De cyberveiligheidsnorm toegepast voor de toeleveringsketen

Artikel 21.2d van de Europese NIS2 richtlijn legt cyberhygiëne vereisten op aan kritieke industrie, diensten en infrastructuur. Essentiële en belangrijke bedrijven dienen daarom samen te werken met hun directe leveranciers om de beveiliging van de toeleveringsketen te waarborgen. Het NIS2 Quality Mark biedt hiervoor een geschikte norm met drie niveaus (Basic, Substantial en High), zodat de maatregelen passen bij het dreigingsniveau.

Dit is de norm NIS2-QM30 High, behorende bij het NIS2 Quality Mark, integraal onderdeel van het Compliance en Certificeringsschema van NIS2 Quality Mark en de Stichting Kwaliteitsinnovatie.

NIS2 Quality Mark High: NIS2 QM30		Mapping* met ISO27001
1. Organisatorische maatregelen		
1.2	**Informatiebeveiligingsbeleid en bestuurlijke goedkeuring**: Het management van de organisatie dient een beleid te formuleren waarin strategische doelstellingen zijn geformuleerd inzake de bescherming van de beschikbaarheid, integriteit en vertrouwelijkheid van informatie tegen cyberdreigingen. Het beleid is akkoord bevonden door het hogere management en gedeeld met medewerkers en andere betrokkenen. De organisatie dient specifieke beleidsregels te formuleren die gebaseerd zijn op het cyberbeleid en die ondersteuning moeten bieden aan proactieve paraatheid en beveiliging tegen incidenten en cyberdreigingen. De beleidsregels geven duidelijkheid over standaardpraktijken zoals toegangsbeveiliging, applicatiebeheer, IT-beheer, netwerkbeheer en back-up-beheer. De beleidsregels zijn goedgekeurd door geschikt management en gecommuniceerd aan relevante medewerkers.	**A.5.1**
1.3	**Toewijzing wie verantwoordelijk is voor cybersecurity:** De organisatie dient taken en verantwoordelijkheden bij cybersecurity te definiëren en toe te wijzen. De verantwoordelijkheden voor het initiëren en beslissen over cybersecuritymaatregelen zijn bekend bij de verantwoordelijken. Er is minstens één persoon aangesteld die verantwoordelijk is voor de cybersecurity van de organisatie.	**A.5.2**
1.4	**Aansturing door het management:** Het management van de organisatie dient expliciet van alle medewerkers, inclusief alle nieuwe medewerkers, te eisen dat ze werken volgens de informatiebeveiligingsregels en informatiebeveiligingsprocedures van de organisatie.	**A.5.4**
1.5	**Beoordeling en inzicht van beveiligingsdreigingen:** De organisatie dient regelmatig geschikte bronnen te raadplegen om op de hoogte te blijven van dreigingen die relevant kunnen zijn voor de informatiebeveiliging. Indien nodig worden extra maatregelen getroffen als bescherming tegen nieuwe of veranderende dreigingen.	**A.5.7**
1.6.1	**Overzicht van informatie:** De organisatie dient een overzicht met categorieën van bedrijfsinformatie op te stellen en te onderhouden. Per categorie is een eigenaar (beheerder) benoemd die verantwoordelijk is voor de bescherming van de informatie in die categorie.	**A.5.9**
1.6.2	**Overzicht van ICT-bedrijfsmiddelen**: De organisatie dient een overzicht van ICT-bedrijfsmiddelen op te stellen en te onderhouden, met inbegrip van servers, dataopslagsystemen en firewalls. Per bedrijfsmiddel (of groep van bedrijfsmiddelen) is een eigenaar (beheerder) benoemd die verantwoordelijk is voor de bescherming ervan.	**A.5.9**

**Mapping: Deze norm is vergelijkbaar, maar niet identiek aan ISO27001. Elk normeringsstelsel heeft zijn eigen specifieke kenmerken. De 'A' waar naar wordt verwezen betreft de nummering uit bijlage A van de 27001 norm.*
*** N/a: Not available, niet van toepassing. Er is geen corresponderende maatregel in ISO27001.*

1.7	**Informatie en aanverwante bedrijfsmiddelen acceptabel gebruiken**: De organisatie moet richtlijnen opstellen en delen over het veilig gebruiken van informatie en daaraan gerelateerde bedrijfsmiddelen zoals computers, laptops, telefoons, opslagmedia en bedrijfsapplicaties.	**A.5.10**
1.8	**Het inleveren van bedrijfsmiddelen na gebruik:** De organisatie dient, met behulp van een procedure en een checklist, te zorgen dat medewerkers en inhuurkrachten bedrijfsmiddelen (zoals laptops, telefoons, keycards en sleutels) inleveren na het aflopen of aanpassen van hun arbeidsovereenkomst.	**A.5.11**
1.9	**Informatie indelen:** De organisatie dient een overzicht bij te houden van verschillende categorieën van bedrijfsinformatie die hetzelfde niveau van vertrouwelijkheid hebben. Per categorie is vastgesteld hoe de betreffende bedrijfsinformatie behandeld en beschermd moet worden om de vertrouwelijkheid ervan te waarborgen. Per categorie is ook vastgesteld of de betreffende bedrijfsinformatie gelabeld moet worden om beter herkenbaar te zijn voor medewerkers.	**A.5.12**
1.11	**Het overbrengen van informatie binnen de organisatie en aan derden:** De organisatie moet richtlijnen opstellen die duidelijk aangeven welke middelen en externe partijen gebruikt mogen worden voor de veilige overdracht van vertrouwelijke informatie, zowel intern als met externe partijen. Daarnaast zorgt de organisatie ervoor dat alle medewerkers op de hoogte zijn van deze richtlijnen voor het veilig overdragen van informatie.	**A.5.14**
1.13	**Registratie en uitschrijving gebruikers**: De organisatie dient een procedure op te stellen en in gebruik te nemen voor het aanmaken, aanpassen en tijdig verwijderen van alle soorten accounts waar geregistreerde medewerkers en inhuurkrachten gebruik van maken.	**A.5.16**
1.14	**Beheer van toegangsrechten**: De organisatie dient een procedure te implementeren die ervoor moet zorgen dat toegangsrechten op de juiste wijze worden verstrekt, aangepast en verwijderd. Er wordt een registratie bijhouden waaruit blijkt wie er logische en fysieke toegangsrechten hebben ontvangen en op welke datum deze weer zijn ingetrokken.	**A.5.18**
1.15	**Bescherming van informatie in samenwerking met leveranciers**: De organisatie dient processen en procedures te definiëren die de organisatie in staat stellen om te bepalen of diensten en producten van leveranciers in voldoende mate aansluiten bij de informatiebeveiligingseisen van de organisatie. Indien nodig worden passende maatregelen getroffen om de risico's te beheersen.	**A.5.19**
1.16	**Borgen van informatieveiligheid in overeenkomsten met leveranciers:** De organisatie dient processen en procedures te definiëren die de organisatie in staat stellen om te bepalen of waarborgen die leveranciers bieden in voldoende mate aansluiten bij de informatiebeveiligingseisen van de organisatie. Indien nodig worden aanvullende afspraken overeengekomen.	**A.5.20**
1.18	**Toezicht, evaluatie en wijzigingsbeheer van leveranciersdiensten:** De organisatie dient op basis van een risicobeoordeling vast te stellen welke leveranciers van diensten in aanmerking komen om extra gemonitord te worden. Van de geselecteerde leveranciers wordt regelmatig op basis van onderzoek beoordeeld of de betrouwbaarheid en veiligheid van de dienstverlening in voldoende mate aansluit bij de daarover gemaakte afspraken en de actuele eisen van de organisatie.	**A.5.22**
1.19	**Informatie veilig houden bij het gebruik van cloudservices:** De organisatie dient processen te definiëren die de organisatie in staat stellen om te bepalen of waarborgen die leveranciers van clouddiensten bieden in voldoende mate aansluiten bij het cybersecuritybeleid van de organisatie.	**5.23**

**Mapping: Deze norm is vergelijkbaar, maar niet identiek aan ISO27001. Elk normeringsstelsel heeft zijn eigen specifieke kenmerken. De 'A' waar naar wordt verwezen betreft de nummering uit bijlage A van de 27001 norm.*
*** N/a: Not available, niet van toepassing. Er is geen corresponderende maatregel in ISO27001.*

1.20	**Richtlijnen voor de aanpak van informatiebeveiligingsincidenten (cybersecurityincidenten)**: Er dient een plan te worden opgesteld dat duidelijk maakt hoe de organisatie omgaat met een vermoede of vastgestelde inbreuk op de beschikbaarheid, integriteit of vertrouwelijkheid van informatie. In het plan wordt duidelijk aangegeven wie verantwoordelijk is voor welke taken.	**5.24**
1.21	**Registratie, beoordeling en afhandeling van informatiebeveiligingsincidenten:** De organisatie dient gebeurtenissen met betrekking tot informatiebeveiliging te beoordelen om vast te stellen of het incidenten betreffen. Incidenten worden geregistreerd en afgehandeld in overeenstemming met gedocumenteerde procedures.	**5.25**
1.22	**Incidenten melden aan externen:** Elke entiteit die op basis van de geldende lokale wetgeving onder de NIS2 richtlijn valt, dient meldplicht procedures te hebben om meldingen te kunnen doen bij de daarvoor bevoegde overheid in geval van incidenten. Alle organisaties hebben en gebruiken een gedocumenteerde procedure om informatiebeveiligingsincidenten in overeenstemming met contractuele eisen te melden aan externen.	**5.26**
1.23	**Voorbereiding ICT ten behoeve van bedrijfscontinuïteit:** De organisatie moet een plan opstellen dat ICT- continuïteitseisen bevat, waaronder doelstellingen voor de maximale hersteltijd van essentiële informatiesystemen. Er zijn technische en organisatorische maatregelen geïmplementeerd om bij een verstoring aan de ICT-continuïteitseisen te kunnen voldoen.	**A.5.30**
1.24	**Objectieve toetsing van de aanpak van informatiebeveiliging:** De organisatie moet op geplande momenten een onafhankelijke beoordeling laten uitvoeren om te bepalen of de informatiebeveiligingsaanpak voldoende bijdraagt aan het behalen van de doelstellingen uit het informatiebeveiligingsbeleid. Als blijkt dat de aanpak tekortschiet, neemt het management corrigerende maatregelen.	**5.35**
1.25	**Handhaven van voorschriften, regelgeving en standaarden voor informatiebeveiliging:**De organisatie dient met geplande tussenpozen een onafhankelijke beoordeling te laten uitvoeren om vast te stellen of de organisatie werkt volgens de eisen van de NIS2 Quality Mark norm en volgens de eigen informatiebeveiligingseisen van de organisatie in de vorm van interne regels, afspraken, processen en procedures.	**5.36**

**Mapping: Deze norm is vergelijkbaar, maar niet identiek aan ISO27001. Elk normeringsstelsel heeft zijn eigen specifieke kenmerken. De 'A' waar naar wordt verwezen betreft de nummering uit bijlage A van de 27001 norm.*
*** N/a: Not available, niet van toepassing. Er is geen corresponderende maatregel in ISO27001.*

1.26	**Samen de toeleveringsketen beveiligen:** Voor de leveringsketen dient de organisatie passende en evenredige technische, operationele en organisatorische maatregelen te nemen om de risico's voor de beveiliging van de netwerk- en informatiesystemen te voorkomen. De maatregelen voor de leveringsketen dienen gebaseerd te zijn op een benadering die alle gevaren omvat met betrekking tot de bescherming van netwerken, informatiesystemen en de fysieke omgeving. De focus moet liggen op leveranciers die risico's vormen voor de bedrijfscontinuïteit, met name waar zij raken aan de 'Te Beschermen Belangen' (kroonjuwelen): essentiële gegevens, diensten, processen of systemen waarvan aantasting aanzienlijke schade kan veroorzaken. De organisatie moet in haar beleid bedrijfsrisico's vaststellen in verband met het gebruik van producten en diensten van leveranciers. De organisatie legt dat beleid schriftelijk vast en past dat beleid aantoonbaar toe. Relevante afspraken over digitale weerbaarheid in de toeleveringsketen zijn contractueel vastgelegd met leveranciers. De bijbehorende maatregelen worden aantoonbaar geborgd via proportionele certificering of audits uitgevoerd door de organisatie zelf of door onafhankelijke auditoren.	**A.5.21**
1.27	**Verzamelen bewijsmateriaal:** De organisatie dient vast te stellen bij welk type incidenten welk bewijsmateriaal verzameld en veilig gesteld moet worden voor het kunnen achterhalen van de oorzaak, of voor het kunnen leveren van bewijs aan derden.	**A.5.28 /5.29**
2. Mensgerichte maatregelen		
2.1	**Geheimhoudingplicht in arbeidsovereenkomsten**: In alle vormen van arbeidsovereenkomsten dient een geheimhoudingsplicht te zijn opgenomen.	**A.6.2**
2.2	**Educatie van bestuurders en medewerkers over digitale veiligheid:** De directie en bestuurders van de organisatie dienen een opleiding of een cursus te volgen zodat ze cyberbeveiligingsrisico's kunnen identificeren en beoordelen. Medewerkers van de organisatie krijgen een opleiding en training over digitale veiligheid die past bij hun functie en ze worden getest op hun kennis van regels en procedures van de organisatie.	**A.6.3**
2.4	**Blijvende verantwoordelijkheden na vertrek of wijziging in de arbeidsrelatie**: Met medewerkers en inhuurkrachten dient te worden overeengekomen dat er een geheimhoudingsplicht blijft gelden na het aflopen of aanpassen van hun arbeidsovereenkomst.	**A.6.5**
2.5	**Overeenkomsten voor geheimhouding:** De organisatie dient ervoor te zorgen dat medewerkers en inhuurkrachten een geheimhoudingsovereenkomst ondertekenen, waarin wordt vastgelegd dat vertrouwelijke informatie die tijdens de samenwerking wordt uitgewisseld, niet openbaar mag worden gemaakt aan derden.	**A.6.6**
2.6	**Thuis- of hybride werken op een veilige manier:** De organisatie dient regels te formuleren en te communiceren voor een veilige informatieverwerking op externe locaties. De organisatie zorgt ervoor dat alle medewerkers de regels voor het werken op externe locaties kennen.	**A.6.7**
2.7	**Melding van gebeurtenissen met betrekking tot informatiebeveiliging**: De organisatie dient alle medewerkers duidelijk te maken hoe waargenomen of mogelijke incidenten met betrekking tot informatiebeveiliging snel en via de juiste communicatiekanalen kunnen worden gemeld.	**A.6.8**

**Mapping: Deze norm is vergelijkbaar, maar niet identiek aan ISO27001. Elk normeringsstelsel heeft zijn eigen specifieke kenmerken. De 'A' waar naar wordt verwezen betreft de nummering uit bijlage A van de 27001 norm.*
*** N/a: Not available, niet van toepassing. Er is geen corresponderende maatregel in ISO27001.*

2.8	**Achtergrondcontroles bij kandidaten voor een dienstverband:** De organisatie moet richtlijnen vaststellen en uitvoeren voor het screenen van kandidaten voordat zij in dienst treden. De breedte en diepgang van de screenings staan in verhouding tot de informatiebeveiligingsrisico's die gepaard gaan met de beoogde functies.	**A.6.1**
3. Fysieke maatregelen		
3.1	**Fysieke toegangsbeveiliging:** De organisatie dient op basis van een risicobeoordeling een passende fysieke beveiliging te ontwerpen en te implementeren voor terreinen, gebouwen, kantoren en ruimten. Het ontwerp houdt rekening met de behoefte van de organisatie om binnen een omgeving specifieke toegang te kunnen verlenen of te voorkomen.	**A.7.1/ A.7.2**
3.5	**Regelgeving voor vertrouwelijke informatie achterlaten op bureau en scherm:** De organisatie dient regels te formuleren en te communiceren voor het vergrendelen van actieve computerschermen en voor het verwijderen van papier en opslagmedia met vertrouwelijke informatie op onbemande werkplekken. De organisatie zorgt ervoor dat alle medewerkers de regels voor onbemande werkplekken kennen en naleven.	**A.7.7**
3.8	**Bedrijfsapparatuur veilig verwijderen of hergebruiken:** De organisatie dient een procedure op te stellen en in gebruik te nemen voor het veilig verwijderen of hergebruiken van bedrijfsapparatuur die ingebouwde opslagmedia bevat. De richtlijnen specificeren dat gevoelige gegevens en software moeten worden gewist of overschreven voordat een apparaat mag worden afgevoerd of hergebruikt.	**A.7.14**
3.9	**Toegangsbeveiliging definiëren**: De organisatie moet per functie of rol toegangsrechten definiëren, afgestemd op de behoeften van elke functie of rol en beperkt tot wat noodzakelijk is.	**A.5.15**
4. Technologische maatregelen		
4.1	**Beveiliging en beheer gebruikersapparaten**: Bedrijfsapparaten die medewerkers en inhuurkrachten gebruiken (zoals PC's, laptops, telefoons en tablets) dienen te worden beveiligd tegen onbevoegd gebruik, het onbevoegd installeren van software en het onbevoegd wijzigen van beveiligingsinstellingen.	**A.8.1**
4.2	**Bijzondere toegangsbevoegdheden:** De organisatie dient een procedure te implementeren die ervoor moet zorgen dat bijzondere toegangsrechten, zoals van systeem- en applicatiebeheerders, op de juiste wijze worden verstrekt, aangepast en verwijderd. Er wordt een registratie bijhouden waaruit blijkt wie er bijzondere toegangsrechten hebben ontvangen en op welke datum deze weer zijn ingetrokken.	**A.8.2**
4.4	**Bestrijding en preventie van malware:** De organisatie dient maatregelen tegen malware te implementeren, waaronder technische maatregelen voor het tijdig detecteren en onschadelijk maken van malware.	**A.8.7**
4.5	**Back-up en herstel:** Back-ups van gegevens en systemen moeten worden uitgevoerd volgens een vastgesteld back-upplan. Back-ups worden getest om te controleren dat ze deugdelijk zijn op het moment dat ze moeten worden gebruikt.	**A.8.13**

**Mapping: Deze norm is vergelijkbaar, maar niet identiek aan ISO27001. Elk normeringsstelsel heeft zijn eigen specifieke kenmerken. De 'A' waar naar wordt verwezen betreft de nummering uit bijlage A van de 27001 norm.*
*** N/a: Not available, niet van toepassing. Er is geen corresponderende maatregel in ISO27001.*

4.6	**Redundantie van infrastructuur:** De organisatie dient op basis van bedrijfscontinuïteitsdoelstellingen en ICT-continuïteitsdoelstellingen (zie 1.23) vast te stellen welke onderdelen van de ICT-infrastructuur meervoudig moeten worden uitgevoerd. De meervoudige uitvoering (redundantie) is geïmplementeerd en getest om de doelstellingen te kunnen realiseren.	**A.8.14**
4.7	**Software op bedrijfsmiddelen up-to-date houden:** De organisatie moet een beleid opstellen en toepassen voor van het voortdurend up-to-date en veilig houden van software op alle bedrijfsmiddelen.	**A.8.19**
4.8	**Netwerken beheren en beveiligen:** De organisatie moet taken en plichten vastleggen en toewijzen voor het beheer en de configuratie van netwerken en netwerkapparatuur. Alle netwerkapparaten zijn opgenomen in een inventaris en hebben een eigenaar (beheerder). De inventaris wordt onderhouden en bevat relevante informatie over de netwerkapparaten.	**A.8.20**
4.9	**Netwerksegmentatie:** De organisatie dient regels vast te stellen en toe te passen voor het segmenteren van groepen gebruikers, informatiesystemen en informatiediensten in de netwerken van de organisatie.	**A.8.22**
4.10	**Authenticatiemethoden toepassen:** De organisatie dient te zorgen dat toegepaste authenticatiemethoden in lijn zijn met de gevoeligheid van de informatie die men probeert te benaderen. MFA moet in ieder geval worden toegepast voor accounts met beheerdersrechten, bij toegang tot systemen met gevoelige informatie en voor alle gebruikers die via het internet inloggen.	**A.8.5**
4.11	**Logbestanden:** De organisatie dient logbestanden van relevante gebeurtenissen te registreren en te analyseren. Op basis van een risicobeoordeling is door de organisatie bepaald wat relevante gebeurtenissen zijn en op welke wijze de geregistreerde logbestanden dienen te worden geanalyseerd.	**A.8.15**
4.12	**Cryptografie en encryptie:** De organisatie dient op basis van een risicobeoordeling regels op te stellen en toe te passen die duidelijk maken in welke gevallen opgeslagen en verzonden informatie beveiligd moet worden met een specifieke vorm van cryptografie. Deze regels maken ook duidelijk hoe cryptografische sleutels veilig moeten worden bewaard.	**A.8.24**
4.14	**Technische kwetsbaarheden tijdig vinden en repareren:** De organisatie moet verantwoordelijkheden vaststellen en toewijzen voor het op tijd opsporen, registreren en repareren van technische kwetsbaarheden in netwerken en informatiesystemen die onder het beheer van de organisatie vallen.	**A.8.8**
4.15	**Gecontroleerd doorvoeren van wijzigingen:** De organisatie dient een proces op te stellen en in te voeren voor het gecontroleerd doorvoeren van wijzigingen in netwerken en informatiesystemen die onder het beheer van de organisatie vallen. Het proces bevat een verplichte analyse van de mogelijke impact op de beschikbaarheid, integriteit en vertrouwelijkheid van informatie.	**A.8.32**

**Mapping: Deze norm is vergelijkbaar, maar niet identiek aan ISO27001. Elk normeringsstelsel heeft zijn eigen specifieke kenmerken. De 'A' waar naar wordt verwezen betreft de nummering uit bijlage A van de 27001 norm.*
*** N/a: Not available, niet van toepassing. Er is geen corresponderende maatregel in ISO27001.*

Hieronder volgen een aantal aanvullende beheersmaatregelen die specifiek gelden voor organisaties die werken in of gebruik maken van Operational Technology (OT) en Information Technology (IT). Vanzelfsprekend hebben de algemene beheersmaatregelen hierboven ook betrekking op deze bedrijven.

5. OT-maatregelen		
5.1	**Register van alle OT-bedrijfsmiddelen:** De organisatie dienst een overzicht van OT-bedrijfsmiddelen op te stellen en te onderhouden, met inbegrip van relevante configuratiegegevens, zoals softwareversies en patchniveaus. Per bedrijfsmiddel is een eigenaar (beheerder) benoemd.	**n/a****
5.2	**Bepaal de afhankelijkheid van OT-systemen:** De organisatie dient per OT-systeem in kaart te brengen hoe afhankelijk de organisatie hiervan is, wat de kans op uitval is, en wat de impact bij uitval is.	**n/a**
5.4	**Back-ups van OT-systemen:** Back-ups van OT-systemen dienen te worden gemaakt volgens een gedefinieerd back-up-plan. Back-ups worden getest om te controleren dat ze deugdelijk zijn op het moment dat ze moeten worden gebruikt.	**n/a**
5.5	**Recovery plan OT-systemen:** De organisatie moet een bedrijfscontinuïteitsplan opstellen dat de continuïteitseisen beschrijft voor mogelijke verstoringen, inclusief de geaccepteerde hersteltijd voor essentiële OT-systemen. Technische en organisatorische maatregelen zijn geïmplementeerd om bij verstoringen te voldoen aan de OT-continuïteitseisen, en de effectiviteit van deze maatregelen is getest.	**n/a**
5.6	**Segmentatie van OT-netwerken**: De organisatie dient regels vast te stellen en toe te passen voor het segmenteren van OT-netwerken van de organisatie.	**n/a**
5.8	**Remote toegang tot kritieke OT-systemen:** De organisatie dient een server te gebruiken die als beveiligd toegangspunt fungeert bij remote toegang tot kritieke OT-systemen die onder het beheer van de organisatie vallen. De betreffende server heeft een eigenaar (beheerder) die verantwoordelijk is voor de beveiliging ervan.	**n/a**
5.9	**OT-patches installeren**: De organisatie dient verantwoordelijkheden vast te stellen en toe te wijzen voor het tijdig toepassen van essentiële patches op de systemen binnen OT-netwerken die onder het beheer van de organisatie vallen.	**n/a**
5.11	**Overzicht van OT-systemen en aanvullende informatie:** De organisatie dienst een overzicht van alle OT- systemen op te stellen en te onderhouden, met inbegrip van informatie over hardware, software, firmware, configuraties, beveiligingsinstellingen, leveranciers en onderhoud. Per OT-systeem is een eigenaar (beheerder) benoemd.	**n/a**
6. IT-maatregelen		
6.1	**Toegang tot broncode**: De organisatie dient de toegang tot broncode en software libraries te beschermen tegen onbevoegde toegang en ongewenste wijzigingen.	**8.4**

**Mapping: Deze norm is vergelijkbaar, maar niet identiek aan ISO27001. Elk normeringsstelsel heeft zijn eigen specifieke kenmerken. De 'A' waar naar wordt verwezen betreft de nummering uit bijlage A van de 27001 norm.*
*** N/a: Not available, niet van toepassing. Er is geen corresponderende maatregel in ISO27001.*

6.2	**Actueel houden van de programmacode en externe componenten:** Organisaties die applicaties ontwikkelen dienen ervoor te zorgen dat programmacode, inclusief externe componenten zoals libraries en frameworks, regelmatig wordt bijgewerkt met de laatste beveiligingsupdates. Dit is vastgelegd in een formeel proces, waarbij updates binnen een vastgestelde termijn worden uitgevoerd en gedocumenteerd. Het proces wordt periodiek geëvalueerd en gecontroleerd op naleving.	**n/a**
6.3	**Veilige software ontwikkelen:** De organisatie dient 'best practices' vast te stellen voor het ontwikkelen van veilige software. De naleving van deze 'best practices' wordt gecontroleerd.	**A.8.27**
6.4	**Bewustwording van informatiebeveiliging bij de ontwikkeling van applicaties:** Organisaties die applicaties ontwikkelen dienen ervoor te zorgen dat ontwikkelaars zich bewust zijn van de informatiebeveiligingsrisico's die samenhangen met het ontwikkelen van applicaties en het gebruiken van die applicaties bij het verwerken van informatie.	**A.6.3**
6.5	**Testen van de beveiliging van applicaties:** Organisaties die applicaties (laten) ontwikkelen dienen vooraf eisen te stellen aan de beveiliging van de applicaties met het oog op het gebruik ervan in de praktijk. Bij het testen van een ontwikkelde applicatie worden niet alleen de gebruikersaspecten getest, maar ook de beveiligingsaspecten van de applicatie.	**A.8.29**
6.6	**Uitbestede softwareontwikkeling:** Wanneer het ontwikkelen van maatwerksoftware (deels) is uitbesteed aan een externe partij bewaakt de organisatie actief de ontwikkelactiviteiten en stelt de organisatie vast of de opgeleverde software voldoet aan de informatiebeveiligingseisen.	**A.8.3**
6.7	**Scheiden van ontwikkel, test, acceptatie en productie:** Organisaties die applicaties (laten) ontwikkelen, dienen ervoor te zorgen dat ontwikkel- en testomgevingen gescheiden blijven van productieomgevingen, bijvoorbeeld door gebruik te maken van gescheiden virtuele of fysieke omgevingen, in combinatie met gescheiden toegangsrechten.	**A.8.31**
6.8	**Procedures en methodes voor het deployen van software:** Organisaties die software op hun operationele systemen (laten) installeren, dienen procedures en maatregelen te implementeren om dit op een veilige en gecontroleerde wijze uit te voeren.	**n/a**
6.9	**Overzicht van geleverde software:** De organisatie dient een overzicht van alle klanten op te stellen en te onderhouden die gebruik maken van software die door de organisatie is gemaakt. Dit overzicht moet duidelijk aangeven welke klant momenteel welke versie van welke software gebruikt.	**n/a**
6.10	**Overzicht houden over geleverde apparatuur en programmatuur:** De organisatie dient alle aan klanten geleverde apparatuur en programmatuur nauwkeurig te inventariseren en vast te leggen in een actueel en gedocumenteerd overzicht van het IT-landschap. Dit overzicht dient periodiek te worden bijgewerkt en gecontroleerd. Het proces moet waarborgen dat proactief onderhoud wordt uitgevoerd en dat beveiligingsupdates tijdig bij klanten worden toegepast.	**n/a**
6.12	**Overzicht houden over geleverde apparatuur en programmatuur:** De organisatie dient alle aan klanten geleverde apparatuur en programmatuur nauwkeurig te inventariseren en vast te leggen in een actueel en gedocumenteerd overzicht van het IT-landschap. Dit overzicht dient periodiek te worden bijgewerkt en gecontroleerd. Het proces moet waarborgen dat proactief onderhoud wordt uitgevoerd en dat beveiligingsupdates tijdig bij klanten worden toegepast.	**n/a**

**Mapping: Deze norm is vergelijkbaar, maar niet identiek aan ISO27001. Elk normeringsstelsel heeft zijn eigen specifieke kenmerken. De 'A' waar naar wordt verwezen betreft de nummering uit bijlage A van de 27001 norm.*
*** N/a: Not available, niet van toepassing. Er is geen corresponderende maatregel in ISO27001.*

Copyright

Toelichting op mapping

Onze norm voor cybersecurity is het resultaat van een uitgebreide samenwerking tussen een divers team van experts op het gebied van cyberbeveiliging. Dit multidisciplinaire team bestond uit vertegenwoordigers van NIS2 organisaties, mkb-bedrijven, onafhankelijke cybersecurityspecialisten en auditoren. Door deze gevarieerde samenstelling hebben we ervoor gezorgd dat onze norm een breed scala aan perspectieven en expertise omvat, wat heeft geleid tot een unieke en uiterst waardevolle benadering van cybersecurity.

Hoewel onze norm mogelijk enige overlap vertoont met andere cybersecuritynormen op bepaalde punten, moeten gebruikers begrijpen dat onze norm een op zichzelf staand product is, dat is ontwikkeld met het oog op de specifieke behoeften en uitdagingen van moderne bedrijven. De inhoud en aanpak van onze norm kunnen daarom verschillen van die van andere normen, zelfs als er enige gelijkenis bestaat.

Het is belangrijk om te benadrukken dat onze norm is ontworpen om de best practices op het gebied van cybersecurity te omvatten, gebaseerd op de inzichten en ervaringen van onze diverse teamleden. Daarom moeten gebruikers onze norm beschouwen als een uniek instrument dat is ontwikkeld met het oog op maximale toegevoegde waarde en effectiviteit voor organisaties die streven naar verbeterde cybersecurity.

Disclaimer

Hoewel de maatregelen opgenomen in het NIS2 Quality Mark en gerelateerde overzicht van maatregelen zijn ontwikkeld door experts en met de grootst mogelijke zorg zijn samengesteld, worden geen garanties gegeven met betrekking tot de correctheid, volledigheid, betrouwbaarheid, geschiktheid, of beschikbaarheid van het NIS2 Quality Mark en de daarin opgenomen informatie, producten, diensten, of gerelateerde grafieken. Het gebruik van het NIS2 Quality Mark en gerelateerde overzicht van maatregelen zijn volledig voor het risico van de gebruiker. Elke aansprakelijkheid voor schade, direct of indirect, voortvloeiend uit of in enig opzicht verband houdend met het gebruik van het NIS2 Quality Mark en gerelateerde overzicht van maatregelen wordt uitgesloten.

In het NIS2 Quality Mark mapping overzicht kunnen verwijzingen zijn opgenomen naar andere standaarden, waaronder ISO 27001 en NEN 7510, uitsluitend voor informatieve doeleinden en om mogelijke samenhang of raakvlakken te identificeren. Deze verwijzingen impliceren geen associatie of goedkeuring van de inhoud van de andere standaarden. Het NIS2 Quality Mark en gerelateerde overzicht van maatregelen en de genoemde andere standaarden zijn afzonderlijke en unieke documenten. Alle rechten met betrekking tot andere standaarden die in het document worden genoemd, behoren toe aan de respectieve rechtmatige eigenaren van die standaarden.

Op NIS2 Quality Mark en gerelateerde overzicht van maatregelen rust auteursrecht. Geen deel van deze standaard mag worden gereproduceerd, opgeslagen in een geautomatiseerd gegevensbestand, of openbaar gemaakt, in enige vorm of op enige wijze, hetzij elektronisch, mechanisch, door fotokopieën, opnamen, of enige andere manier, zonder voorafgaande schriftelijke toestemming.