Tabel voor Risicobehandeling

implementeerd van [datum] tot [datum]

Bedrijfsmiddelen / bedreigingen / kwetsbaarheden						[illegible]			*Risicobehandeling*		*Waarden na behandeling*		
Nr.	**Naam bedrijfsmiddel**	[illegible]	**Bedreiging**	[illegible]	**Risico-eigenaar**	[illegible]	[illegible]	**Risk**	**Selectie van opties**	[illegible]	**Gevolg**	[illegible]	**Risk**
													0
													0
													0

Risicobehandelingsopties

1. Selectie van (beheers)maatregelen
2. Overdracht van risico's naar een derde partij
3. Risicovermijding
4. Risicoacceptatie

Beheersmaatregelen volgens Bijlage A van de ISO/IEC 27001 norm

A.5.1.1 Beleidsdocumenten voor informatiebeveiliging
A.5.1.2 Beoordeling van het Informatiebeveiligingsbeleid
A.6.1.1 Informatiebeveiligings rollen en verantwoordelijkheden
A.6.1.2 Functiescheiding
A.6.1.3 Contact met autoriteiten
A.6.1.4 Contact met speciale groepen belanghebbenden
A.6.1.5 Informatiebeveiliging in projectmanagement
A.6.2.1 Beleid voor mobiele apparaten
A.6.2.2 Telewerken
A.7.1.1 Screening
A.7.1.2 Arbeidsvoorwaarden
A.7.2.1 Management verantwwoordelijkheden
A.7.2.2 Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging
A.7.2.3 Disciplinair proces
A.7.3.1 Beëindiging of wijziging van verantwoordelijkheden dienstverband
A.8.1.1 Inventarisatie van bedrijfsmiddelen
A.8.1.2 Eigenaarschap van bedrijfsmiddelen
A.8.1.3 Aanvaardbaar gebruik van bedrijfsmiddelen
A.8.1.4 Retournering van bedrijfsmiddelen
A.8.2.1 Classificatie van Informatie
A.8.2.2 Labeling van informatie
A.8.2.3 Behandeling van bedrijfsmiddelen
A.8.3.1 Beheer van verwijderbare media
A.8.3.2 Verwijdering van media
A.8.3.3 Fysieke gegevens-uitwisseling
A.9.1.1 Toegangsbeleid
A.9.1.2 Toegang tot netwerken en netwerkdiensten
A.9.2.1 Gebruikersregistratie en deregistratie
A.9.2.2 Beschikbaarstellen toegang gebruikers
A.9.2.3 Beheer van speciale bevoegdheden
A.9.2.4 Beheer van geheime authenticatie informatie van gebruikers
A.9.2.5 Beoordeling van toegangsrechten van gebruikers
A.9.2.6 Verwijdering of aanpassing van toegangsrechten
A.9.3.1 Gebruik van geheime authenticatie informatie
A.9.4.1 Beperking van toegang tot informatie
A.9.4.2 Beveiligde login procedures
A.9.4.3 Wachtwoorden managementsysteem
A.9.4.4 Gebruik van bevoorrecht gebruiksprogramma's
A.9.4.5 Toegangscontrole tot programma broncode
A.10.1.1 Beleid voor het gebruik van cryptografische beheersmaatregelen
A.10.1.2 Sleutelbeheer
A.11.1.1 Omtrek van fysieke beveiliging
A.11.1.2 Fysiek entree maatregelen
A.11.1.3 Beveiligen kantoren, kamers en faciliteiten.
A.11.1.4 Bescherming tegen
A.11.1.5 Werken in beveiligde ruimten
A.11.1.6 Openbare toegang en gebieden voor laden en lossen
A.11.2.1 Plaatsing en beschermingvan apparatuur

A.11.2.2 Nutsvoorzieningen (stroomtoevoer, etc.)
A.11.2.3 Beveiliging van kabels
A.11.2.4 Onderhoud van apparatuur
A.11.2.5 Verwijdering van bedrijfsmiddelen
A.11.2.6 Beveiliging van apparatuur buiten het terrein
A.11.2.7 Veilig verwijderen en hergebruiken van apparatuur
A.11.2.8 Onbeheerde gebruikersapparatuur
A.11.2.9 'Clear desk'- en 'clear screen'-beleid
A.12.1.1 Gedocumenteerde bedieningsprocedures
A.12.1.2 Wijzigingsbeheer
A.12.1.3 Capaciteitsbeheer
A.12.1.4 Scheiding van faciliteiten voor ontwikkeling, testen en productie
A.12.2.1 Maatregelen tegen virussen
A.12.3.1 Reservekopieën maken van informatie (back-ups)
A.12.4.1 Event logging
A.12.4.2 Bescherming van informatie in logbestanden
A.12.4.3 Logbestanden van administrators en operators
A.12.4.4 Synchronisatie van systeemklokken
A.12.5.1 Installatie van software op operationele systemen
A.12.6.1 Beheersing van technische kwetsbaarheden
A.12.6.2 Beperking in installatie van software
A.12.7.1 Beheersmaatregelen voor audits van informatiesystemen
A.13.1.1 Maatregelen voor netwerken
A.13.1.2 Beveiliging van netwerkdiensten
A.13.1.3 Scheding van netwerken
A.13.2.1 Beleid informatie-overdracht en procedures
A.13.2.2 Overeenkomsten inzake informatieuitwisseling
A.13.2.3 Elektronische berichtenverkeer
A.13.2.4 Vertrouwelijkheid of geheimhoudingsovereen-komsten
A.14.1.1 Analyse en specificatie van beveiligingseisen
A.14.1.2 Beveiliging applicaties op publieke netwerken
A.14.1.3 Beveiligen toepassing dienstentransacties
A.14.2.1 Beleid voor beveiligde ontwikkeling
A.14.2.2 Procedures voor wijzigingsbeheer
A.14.2.3 Technische beoordeling van toepassingen na wijzigingen in het besturingssysteem
A.14.2.4 Restricties op wijzigingen in programmatuurpakketten
A.14.2.5 Priciipes voor het bouwen van beveiigde systemen
A.14.2.6 Beveiligde ontwikkelingsomgeving
A.14.2.7 Uitbestede ontwikkeling
A.14.2.8 Testen beveiligingsysteem
A.14.2.9 Systeemacceptatie
A.14.3.1 Beveiliging van testgegevens
A.15.1.1 Informatiebeveiligingsbeleid voor leveranciersrelaties
A.15.1.2 Adresseren beveiliging binnen leveranciersovereennkomsten
A.15.1.3 Informatie en communicatietechnologie toevoerketen
A.15.2.1 Bewaken en herboordelen van leveranciersdiensten
A.15.2.2 Beheersing wijzigingen in leveranciersdiensten
A.16.1.1 Verantwoordelijkheden en procedures
A.16.1.2 Rapportage van informatiebeveiligings-gebeurtenissen
A.16.1.3 Rapportage van zwakke plekken in de beveiliging

A.16.1.4 Beoordeling van en besluit inzake beveiligingsgebeurtenissen
A.16.1.5 Reactie op informatiebeveiligingsincidenten
A.16.1.6 Leren van informatie-beveiligingsincidenten
A.16.1.7 Verzamelen van bewijsmateriaal
A.17.1.1 Planning informatiebeveiliging in het proces van bedrijfscontinuïteitsbeheer
A.17.1.2 Implementatie informatiebeveiliging in het proces van bedrijfscontinuïteitsbeheer
A.17.1.3 Verifieer, herbeoordeel en evalueer informatiebeveiliging in het proces van bedrijfscontinuï
A.17.2.1 Beschikbaarheid van informatie verwerkende faciliteiten
A.18.1.1 Identificatie van toepasselijke wetgeving en contractuele verplichtingen
A.18.1.2 Intellectuele eigendomsrechten (Intellectual Property Rights, (Intellectual Property Rights,IP
A.18.1.3 Bescherming van bedrijfsdocumenten
A.18.1.4 Bescherming van gegevens en geheimhouding van persoonsgegevens
A.18.1.5 Voorschriften voor het gebruik van cryptografische beheersmaatregelen
A.18.2.1 Onafhankelijk herbeoordeling van informatiebeveiliging
A.18.2.2 Naleving van informatie-beveiligingsbeleid en normen
A.18.2.3 Herbeoordeling technische naleving