| ISO 27001:2022 | Bijlage A: Referentiebeheersdoelstellingen en -maatregelen | ISO 27001:2013 |
|---|---|---|
| **5** | **Organisatorische maatregelen** | |
| 5.1 | Beleid voor informatiebeveiliging | A5.1.1 |
| 5.2 | Rollen en verantwoordelijkheden op het gebied van informatiebeveiliging | A6.1.1 |
| 5.3 | Functiescheiding | A6.1.2 |
| 5.4 | Beheersverantwoordelijkheden | A6.1.1 |
| 5.5 | Contact met autoriteiten | A6.1.3 |
| 5.6 | Contact met speciale belangengroepen | A6.1.4 |
| 5.7 | Bedreigingsinformatie | Nieuw |
| 5.8 | Informatiebeveiliging in projectmanagement | A6.1.5 |
| 5.9 | Inventarisatie van informatie en andere bijbehorende assets | A8.1.1 |
| 5.10 | Aanvaardbaar gebruik van informatie en andere bijbehorende assets | A8.1.3 |
| 5.11 | Teruggave van assets | A8.1.4 |
| 5.12 | Classificatie van informatie | A8.2.1 |
| 5.13 | Labelen van informatie | A8.2.2 |
| 5.14 | Informatieoverdracht | A13.2 |
| 5.15 | Toegangsbeveiliging | A9 |
| 5.16 | Identiteitsbeheer | A9.2.1 |
| 5.17 | Authenticatie-informatie | A9 |
| 5.18 | Toegangsrechten | A9.2 |
| 5.19 | Informatiebeveiliging in leveranciersrelaties | A15 |
| 5.20 | Aanpak informatiebeveiliging binnen leveranciersovereenkomsten | A15.1 |
| 5.21 | Beheer van informatiebeveiliging in de ICT-toeleveringsketen | A15.2 |
| 5.22 | Monitoring, beoordeling en wijzigingsbeheer van leveranciersdiensten | A15.2 |
| 5.23 | Informatiebeveiliging bij het gebruik van cloud diensten | Nieuw |
| 5.24 | Planning en voorbereiding van informatiebeveiligingsincidenten | A16.1 |
| 5.25 | Beoordeling en besluit over informatiebeveiligingsgebeurtenissen | A16.1.4 |
| 5.26 | Reactie op informatiebeveiligingsincidenten | A16.1.5 |
| 5.27 | Leren van informatiebeveiligingsincidenten | A16.1.6 |
| 5.28 | Verzameling van bewijs | A16.1.7 |
| 5.29 | Informatiebeveiliging tijdens verstoring | A17.1 |
| 5.30 | ICT-gereedheid voor bedrijfscontinuïteit | Nieuw |
| 5.31 | Identificatie van wettelijke, statutaire, regelgevende en contractuele vereisten | A18.1.1 |
| 5.32 | Intellectuele eigendomsrechten | A18.1.2 |
| 5.33 | Gegevensbescherming | A18.1.3 |
| 5.34 | Privacy en bescherming van PII | A18.1.4 |
| 5.35 | Onafhankelijke beoordeling van informatiebeveiliging | A18.2.1 |
| 5.36 | Naleving van beleidslijnen en normen voor informatiebeveiliging | A18.2.2 |

| | | |
|---|---|---|
| 5.37 | Gedocumenteerde bedieningsprocedures | A12.1.1 |
| **6.** | **Maatregelen tav mensen** | |
| 6.1 | Screening | A7.1.1 |
| 6.2 | Arbeidsvoorwaarden | A7.1.2 |
| 6.3 | Bewustwording, opleiding en training op het gebied van informatiebeveiliging | A7.2.2 |
| 6.4 | Disciplinair proces | A7.2.3 |
| 6.5 | Verantwoordelijkheden na beëindiging of verandering van dienstverband | A7.3.1 |
| 6.6 | Geheimhoudings- of geheimhoudingsovereenkomsten | A7.2/A15.1.2 |
| 6.7 | Werken op afstand | A6.2.2 |
| 6.8 | Rapportage van informatiebeveiligingsgebeurtenissen | A12.4 |
| **7.** | **Fysieke maatregelen** | |
| 7.1 | Fysieke beveiligingszone | A11.1.1 |
| 7.2 | Fysieke toegangscontroles | A11.1.2 |
| 7.3 | Beveiligen van kantoren, kamers en faciliteiten | A11.1.3 |
| 7.4 | Fysieke beveiligingsmonitoring | Nieuw |
| 7.5 | Bescherming tegen fysieke en omgevingsbedreigingen | A11.1.4 |
| 7.6 | Werken in beveiligde ruimtes | A11.1.5 |
| 7.7 | Clear desk, clear screen | A11.2.9 |
| 7.8 | Plaatsing en bescherming van de uitrusting | A11.2.1 |
| 7.9 | Beveiliging van assets buiten de bedrijfsruimten | A11.2.6 |
| 7.10 | Opslagmedia | A8.3 |
| 7.11 | Ondersteunende systemen | A11.2.2 |
| 7.12 | Bekabelingbeveiliging | A11.2.3 |
| 7.13 | Onderhoud van de apparatuur | A11.2.4 |
| 7.14 | Veilige verwijdering of hergebruik van apparatuur | A11.2.7 |
| **8.** | **Technische maatregelen** | |
| 8.1 | Eindgebruikers apparatuur | A6.2.1, A11.2.8 |
| 8.2 | Speciale toegangsrechten | A9.2.3 |
| 8.3 | Beperking van toegang tot informatie | A9.4.1 |
| 8.4 | Toegang tot broncode | A9.4.5 |
| 8.5 | Beveiligde authenticatie | A9.3 |
| 8.6 | Capaciteitsbeheer | A12.1.3 |
| 8.7 | Bescherming tegen malware | A12.2 |
| 8.8 | Beheer van technische kwetsbaarheden | A12.6 |
| 8.9 | Configuratiebeheer | Nieuw |
| 8.10 | Informatie verwijderen | Nieuw |
| 8.11 | Gegevensmaskering | Nieuw |
| 8.12 | Preventie van datalekken | Nieuw |
| 8.13 | Informatie back-up | A12.3 |
| 8.14 | Redundantie van informatieverwerkingsfaciliteiten | A17.2 |

| | | |
|---|---|---|
| 8.15 | Loggen | A12.4 |
| 8.16 | Bewaking van activiteiten | Nieuw |
| 8.17 | Kloksynchronisatie | A12.4.4 |
| 8.18 | Gebruik van geprivilegieerde hulpprogramma's | A12.7.1 |
| 8.19 | Installatie van software op operationele systemen | A12.5.1 |
| 8.20 | Netwerkbediening | A13.1 |
| 8.21 | Beveiliging van netwerkdiensten | A13.1 |
| 8.22 | Segregatie in netwerken | A13.1.3 |
| 8.23 | Webfiltering | Nieuw |
| 8.24 | Gebruik van cryptografie | A10 |
| 8.25 | Veilige ontwikkelingslevenscyclus | A10.1.3 |
| 8.26 | Beveiligingsvereisten voor toepassingen | A14.1 |
| 8.27 | Veilige systeemarchitectuur en engineeringprincipes | A14.2.5 |
| 8.28 | Veilig programmeren | Nieuw |
| 8.29 | Beveiligingstesten in ontwikkeling en acceptatie | A14.2.8/9 |
| 8.30 | Uitbestede ontwikkeling | A14.2.7 |
| 8.31 | Scheiding van ontwikkel-, test- en productieomgevingen | A12.1.4 |
| 8.32 | Wijzigingsbeheer | A14.2.2 |
| 8.33 | Testinformatie | A14.3 |
| 8.34 | Bescherming van informatiesystemen tijdens audit en testen | A12.7.1 |