AXS ict • Verklaring van Toepasselijkheid ISO 27001

15-10-2020

Index: WE: Wettelijke Eis, **CE**: Contractuele Eis, **BR**: Business Requirements/Best Practice), **RA**: Risico Analyse

				Reden van selectie (zie index)			
Nr.	**Doelstelling en maatregel ISO 27001:2013**	**Geselecteerd & Geïmplementeerd Ja/Nee**	**Onderbouwing (indien niet geselecteerd)**	**WE**	**CE**	**BR/BP**	**RA**
A.5	**Informatiebeveiligingsbeleid**						
A.5.1	**Aansturing door de directie van de informatiebeveiliging**						
A.5.1.1	Beleidsregels voor informatiebeveiliging	Ja				■	■
A.5.1.2	Beoordeling van het informatiebeveiligingsbeleid	Ja				■	
A.6	**Organiseren van informatiebeveiliging**						
A.6.1	**Interne organisatie**						
A.6.1.1	Rollen en verantwoordelijkheden bij informatiebeveiliging	Ja				■	■
A.6.1.2	Scheiding van taken	Ja				■	■
A.6.1.3	Contact met overheidsinstanties	Ja		■			
A.6.1.4	Contact met speciale belangengroepen	Ja				■	
A.6.1.5	Informatiebeveiliging in projectbeheer	Ja				■	
A.6.2	**Mobiele apparatuur en telewerken**						
A.6.2.1	Beleid voor mobiele apparatuur	Ja					■
A.6.2.2	Telewerken	Ja					■
A.7	**Veilig personeel**						
A.7.1	**Voorafgaand aan het dienstverband**						
A.7.1.1	Screening	Ja				■	■
A.7.1.2	Arbeidsvoorwaarden	Ja				■	■
A.7.2	**Tijdens het dienstverband**						
A.7.2.1	Directieverantwoordelijkheden	Ja				■	
A.7.2.2	Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	Ja					■
A.7.2.3	Disciplinaire procedure	Ja					■
A.7.3	**Beëindiging en wijziging van dienstverband**						
A.7.3.1	Beëindiging of wijziging van verantwoordelijkheden van het dienstverband	Ja					■
A.8	**Beheer van bedrijfsmiddelen**						
A.8.1	**Verantwoordelijkheid voor bedrijfsmiddelen**						
A.8.1.1	Inventariseren van bedrijfsmiddelen	Ja				■	
A.8.1.2	Eigendom van bedrijfsmiddelen	Ja				■	
A.8.1.3	Aanvaardbaar gebruik van bedrijfsmiddelen	Ja				■	
A.8.1.4	Teruggeven van bedrijfsmiddelen	Ja				■	
A.8.2	**Informatieclassificatie**						
A.8.2.1	Classificatie van informatie	Ja				■	
A.8.2.2	Informatie labelen	Ja				■	
A.8.2.3	Behandelen van bedrijfsmiddelen	Ja				■	
A.8.3	**Behandelen van media**						
A.8.3.1	Beheer van verwijderbare media	Ja				■	
A.8.3.2	Verwijderen van media	Ja				■	
A.8.3.3	Media fysiek overdragen	Ja				■	
A.9	**Toegangsbeveiliging**						
A.9.1	**Bedrijfseisen voor toegangsbeveiliging**						
A.9.1.1	Beleid voor toegangsbeveiliging	Ja					■
A.9.1.2	Toegang tot netwerken en netwerkdiensten	Ja					■
A.9.2	**Beheer van toegangsrechten van gebruikers**						
A.9.2.1	Registratie en afmelden van gebruikers	Ja				■	
A.9.2.2	Gebruikers toegang verlenen	Ja				■	
A.9.2.3	Beheren van speciale toegangsrechten	Ja					■
A.9.2.4	Beheer van geheime authenticatie-informatie van gebruikers	Ja				■	■
A.9.2.5	Beoordeling van toegangsrechten van gebruikers	Ja					■
A.9.2.6	Toegangsrechten intrekken of aanpassen	Ja				■	
A.9.3	**Verantwoordelijkheden van gebruikers**						
A.9.3.1	Geheime authenticatie-informatie gebruiken	Ja					■
A.9.4	**Toegangsbeveiliging van systeem en toepassing**						
A.9.4.1	Beperking toegang tot informatie	Ja					■
A.9.4.2	Beveiligde inlogprocedures	Ja				■	
A.9.4.3	Systeem voor wachtwoordbeheer	Ja					■
A.9.4.4	Speciale systeemhulpmiddelen gebruiken	Ja					■
A.9.4.5	Toegangsbeveiliging op programmabroncode	Ja					♑♒
A.10	**Cryptografie**						
A.10.1	**Cryptografische beheersmaatregelen**						
A.10.1.1	Beleid inzake het gebruik van cryptografische beheersmaatregelen	Ja					■
A.10.1.2	Sleutelbeheer	Ja					■
A.11	**Fysieke beveiliging en beveiliging van de omgeving**						

Nr.	Doelstelling en maatregel ISO 27001:2013	Geselecteerd & Geïmplementeerd Ja/Nee	Onderbouwing (indien niet geselecteerd)	WE	CE	BR/BP	RA
A.11.1	**Beveiligde gebieden**						
A.11.1.1	Fysieke beveiligingszone	Ja					■
A.11.1.2	Fysieke toegangsbeveiliging	Ja					■
A.11.1.3	Kantoren, ruimten en faciliteiten beveiligen	Ja					■
A.11.1.4	Beschermen tegen bedreigingen van buitenaf	Ja					■
A.11.1.5	Werken in beveiligde gebieden	Ja					■
A.11.1.6	Laad- en loslocatie	Nee	AXS ict heeft geen seperate laad- en loslocatie				
A.11.2	**Apparatuur**						
A.11.2.1	Plaatsing en bescherming van apparatuur	Ja					■
A.11.2.2	Nutsvoorzieningen	Ja					■
A.11.2.3	Beveiliging van bekabeling	Ja				■	
A.11.2.4	Onderhoud van apparatuur	Ja				■	
A.11.2.5	Verwijdering van bedrijfsmiddelen	Ja				■	
A.11.2.6	Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein	Ja					■
A.11.2.7	Veilig verwijderen of hergebruiken van apparatuur	Ja					■
A.11.2.8	Onbeheerde gebruikersapparatuur	Ja					■
A.11.2.9	'Clear desk'- en 'clear screen'-beleid	Ja					■
A.12	**Beveiliging bedrijfsvoering**						
A.12.1	**Bedieningsprocedures en verantwoordelijkheden**						
A.12.1.1	Gedocumenteerde bedieningsprocedures	Ja				■	■
A.12.1.2	Wijzigingsbeheer	Ja					■
A.12.1.3	Capaciteitsbeheer	Ja			■		■
A.12.1.4	Scheiding van ontwikkel-, test- en productieomgevingen	Ja					■
A.12.2	**Bescherming tegen malware**						
A.12.2.1	Beheersmaatregelen tegen malware	Ja					■
A.12.3	**Back-up**						
A.12.3.1	Back-up van informatie	Ja					■
A.12.4	**Verslaglegging en monitoren**						
A.12.4.1	Gebeurtenissen registreren	Ja				■	■
A.12.4.2	Beschermen van informatie in logbestanden	Ja				■	
A.12.4.3	Logbestanden van beheerders en operators	Ja				■	■
A.12.4.4	Kloksynchronisatie	Ja				■	
A.12.5	**Beheersing van operationele software**						
A.12.5.1	Software installeren op operationele systemen	Ja				■	
A.12.6	**Beheer van technische kwetsbaarheden**						
A.12.6.1	Beheer van technische kwetsbaarheden	Ja					■
A.12.6.2	Beperkingen voor het installeren van software	Ja				■	
A.12.7	**Overwegingen betreffende audits van informatiesystemen**						
A.12.7.1	Beheersmaatregelen betreffende audits van informatiesystemen	Ja				■	
A.13	**Communicatiebeveiliging**						
A.13.1	**Beheer van netwerkbeveiliging**						
A.13.1.1	Beheersmaatregelen voor netwerken	Ja					■
A.13.1.2	Beveiliging van netwerkdiensten	Ja			■		■
A.13.1.3	Scheiding in netwerken	Ja					■
A.13.2	**Informatietransport**						
A.13.2.1	Beleid en procedures voor informatietransport	Ja					■
A.13.2.2	Overeenkomsten over informatietransport	Ja			■		
A.13.2.3	Elektronische berichten	Ja				■	
A.13.2.4	Vertrouwelijkheids- of geheimhoudingsovereenkomst	Ja			■		
A.14	**Acquisitie, ontwikkeling en onderhoud van informatiesystemen**						
A.14.1	**Beveiligingseisen voor informatiesystemen**						
A.14.1.1	Analyse en specificatie van informatiebeveiligingseisen	Ja					■
A.14.1.2	Toepassingen op openbare netwerken beveiligen	Ja				■	
A.14.1.3	Transacties van toepassingen beschermen	Ja				■	
A.14.2	**Beveiliging in ontwikkelings- en ondersteunende processen**						
A.14.2.1	Beleid voor beveiligd ontwikkelen	Ja					■
A.14.2.2	Procedures voor wijzigingsbeheer met betrekking tot systemen	Ja					■
A.14.2.3	Technische beoordeling van toepassingen na wijzigingen besturingsplatform	Ja				■	
A.14.2.4	Beperkingen op wijzigingen aan softwarepakketten	Ja				■	
A.14.2.5	Principes voor engineering van beveiligde systemen	Ja				■	
A.14.2.6	Beveiligde ontwikkelomgeving	Ja				■	
A.14.2.7	Uitbestede softwareontwikkeling	Ja					■
A.14.2.8	Testen van systeembeveiliging	Ja					■
A.14.2.9	Systeemacceptatietests	Ja					■
A.14.3	**Testgegevens**						
A.14.3.1	Bescherming van testgegevens	Ja					■

Nr.	Doelstelling en maatregel ISO 27001:2013	Geselecteerd & Geïmplementeerd Ja/Nee	Onderbouwing (indien niet geselecteerd)	WE	CE	BR/BP	RA
A.15	**Leveranciersrelaties**						
A.15.1	**Informatiebeveiliging in leveranciersrelaties**						
A.15.1.1	Informatiebeveiligingsbeleid voor leveranciersrelaties	Ja					■
A.15.1.2	Opnemen van beveiligingsaspecten in leveranciersovereenkomsten	Ja			■		■
A.15.1.3	Toeleveringsketen van informatie- en communicatietechnologie	Ja					
A.15.2	**Beheer van dienstverlening van leveranciers**						
A.15.2.1	Monitoring en beoordeling van dienstverlening van leveranciers	Ja					■
A.15.2.2	Beheer van veranderingen in dienstverlening van leveranciers	Ja				■	
A.16	**Beheer van informatiebeveiligingsincidenten**						
A.16.1	**Beheer van informatiebeveiligingsincidenten en -verbeteringen**						
A.16.1.1	Verantwoordelijkheden en procedures	Ja				■	
A.16.1.2	Rapportage van informatiebeveiligingsgebeurtenissen	Ja				■	
A.16.1.3	Rapportage van zwakke plekken in de	Ja				■	
A.16.1.4	Beoordeling van en besluitvorming over informatiebeveiligingsgebeurtenissen	Ja				■	
A.16.1.5	Respons op informatiebeveiligingsincidenten	Ja				■	
A.16.1.6	Lering uit informatiebeveiligingsincidenten	Ja				■	
A.16.1.7	Verzamelen van bewijsmateriaal	Ja				■	
A.17	**Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer**						
A.17.1	**Informatiebeveiligingscontinuïteit**						
A.17.1.1	Informatiebeveiligingscontinuïteit plannen	Ja					■
A.17.1.2	Informatiebeveiligingscontinuïteit implementeren	Ja				■	
A.17.1.3	Informatiebeveiligingscontinuïteit verifiëren, beoordelen en evalueren	Ja				■	
A.17.2	**Redundante componenten**						
A.17.2.1	Beschikbaarheid van informatieverwerkende faciliteiten	Ja					■
A.18	**Naleving**						
A.18.1	**Naleving van wettelijke en contractuele eisen**						
A.18.1.1	Vaststellen van toepasselijke wetgeving en contractuele eisen	Ja		■	■		■
A.18.1.2	Intellectuele-eigendomsrechten	Ja		■			
A.18.1.3	Beschermen van registraties	Ja				■	
A.18.1.4	Privacy en bescherming van persoonsgegevens	Ja		■	■		■
A.18.1.5	Voorschriften voor het gebruik van cryptografische beheersmaatregelen	Ja		■		■	
A.18.2	**Informatiebeveiligingsbeoordelingen**						
A.18.2.1	Onafhankelijke beoordeling van informatiebeveiliging	Ja					■
A.18.2.2	Naleving van beveiligingsbeleid en -normen	Ja				■	
A.18.2.3	Beoordeling van technische naleving	Ja					■