

Verklaring van toepasseljkheid ISO/IEC 27001:2017

ISO 27001:2017 Beheersmaatregelen			
5. Informatiebeveiligingsbeleid	Toepasselijk	Toelichting	Implementatie
5.1. Management direction for information security			
5.1.1. Beleidsregels voor informatiebeveiliging	✓	Risico-analyse	✓
5.1.2. Beoordeling van het informatiebeveiligingsbeleid	✓	Risico-analyse	✓
6. Organiseren van informatiebeveiliging	Toepasselijk	Toelichting	Implementatie
6.1. Interne organisatie			
6.1.1. Rollen en verantwoordelijkheden bij informatiebeveiliging	✓	Risico-analyse	✓
6.1.2. Scheiding van taken	✓	Risico-analyse	✓
6.1.3. Contact met overheidsinstanties	✓	Risico-analyse	✓
6.1.4. Contact met speciale belangengroepen	✓	Risico-analyse	✓
6.1.5. Informatiebeveiliging in projectbeheer	✓	Risico-analyse	✓
6.2. Mobiele apparatuur en telewerken			
6.2.1. Beleid voor mobiele apparatuur	✓	Risico-analyse	✓
6.2.2. Telewerken	✓	Risico-analyse	✓
7. Veilig personeel	Toepasselijk	Toelichting	Implementatie
7.1. Voorafgaand aan het dienstverband			
7.1.1. Screening	✓	Risico-analyse	✓
7.1.2. Arbeidsvoorwaarden	✓	Risico-analyse	✓
7.2. Tijdens het dienstverband			
7.2.1. Directieverantwoordelijkheden	✓	Risico-analyse	✓
7.2.2. Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	✓	Risico-analyse	✓
7.2.3. Disciplinaire procedure	✓	Risico-analyse	✓
7.3. Beeindiging en wijziging van het dienstverband			
7.3.1. Beëindiging of wijziging van verantwoordelijkheden van het dienstverband	✓	Risico-analyse	✓
8. Beheer van bedrijfsmiddelen	Toepasselijk	Toelichting	Implementatie
8.1. Verantwoordelijkheden voor bedrijfsmiddelen			
8.1.1. Inventariseren van bedrijfsmiddelen	✓	Risico-analyse	✓
8.1.2. Eigendom van bedrijfsmiddelen	✓	Risico-analyse	✓
8.1.3. Aanvaardbaar gebruik van bedrijfsmiddelen	✓	Risico-analyse	✓
8.1.4. Teruggeven van bedrijfsmiddelen	✓	Risico-analyse	✓
8.2. Informatieclassificatie			
8.2.1. Classificatie van informatie	✓	Risico-analyse	✓
8.2.2. Informatie labelen	✓	Risico-analyse	✓
8.2.3. Behandelen van bedrijfsmiddelen	✓	Risico-analyse	✓
8.3. Behandelen van media			
8.3.1. Beheer van verwijderbare media	✓	Risico-analyse	✓
8.3.2. Verwijderen van media	✓	Risico-analyse	✓
8.3.3. Media fysiek overdragen	✓	Risico-analyse	✓

9. Toegangsbeveiliging	Toepasselijk	Toelichting	Implementatie
9.1. Bedrijfseisen voor toegangsbeveiliging			
9.1.1. Beleid voor toegangsbeveiliging	✓	Risico-analyse	✓
9.1.2. Toegang tot netwerken en netwerkdiensten	✓	Risico-analyse	✓
9.2. Beheer van toegangsrechten voor gebruikers			
9.2.1. Registratie en afmelden van gebruikers	✓	Risico-analyse	✓
9.2.2. Gebruikers toegang verlenen	✓	Risico-analyse	✓
9.2.3. Beheren van speciale toegangsrechten	✓	Risico-analyse	✓
9.2.4. Beheer van geheime authenticatie-informatie van gebruikers	✓	Risico-analyse	✓
9.2.5. Beoordeling van toegangsrechten van gebruikers	✓	Risico-analyse	✓
9.2.6. Toegangsrechten intrekken of aanpassen	✓	Risico-analyse	✓
9.3. Gebruikersverantwoordelijkheden			
9.3.1. Geheime authenticatie-informatie gebruikers	✓	Risico-analyse	✓
9.4. Toegangsbeveiliging van systeem en toepassing			
9.4.1. Beperking toegang tot informatie	✓	Risico-analyse	✓
9.4.2. Beveiligde inlogprocedures	✓	Risico-analyse	✓
9.4.3. Systeem voor wachtwoordbeheer	✓	Risico-analyse	✓
9.4.4. Speciale systeemhulpmiddelen gebruiken	✓	Risico-analyse	✓
9.4.5. Toegangsbeveiliging op programmabroncode	✓	Risico-analyse	✓
10. Cryptografie	Toepasselijk	Toelichting	Implementatie
10.1. Cryptografische beheersmaatregelen			
10.1.1. Beleid inzake het gebruik van cryptografisch beheersmaatregelen	✓	Risico-analyse	✓
10.1.2. Sleutelbeheer	✓	Risico-analyse	✓
11. Fysieke beveiliging en beveiliging van de omgeving	Toepasselijk	Toelichting	Implementatie
11.1. Fysieke beveiliging en beveiliging van de omgeving			
11.1.1. Fysieke beveiligingszone	✓	Risico-analyse	✓
11.1.2. Fysieke toegangsbeveiliging	✓	Risico-analyse	✓
11.1.3. Kantoren, ruimten en faciliteiten beveiligen	✓	Risico-analyse	✓
11.1.4. Beschermen tegen bedreigingen van buitenaf	✓	Risico-analyse	✓
11.1.5. Werken in beveiligde gebieden	✓	Risico-analyse	✓
11.1.6. Laad- en loslocatie	✓	Risico-analyse	✓
11.2. Apparatuur			
11.2.1. Plaatsing en bescherming van apparatuur	✓	Risico-analyse	✓
11.2.2. Nutsvoorzieningen	✓	Risico-analyse	✓
11.2.3. Beveiliging van bekabeling	✓	Risico-analyse	✓
11.2.4. Onderhoud van apparatuur	✓	Risico-analyse	✓
11.2.5. Verwijdering van bedrijfsmiddelen	✓	Risico-analyse	✓
11.2.6. Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein	✓	Risico-analyse	✓
11.2.7. Veilig verwijderen of hergebruiken van apparatuur	✓	Risico-analyse	✓
11.2.8. Onbeheerde gebruikersapparatuur	✓	Risico-analyse	✓
11.2.9. 'Clear desk'- end 'clear screen'-beleid	✓	Risico-analyse	✓

12. Beveiliging bedrijfsvoering	Toepasselijk	Toelichting	Implementatie
12.1. Bedieningsprocedures en verantwoordelijkheden			
12.1.1. Gedocumenteerde bedieningsprocedures	✓	Risico-analyse	✓
12.1.2. Wijzigingsbeheer	✓	Risico-analyse	✓
12.1.3. Capaciteitsbeheer	✓	Risico-analyse	✓
12.1.4. Scheiding van ontwikkel-, test- en productieomgevingen	✓	Risico-analyse	✓
12.2. Beschermingsmaatregelen tegen malware			
12.2.1. Beheersmaatregelen tegen malware	✓	Risico-analyse	✓
12.3. Back-up			
12.3.1. Back-up van informatie	✓	Risico-analyse	✓
12.4. Verslaglegging en monitoring			
12.4.1. Gebeurtenissen registreren	✓	Risico-analyse	✓
12.4.2. Beschermen van informatie in logbestanden	✓	Risico-analyse	✓
12.4.3. Logbestanden van beheerders en operators	✓	Risico-analyse	✓
12.4.4. Kloksynchronisatie	✓	Risico-analyse	✓
12.5. Beheersing van operationele software			
12.5.1. Software installeren op operationele systemen	✓	Risico-analyse	✓
12.6. Beheer van technische kwetsbaarheden			
12.6.1. Beheer van technische kwetsbaarheden	✓	Risico-analyse	✓
12.6.2. Beperkingen voor het installeren van software	✓	Risico-analyse	✓
12.7. Overwegingen betreffende audits van informatiesystemen			
12.7.1. Beheersmaatregelen betreffende audits van informatiesystemen	✓	Risico-analyse	✓
13. Communicatiebeveiliging	Toepasselijk	Toelichting	Implementatie
13.1. Beheer van netwerkbeveiliging			
13.1.1. Beheersmaatregelen voor netwerken	✓	Risico-analyse	✓
13.1.2. Beveiliging van netwerkdiensten	✓	Risico-analyse	✓
13.1.3. Scheiding in netwerken	✓	Risico-analyse	✓
13.2. Informatietransport			
13.2.1. Beleid en procedures voor informatietransport	✓	Risico-analyse	✓
13.2.2. Overeenkomsten over informatietransport	✓	Risico-analyse	✓
13.2.3. Elektronische berichten	✓	Risico-analyse	✓
13.2.4. Vertrouwelijkheids- of geheimhoudingsovereenkomst	✓	Risico-analyse	✓
14.1. Beveiligingseisen voor informatiebeveiliging			
14.1.1. Analyse en specificatie van informatiebeveiligingseisen	✓	Risico-analyse	✓

14. Acquisitie, ontwikkeling en onderhoud van informatiesystemen	Toepasselijk	Toelichting	Implementatie
14.1.2. Toepassingsdiensten op openbare netwerken beveiligen	✓	Risico-analyse	✓
14.1.3. Transactie van toepassingsdiensten beschermen	✓	Risico-analyse	✓
14.2. Beveiliging in ontwikkelings- en ondersteunende processen			
14.2.1. Beleid voor beveiligd ontwikkelen	✓	Risico-analyse	✓
14.2.2. Procedures voor wijzigingsbeheer met betrekking tot systemen	✓	Risico-analyse	✓
14.2.3. Technische beoordeling van toepassingen na wijzigingen bedieningsplatform	✓	Risico-analyse	✓
14.2.4. Beperkingen op wijzigingen aan softwarepakketten	✓	Risico-analyse	✓
14.2.5. Principes voor engineering van beveiligde systemen	✓	Risico-analyse	✓
14.2.6. Beveiligde ontwikkelomgeving	✓	Risico-analyse	✓
14.2.7. Uitbestede softwareontwikkeling	✗		
14.2.8. Testen van systeembeveiliging	✓	Risico-analyse	✓
14.2.9. Systeemacceptatietests	✓	Risico-analyse	✓
14.3. Testgegevens			
14.3.1. Bescherming van testgegevens	✓	Risico-analyse	✓
15. Leveranciersrelaties	Toepasselijk	Toelichting	Implementatie
15.1. Informatiebeveiliging voor leveranciersrelaties			
15.1.1. Informatiebeveiligingsbeleid voor leveranciersrelaties	✓	Risico-analyse	✓
15.1.2. Opnamen van beveiligingsaspecten in leveranciersovereenkomsten	✓	Risico-analyse	✓
15.1.3. Toeleveringsketen van informatie- en communicatietechnologie	✓	Risico-analyse	✓
15.2. Beheer van dienstverlening van leveranciers			
15.2.1. Monitoring en beoordeling van dienstverlening van leveranciers	✓	Risico-analyse	✓
15.2.2. Beheer van veranderingen in dienstverlening van leveranciers	✓	Risico-analyse	✓
16. Beheer van informatiebeveiligingsincidenten	Toepasselijk	Toelichting	Implementatie
16.1. Beheer van informatiebeveiligingsincidenten en - verbeteringen			
16.1.1. Verantwoordelijkheden en procedures	✓	Risico-analyse	✓
16.1.2. Rapportage van informatiebeveiligingsgebeurtenissen	✓	Risico-analyse	✓
16.1.3. Rapportage van zwakke plekken in de informatiebeveiliging	✓	Risico-analyse	✓
16.1.4. Beoordeling van en besluitvorming over informatiebeveiligingsgebeurtenissen	✓	Risico-analyse	✓
16.1.5. Respons op informatiebeveiligingsincidenten	✓	Risico-analyse	✓
16.1.6. Lering uit informatiebeveiligingsincidenten	✓	Risico-analyse	✓
16.1.7. Verzamelen van bewijsmateriaal	✓	Risico-analyse	✓
17. Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer	Toepasselijk	Toelichting	Implementatie
17.1. Informatiebeveiligingscontinuïteit			
17.1.1. Informatiebeveiligingscontinuïteit plannen	✓	Risico-analyse	✓
17.1.2. Informatiebeveiligingscontinuïteit implementeren	✓	Risico-analyse	✓
17.1.3. Informatiebeveiligingscontinuïteit verifiëren, beoordelen en evalueren	✓	Risico-analyse	✓
17.2. Redundancies			
17.2.1. Beschikbaarheid van informatieverwerkende faciliteiten	✓	Risico-analyse	✓

18. Naleving	Toepasselijk	Toelichting	Implementatie
18.1. Compliance with legal and contractual requirements			
18.1.1. Vaststellen van toepasselijke wetgeving en contractuele eisen	✓	Risico-analyse	✓
18.1.2. Intellectuele eigendomsrechten	✓	Risico-analyse	✓
18.1.3. Beschermen van registraties	✓	Risico-analyse	✓
18.1.4. Privacy en bescherming van persoonsgegevens	✓	Risico-analyse	✓
18.1.5. Voorschriften voor het gebruik van cyptografische beheersmaatregelen	✓	Risico-analyse	✓
18.2. Information security reviews			
18.2.1. Onafhankelijke beoordeling van informatiebeveiliging	✓	Risico-analyse	✓
18.2.2. Naleving van beveiligingsbeleid en -normen	✓	Risico-analyse	✓
18.2.3. Beoordeling van technische nalevering	✓	Risico-analyse	✓