De cyberveiligheidsnorm 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-QM20 Substantial, behorende bij het NIS2 Quality Mark, integraal onderdeel van het Compliance en Certificeringsschema van NIS2 Quality Mark en de Stichting Kwaliteitsinnovatie.

NIS2 Quality Mark Substantial: NIS2 QM20		Mapping* met ISO27001
1. Organisatorische beheersmaatregelen		
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
1.6.1	**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
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

**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. .*

NIS2 Quality Mark Substantial: NIS2 QM20		Mapping* met ISO27001
1. Organisatorische beheersmaatregelen		
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
1.20	**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
1.23	**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
1.26	**Samen de toeleveringsketen beveiligen:** De organisatie moet de informatiebeveiligingsrisico's vaststellen gerelateerd aan de afname van ICT-producten en -diensten van leveranciers, of van leveranciers dieper in de toeleveringsketen. Relevante afspraken met betrekking tot informatiebeveiliging in de ICT-toeleveringsketen zijn overeengekomen met leveranciers van de organisatie.	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 beheersmaatregelen		
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

**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.*

De cyberveiligheidsnorm voor de toeleveringsketen

NIS2 Quality Mark Substantial: NIS2 QM20		Mapping* met ISO27001
2. Mensgerichte maatregelen		
2.6	**Thuis en 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
3. Fysieke beheersmaatregelen		
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 beheersmaatregelen		
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
4.4	**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
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

**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.*

NIS2 Quality Mark Substantial: NIS2 QM20		Mapping* met ISO27001
4. Technologische beheersmaatregelen		
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

**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.*

De cyberveiligheidsnorm voor de toeleveringsketen

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.

NIS2 Quality Mark Substantial: NIS2 QM20		Mapping* met ISO27001
OT- beheersmaatregelen		
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
5.11	**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
IT-beheersmaatregelen		
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
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
6.9	**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
6.12	**Afstemming met klanten over nieuwe software en updates:** De organisatie dient een proces op te stellen en in te voeren voor het in overleg met klanten installeren van nieuwe versies van software of van patches.	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