Ja			V	V
A.12.1.3	Capaciteitsbeheer	Ja	Ja			V	V
A.12.1.4	Scheiding van ontwikkel-, test- en productieomgevingen	Ja	Ja				V
A.12.2	**Bescherming tegen malware**						
	Doelstelling: Waarborgen dat informatie en informatieverwerkende faciliteiten beschermd zijn tegen malware.						
A.12.2.1	Beheersmaatregelen tegen malware	Ja	Ja			V	V
A.12.3	**Back-up**						
	Doelstelling: Beschermen tegen het verlies van gegevens.						
A.12.3.1	Back-up van informatie	Ja	Ja			V	V
A.12.4	**Verslaglegging en monitoren**						
	Doelstelling: Gebeurtenissen vastleggen en bewijs verzamelen.						
A.12.4.1	Gebeurtenissen registreren	Ja	Ja			V	V
A.12.4.2	Beschermen van informatie in logbestanden	Ja	Ja				V
A.12.4.3	Logbestanden van beheerders en operators	Ja	Ja				V
A.12.4.4	Kloksynchronisatie	Ja	Ja				V
A.12.5	**Beheersing van operationele software**						
	Doelstelling: De integriteit van operationele systemen waarborgen.						
A.12.5.1	Software installeren op operationele systemen	Ja	Ja			V	V
A.12.6	**Beheer van technische kwetsbaarheden**						
	Doelstelling: Benutting van technische kwetsbaarheden voorkomen.						
A.12.6.1	Beheer van technische kwetsbaarheden	Ja	Ja			V	V
A.12.6.2	Beperkingen voor het installeren van software	Ja	Ja			V	V
A.12.7	**Overwegingen betreffende audits van informatiesystemen**						
	Doelstelling: De impact van auditactiviteiten op uitvoeringssystemen zo gering mogelijk maken.						
A.12.7.1	Beheersmaatregelen betreffende audits van informatiesystemen	Ja	Ja			V	V
A.13	**Communicatiebeveiliging**						
A.13.1	**Beheer van netwerkbeveiliging**						
	Doelstelling: De bescherming van informatie in netwerken en de ondersteunende informatieverwerkende faciliteiten waarborgen.						
A.13.1.1	Beheersmaatregelen voor netwerken	Ja	Ja			V	V
A.13.1.2	Beveiliging van netwerkdiensten	Ja	Ja			V	V
A.13.1.3	Scheiding in netwerken	Ja	Ja			V	V
A.13.2	**Informatietransport**						
	Doelstelling: Handhaven van de beveiliging van informatie die wordt uitgewisseld binnen een organisatie en met een externe entiteit.						
A.13.2.1	Beleid en procedures voor informatietransport	Ja	Ja			V	V
A.13.2.2	Overeenkomsten over informatietransport	Ja	Ja			V	V
A.13.2.3	Elektronische berichten	Ja	Ja			V	V
A.13.2.4	Vertrouwelijkheids- of geheimhoudingsovereenkomst	Ja	Ja			V	V
A.14	**Acquisitie, ontwikkeling en onderhoud van informatiesystemen**						
A.14.1	**Beveiligingseisen voor informatiesystemen**						
	Doelstelling: 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.						
A.14.1.1	Analyse en specificatie van informatiebeveiligingseisen	Ja	Ja			V	V
A.14.1.2	Toepassingsdiensten op openbare netwerken beveiligen	Ja	Ja				V
A.14.1.3	Transacties van toepassingsdiensten beschermen	Ja	Ja			V	V
A.14.2	**Beveiliging in ontwikkelings- en ondersteunende processen**						
	Doelstelling: Bewerkstelligen dat informatiebeveiliging wordt ontworpen en geïmplementeerd binnen de ontwikkelingslevenscyclus van informatiesystemen.						
A.14.2.1	Beleid voor beveiligd ontwikkelen	Ja	Ja			V	V
A.14.2.2	Procedures voor wijzigingsbeheer met betrekking tot systemen	Ja	Ja			V	V
A.14.2.3	Technische beoordeling van toepassingen na wijzigingen bedieningsplatform	Ja	Ja			V	V
A.14.2.4	Beperkingen op wijzigingen aan softwarepakketten	Ja	Ja			V	V
A.14.2.5	Principes voor engineering van beveiligde systemen	Ja	Ja			V	V
A.14.2.6	Beveiligde ontwikkelomgeving	Ja	Ja			V	V
A.14.2.7	Uitbestede softwareontwikkeling	Ja	Ja		V	V	V
A.14.2.8	Testen van systeembeveiliging	Ja	Ja			V	V
A.14.2.9	Systeem acceptatietests	Ja	Ja			V	V
A.14.3	**Testgegevens**						
	Doelstelling: Bescherming waarborgen van gegevens die voor het testen zijn gebruikt.						V
A.14.3.1	Bescherming van testgegevens	Ja	Ja			V	V
A.15	**Leveranciersrelaties**						
A.15.1	**Informatiebeveiliging in leveranciersrelaties**						
	Doelstelling: De bescherming waarborgen van bedrijfsmiddelen van de organisatie die toegankelijk zijn voor leveranciers.						
A.15.1.1	Informatiebeveiligingsbeleid voor leveranciersrelaties	Ja	Ja				V
A.15.1.2	Opnemen van beveiligingsaspecten in leveranciersovereenkomsten	Ja	Ja		V		V
A.15.1.3	Toeleveringsketen van informatie- en communicatietechnologie	Ja	Ja				V
A.15.2	**Beheer van dienstverlening van leveranciers**						
	Doelstelling: Een overeengekomen niveau van informatiebeveiliging en dienstverlening in overeenstemming met de leveranciersovereenkomsten handhaven.						
A.15.2.1	Monitoring en beoordeling van dienstverlening van leveranciers	Ja	Ja				V
A.15.2.2	Beheer van veranderingen in dienstverlening van leveranciers	Ja	Ja				V
A.16	**Beheer van informatiebeveiligingsincidenten**						
A.16.1	**Beheer van informatiebeveiligingsincidenten en -verbeteringen**						
	Doelstelling: Een consistente en doeltreffende aanpak bewerkstelligen van het beheer van informatiebeveiligingsincidenten, met inbegrip van communicatie over beveiligingsgebeurtenissen en zwakke plekken in de beveiliging.						
A.16.1.1	Verantwoordelijkheden en procedures	Ja	Ja			V	V
A.16.1.2	Rapportage van informatiebeveiligingsgebeurtenissen	Ja	Ja	V			V
A.16.1.3	Rapportage van zwakke plekken in de informatiebeveiliging	Ja	Ja			V	V
A.16.1.4	Beoordeling van en besluitvorming over informatiebeveiligingsgebeurtenissen	Ja	Ja				V
A.16.1.5	Respons op informatiebeveiligingsincidenten	Ja	Ja			V	V
A.16.1.6	Lering uit informatiebeveiligingsincidenten	Ja	Ja			V	V
A.16.1.7	Verzamelen van bewijsmateriaal	Ja	Ja				V

	Beheersaspect	van Toepassing	Geïmplementeerd	Rechtvaardiging			
		Ja / Nee	Ja / Deels / Niet	WE	CE	BR	RA
A.17	**Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer**						
A.17.1	**Informatiebeveiligingscontinuïteit**						
	Doelstelling: Informatiebeveiligingscontinuïteit moet worden ingebed in de systemen van het bedrijfscontinuïteitsbeheer van de organisatie.						
A.17.1.1	Informatiebeveiligingscontinuïteit plannen	Ja	Ja				V
A.17.1.2	Informatiebeveiligingscontinuïteit implementeren	Ja	Ja				V
A.17.1.3	Informatiebeveiligingscontinuïteit verifiëren, beoordelen en evalueren	Ja	Ja				V
A.17.2	**Redundante componenten**						
	Doelstelling: Beschikbaarheid van informatieverwerkende faciliteiten bewerkstelligen.						
A.17.2.1	Beschikbaarheid van informatieverwerkende faciliteiten	Ja	Ja		V	V	V
A.18	Naleving						
A.18.1	**Naleving van wettelijke en contractuele eisen**						
	Doelstelling: Voorkomen van schendingen van wettelijke, statutaire, regelgevende of contractuele verplichtingen betreffende informatiebeveiliging en beveiligingseisen.						
A.18.1.1	Vaststellen van toepasselijke wetgeving en contractuele eisen	Ja	Ja	V	V	V	V
A.18.1.2	Intellectuele eigendomsrechten	Ja	Ja	V	V	V	
A.18.1.3	Beschermen van registraties	Ja	Ja		V	V	V
A.18.1.4	Privacy en bescherming van persoonsgegevens	Ja	Ja	V			V
A.18.1.5	Voorschriften voor het gebruik van cryptografische beheersmaatregelen	Ja	Ja		V	V	V
A.18.2	**Informatiebeveiligingsbeoordelingen**						
	Doelstelling: Verzekeren dat informatiebeveiliging wordt geïmplementeerd en uitgevoerd in overeenstemming met de beleidsregels en procedures van de organisatie.						
A.18.2.1	Onafhankelijke beoordeling van informatiebeveiliging	Ja	Ja			V	V
A.18.2.2	Naleving van beveiligingsbeleid en -normen	Ja	Ja			V	V
A.18.2.3	Beoordeling van technische naleving	Ja	Ja			V	V

Legenda: **Geïmplementeerd:**
Ja: Alle mogelijke maatreglen zijn geïmplementeerd
Nee: Geen enkele beheersmaatregel geïmplementeerd

Rechtvaardiging:
WE: Wettelijke Eis
CE: Contractuele Eis
BR: Business Requirements/Best Practice
RA: Risico Analyse

Delft, 31-03-2023

Aldus vastgesteld door de Directie