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.

NIS2-Quality Mark Substantial: NIS2-QM20		Mapping* met ISO27001
1. Organisatorische beheersmaatregelen		
1.2	**Beleidsvorming voor informatiebeveiliging en bestuurlijke goedkeuring:** Formuleer een cybersecurity strategie en borg deze. Het formuleren van een informatiebeveiligings-en governancebeleid vereist het opstellen van gedetailleerde richtlijnen. Deze dienen minimaal een basis cyberhygiënebeleid te bevatten, inclusief standaardpraktijken zoals updates, wachtwoordwijzigingen, installatiebeheer, het beperken van toegangsniveaus en data-back-ups, ondersteunend aan proactieve paraatheid en beveiliging tegen incidenten of dreigingen. De verantwoordelijkheden voor het initiëren en beslissen over alle cybersecurity maatregelen moeten duidelijk zijn. Zorg altijd voor formele bestuurlijke goedkeuring.	5.1
1.3	**Toewijzing wie verantwoordelijk is bij informatiebeveiliging:** Elke medewerker krijgt specifieke taken en verantwoordelijkheden toegewezen in het kader van informatiebeveiliging. Het is cruciaal om een aangewezen persoon te hebben die verantwoordelijk is voor informatiebeveiliging.	5.2
1.6.1	**Overzicht van informatie:** Creëer een overzichtelijke lijst van alle organisatiegegevens, zoals klantinformatie en contracten. Wijs tevens een eigenaar/beheerder aan voor specifieke informatie.	5.9
1.6.2	**Overzicht van ICT-bedrijfsmiddelen:** Stel een gedetailleerde lijst op van alle organisatie-ICT-middelen met software, servers, dataopslagsystemen en firewalls. Benoem ook een verantwoordelijke eigenaar/beheerder per bedrijfsmiddel.	5.9
1.7	**Informatie en aanverwante bedrijfsmiddelen acceptabel gebruiken:** Er dienen voorschriften te worden opgesteld voor veilig gebruik van informatie. Dit omvat tevens ICT-middelen die gerelateerd zijn aan informatie, zoals netwerkapparatuur en clouddiensten.	5.10
1.8	**Het inleveren van bedrijfsmiddelen na gebruik:** Bij vertrek leveren medewerkers bedrijfsmiddelen in, zoals computers en smartphones, om vertrouwelijke informatie te waarborgen. Stel een procedure en checklist op voor een correcte teruggave.	5.11
1.9	**Informatie indelen:** Met behulp van een opgesteld classificatieschema wordt informatie geclassificeerd door middel van labeling, waarbij bijvoorbeeld wordt vastgesteld dat een kopie van een paspoort onderdeel is van de categorie personeelsgegevens. Dit verschaft medewerkers die met informatie werken een beknopt overzicht van hoe zij de informatie dienen te behandelen en te beschermen.	5.12
1.13	**Regulering van identiteitsgegevens:** De identiteit van het personeel dient vastgelegd te worden, en er dient een procedure geïmplementeerd te worden waarin beschreven staat hoe deze gegevens geregistreerd, aangepast en verwijderd dienen te worden (de "levenscyclus").	5.16

**Mapping: Deze norm is vergelijkbaar, maar niet identiek aan ISO27001. Elk normeringsstelsel heeft zijn eigen specifieke kenmerken.*

NIS2-Quality Mark Substantial: NIS2-QM20		Mapping* met ISO27001
1. Organisatorische beheersmaatregelen		
1.14	**Verlening en beheer van toegangsbevoegdheden:** Bij nieuwe medewerkers of functiewijzigingen is er risico op ongeoorloofde toegangsrechten. Controleer bij beëindiging van een dienstverband of accounts correct worden afgesloten. Registreer wie toegang heeft, definieer logische en fysieke toegangsrechten en noteer de beëindigingsdatum.	5.18
1.15	**Bescherming van informatie in samenwerking met leveranciers:** Er dient een inventarisatie te worden gemaakt van de risico's die zich voordoen bij de leveranciers, waarna deze worden beoordeeld en er maatregelen worden genomen om de risico's te beperken.	5.19
1.20	**Richtlijnen voor de aanpak van informatiebeveiligingsincidenten (cybersecurityincidenten):** Er dient een plan te worden opgesteld met betrekking tot hoe de organisatie omgaat met informatiebeveiligingsincidenten, zoals een inbreuk die beschikbaarheid, integriteit of vertrouwelijkheid van informatie bedreigt. Hierbij wordt duidelijk aangegeven wie verantwoordelijk is voor welke taken.	5.24
1.23	**Voorbereiding en optimalisatie van ICT voor het bedrijfscontinuïteitsproces:** Bij onverwachte gebeurtenissen, zoals een cyberaanval, is het cruciaal om snel operationeel te zijn. Formuleer doelen en bijbehorende continuïteitseisen, zoals een proces inclusief back-upbeheer, de noodvoorzieningenplannen en crisisbeheer inclusief cyberveiligheid. Zet de continuïteitseisen in een plan.	5.30
1.26	**Samen de toeleveringsketen beveiligen:** Voer een grondige risico-inventarisatie uit voor belangrijke leveranciers en maak gezamenlijke afspraken over digitale beveiliging. Zorg dat ontvangers (personen of organisaties) tijdig geïnformeerd zijn over de beheersmaatregelen die ze kunnen nemen bij een significante cyberdreiging in de organisatie. Significante cyberdreiging: een dreiging die, gezien de technische kenmerken, ernstige schade (materieel of immaterieel) aan organisaties, systemen of dienstgebruikers kan veroorzaken.	n/a**
1.27	**Informatiebeveiliging en bewijsverzameling tijdens een incident:** Om ervoor te zorgen dat de organisatie operationeel blijft en er adequaat gereageerd wordt op een beveiligingsincident, is het essentieel om vast te leggen hoe en wanneer bewijsmateriaal verzameld wordt, en hoe een passend niveau van informatiebeveiliging gehandhaafd blijft, zelfs in geval van een incident.	5.28/ 5.29
2. Mensgerichte beheersmaatregelen		
2.2	**Educatie van bestuurders en medewerkers en bewustwording voor het beveiligen van informatie:** Zorg dat directie en bestuurders een opleiding of een cursus volgen zodat ze cyberbeveiligingsrisico's kunnen identificeren en beoordelen. Het is belangrijk dat iedereen in de organisatie de risico's van informatieverwerking begrijpt. Gebruik bijvoorbeeld video-trainingsmodules voor medewerkers over digitale veiligheid. Zorg voor opleidingen die passen bij de verschillende functies. Medewerkers moeten worden getest op hun kennis en naleving van het beleid.	6.3

**Mapping: Deze norm is vergelijkbaar, maar niet identiek aan ISO27001. Elk normeringsstelsel heeft zijn eigen specifieke kenmerken.*
*** N/a: Not available, niet van toepassing. Er is geen corresponderende maatregel in ISO27001.*

De cyberveiligheidsnorm toegepast voor de toeleveringsketen

NIS2-Quality Mark Substantial: NIS2-QM20		Mapping* met ISO27001
2. Mensgerichte maatregelen		
2.6	**Thuis- of hybride werken op een veilige manier:** Werken buiten de organisatie vergroot het cyberincidentrisico. Formuleer regels voor veilige informatieverwerking op externe locaties en zorg dat alle medewerkers deze kennen en naleven.	6.7
2.7	**Registratie en rapportage van gebeurtenissen met betrekking tot informatiebeveiliging:** Maak afspraken om een snelle melding van bedreigingen voor de informatieveiligheid te waarborgen. Gebruik interne communicatiekanalen zoals e-mail, WhatsApp en bij voorkeur telefonie voor directe respons. Overweeg een digitaal meldsysteem of app voor uitgebreidere rapportage.	6.8
3. Fysieke beheersmaatregelen		
3.5	**Regelgeving voor vertrouwelijke informatie achterlaten op bureau en scherm:** Om te voorkomen dat vertrouwelijke informatie op een bureau of op een scherm in verkeerde handen valt, zijn duidelijke en eenduidige regels noodzakelijk waar werknemers zich aan dienen te houden. Er worden regels opgesteld voor een "Clear Desk" en "Clear Screen", zodat gevoelige of vertrouwelijke informatie niet in handen komt van onbevoegden.	7.7
3.8	**Gevoelige informatie en software op de juiste manier (veilig) verwijderen of overschrijven:** Indien apparatuur wordt vervangen of hergebruikt, is het cruciaal om datalekken te voorkomen door ervoor te zorgen dat gevoelige/informatie en software veilig worden verwijderd of overschreven. Een checklist voor (onderdelen van) apparatuur met opslagmedia kan hierbij van dienst zijn. Deze checklist geeft aan hoe gecontroleerd kan worden of alle gevoelige/informatie correct is verwijderd.	7.14
3.9	**Beveiligingsmaatregelen voor toegang:** Voorkom ongeautoriseerde toegang tot bedrijfsmiddelen met gevoelige informatie. Formuleer heldere toegangsregels, met bijzondere aandacht voor de beveiliging van essentiële bedrijfsmiddelen.	5.15
4. Technologische beheersmaatregelen		
4.1	**Beveiliging en beheer gebruikersapparaten:** Beveilig medewerkersapparaten, zoals laptops en telefoons, tegen cyberincidenten. Implementeer maatregelen zoals laptopversleuteling en beperking van adminrechten. Onderhoud en verspreid een actuele lijst met regels, inclusief vereisten voor sterke wachtwoorden en pincodes.	8.1
4.4	**Bestrijding en preventie van malware:** Malware kan schade aanrichten en gevoelige informatie blootleggen. Bescherm de digitale omgeving met anti-malwaresoftware, een virusscanner en een spamfilter. Overweeg encryptie voor belangrijke documenten.	8.7
4.5	**Informatiebehoud: back-up en herstel:** Voorkom dataverlies met een back-up plan (volgens de 3-2-1-systematiek), maak regelmatig back-ups van belangrijke data en systemen en test deze periodiek op betrouwbaarheid.	8.13
4.7	**Software op computers en apparaten up-to-date houden:** Houd computers en apparaten veilig met regelmatige updates. Installeer direct alle updates volgens de vastgestelde procedures voor veilig updaten op alle apparaten.	8.19

**Mapping: Deze norm is vergelijkbaar, maar niet identiek aan ISO27001. Elk normeringsstelsel heeft zijn eigen specifieke kenmerken.*

NIS2-Quality Mark Substantial: NIS2-QM20		Mapping* met ISO27001
4. Technologische beheersmaatregelen		
4.9	**Indeling van netwerken:** Door middel van netwerksegmentatie wordt voorkomen dat één groot netwerk wordt gecreëerd; in plaats daarvan wordt het opgedeeld in specifieke segmenten, waardoor problemen die zich voordoen in één deel niet het hele netwerk treffen.	8.22
4.10	**Authenticatie op cruciale systemen:** Zorg ervoor dat bij authenticatie- en communicatiesystemen gebruik wordt gemaakt van multifactor-authenticatie(MFA) of continue-authenticatieoplossingen, alsmede beveiligde spraak-, video- en tekstcommunicatie en veilige noodcommunicatiesystemen. Gebruik authenticatiemethoden (zoals wachtwoorden of MFA) die in lijn zijn met de gevoeligheid van de informatie die men probeert te benaderen. Implementeer MFA voor accounts met beheerdersrechten en voor alle toegang tot systemen met bedrijfsgevoelige informatie. Bovendien dienen gebruikers die via het internet inloggen ook MFA te gebruiken.	8.5
4.11	**Logboekregistratie:** Door logbestanden te creëren, te beschermen en te analyseren, kunnen onregelmatigheden in netwerken, systemen en applicaties vroegtijdig worden opgespoord.	8.15

**Mapping: Deze norm is vergelijkbaar, maar niet identiek aan ISO27001. Elk normeringsstelsel heeft zijn eigen specifieke kenmerken.*

De cyberveiligheidsnorm toegepast 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:** Identificeer en documenteer alle hardware- en softwarecomponenten (OT-bedrijfsmiddelen) die binnen de organisatie worden gebruikt. Als er al een gedetailleerd overzicht bestaat, zorg dan dat dit overzicht ook informatie bevat over de specifieke softwareversies en de huidige patch niveaus van elke component.	n/a**
5.2	**Bepaal de afhankelijkheid van OT-bedrijfsmiddelen:** Breng per OT-bedrijfsmiddel in kaart hoe afhankelijk de organisatie hiervan is en wat de risico's zijn bij uitval.	n/a
5.4	**Configuratie en operationele parameter back-up :** Deze back-ups zijn van vitaal belang. Ze helpen bij het snel herstellen van systemen na technische problemen of cyberaanvallen, waardoor lange stilstand wordt voorkomen en de bedrijfscontinuïteit gewaarborgd blijft.	n/a
5.5	**Recovery plan:** Stel een herstelplan op en voer periodieke tests uit. Indien daadwerkelijke testen niet haalbaar zijn, voer dan een zogenaamde droogoefening uit. Simuleer het herstelproces door het plan te volgen en zorg ervoor dat de benodigde middelen (zoals configuraties, documentatie en reserveonderdelen) en betrokken personen (inclusief externe partijen) beschikbaar zijn of zouden zijn geweest.	n/a
5.11	**Weten welke versies/revisies van OT-apparatuur en welke leverancier daarbij hoort:** Het accuraat bijhouden van deze gegevens draagt bij aan de organisatorische capaciteit om adequaat te reageren op beveiligingskwesties, updates efficiënt door te voeren en onderhoudsplanning te optimaliseren.	n/a
IT-beheersmaatregelen		
6.1	**Broncode bescherming (versiebeheer en toegang) van software (ontwikkeling):** Bescherm de broncode van software door middel van strikt versiebeheer en gedegen toegangscontrolemechanismen. Op deze wijze wordt de integriteit en veiligheid van uw softwaretoepassingen gehandhaafd en gewaarborgd.	8.4
6.3	**Gebruik van recommendations (volgen architectuurrichtlijnen & richtlijnen van OWASP):** Om informatieveiligheid te waarborgen is het belangrijk om altijd architectuurrichtlijnen en OWASP te volgen bij het ontwikkelen van software.	8.27
6.9	**Alle geleverde programmatuur exact in kaart (welke klant heeft welke software en versies):** Verkrijg inzicht in de gebruikte software en versienummers door klanten, om zo het onderhoud en de updates adequaat te kunnen plannen en een effectief licentiebeheer te kunnen handhaven.	n/a
6.12	**Voorbereid zijn om verbeteringen eenvoudig te installeren (plan hoe te gaan releasen en patchen bij klanten):** Vereenvoudig de implementatie van nieuwe versies en patches door een gestandaardiseerd stappenplan te volgen, bestaande uit identificatie, communicatie en distributie.	n/a

**Mapping: Deze norm is vergelijkbaar, maar niet identiek aan ISO27001. Elk normeringsstelsel heeft zijn eigen specifieke kenmerken.*
*** 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