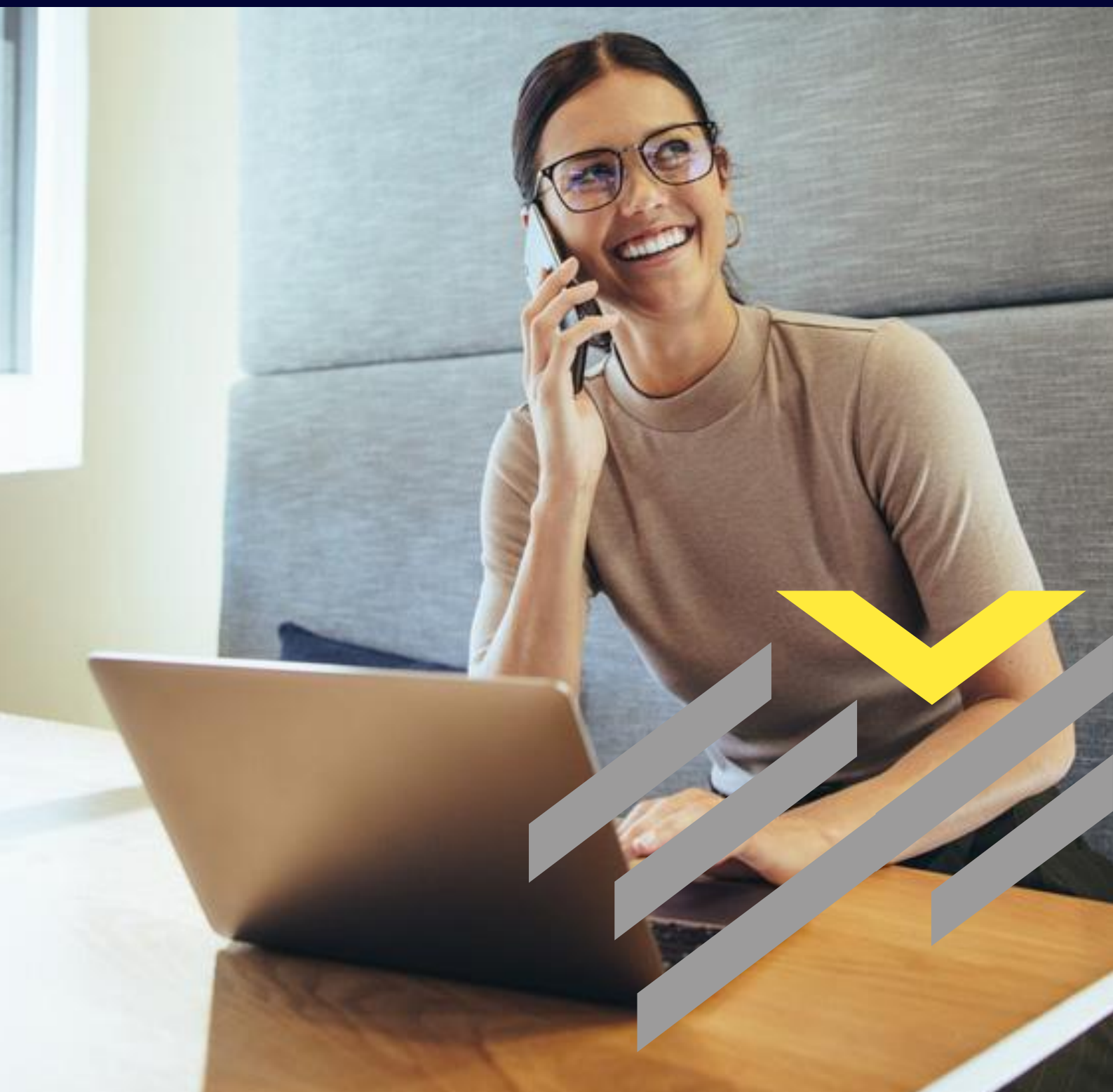
NIS2 Quality Mark

NIS2-QM10 BASIC

Versie 3.0
16 oktober 2024

NIS2 QUALITY MARK



Inhoud

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
Versie 3.0 © 2024

Er zijn meer normen gericht op het vergroten van de cyberweerbaarheid. Om daarin de weg te wijzen en mogelijk dubbel werk te voorkomen, wordt bij elke norm een mapping indication meegegeven, zodat de lezer ziet hoe elk onderdeel van de norm zich mogelijk verhoudt tot andere gezagvolle normen in Europa, in het bijzonder de ISO-norm 27001.

***Mapping indication:** De maatregel toont gelijkenis met een andere norm, maar kan niet als volledig identiek worden beschouwd. Het dient als hulpmiddel bij het identificeren van overlappende gebieden, zonder de unieke kenmerken van de normen te verliezen.*

Voor wat betreft de maatregelen uit de ISO-norm 27001: de 'A' waarnaar wordt verwezen betreft de nummering uit bijlage A van de 27001 norm. Deze is leidend voor 27001.

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.

Doel

Voorkomen dat er informatiebeveiligingsincidenten optreden doordat medewerkers te weinig urgentie voelen en kaders meekrijgen voor het beschermen van de beschikbaarheid, integriteit en vertrouwelijkheid van informatie tegen cyberdreigingen.

Focuspunten

- Ontwikkel een gedetailleerd informatiebeveiligingsbeleid dat standaardpraktijken en procedures omvat. Dit beleid moet formeel goedgekeurd worden door het management en gedeeld worden met alle betrokkenen.
- Zorg voor regelmatige updates, wachtwoordwijzigingen, installatiebeheer, toegangsbeperkingen en data-back-ups. Deze praktijken ondersteunen de proactieve beveiliging tegen incidenten en dreigingen.
- Definieer duidelijk wie verantwoordelijk is voor het initiëren en beslissen over cybersecuritymaatregelen. Formele bestuurlijke goedkeuring van het beleid is essentieel voor de naleving en implementatie.
- Het beleid moet regelmatig gecontroleerd en bijgesteld worden, vooral bij belangrijke veranderingen in de organisatie of de externe dreigingsomgeving. Dit garandeert voortdurende effectiviteit en relevantie.

Mapping indication

ISO 27001: A.5.1
IEC 62443-2-1: 2010, Clause 4.2.2, 4.2.3.6
NIST SP 800-53: PL-1 - Policy and procedures

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.

Doel

Voorkomen dat er informatiebeveiligingsincidenten optreden doordat noodzakelijke acties niet, niet goed, of niet op tijd worden uitgevoerd, door onduidelijkheden over verantwoordelijkheden.

Focuspunten

- Definieer en wijs duidelijke rollen en verantwoordelijkheden toe voor informatiebeveiliging aan alle medewerkers. Dit helpt bij het waarborgen van een gecoördineerde en consistente aanpak van beveiligingspraktijken binnen de organisatie. Er moet een specifieke persoon zijn die verantwoordelijk is voor de algehele informatiebeveiliging.
- Documenteer en communiceer de rollen en verantwoordelijkheden voor informatiebeveiliging naar alle medewerkers. Dit zorgt voor duidelijkheid en helpt medewerkers hun taken en verantwoordelijkheden beter te begrijpen. Training en ondersteuning moeten beschikbaar zijn om ervoor te zorgen dat medewerkers effectief kunnen bijdragen aan de informatiebeveiliging.
- Evalueer en herzie regelmatig de toegewezen rollen en verantwoordelijkheden om ervoor te zorgen dat deze blijven aansluiten bij de veranderende behoeften en risico's van de organisatie. Dit omvat het aanpassen van verantwoordelijkheden bij veranderingen in de organisatie of technologie en het continu informeren van medewerkers over hun rol in de informatiebeveiliging.

Mapping indication

ISO 27001: A.5.2
CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 17
IEC 62443-2-1:2010, Clause 4.3.2.3.3
NIST SP 800-53: PM-1 - Information security program plan

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.

Doel

Voorkomen dat er informatiebeveiligingsincidenten optreden doordat informatie niet is geïdentificeerd en geen eigenaar heeft, en daardoor onvoldoende wordt beschermd.

Focuspunten

- Inventariseer alle informatiegegevens binnen de organisatie, zoals klantgegevens, contracten en financiële administratie. Dit overzicht helpt bij het identificeren en effectief beveiligen van alle informatie.
- Stel een informatieregister op dat alle soorten informatie, inclusief opslaglocaties, vormen (digitaal of op papier) en bewaartermijnen, bevat. Dit register moet compleet, correct en actueel zijn.
- Wijs eigenaren/beheerders aan voor specifieke informatiecategorieën in het register. Deze personen zijn verantwoordelijk voor het beheer en de beveiliging van hun toegewezen informatie.
- Controleer en actualiseer het informatieregister regelmatig om ervoor te zorgen dat het volledig en up-to-date blijft. Dit garandeert dat de informatie correct beheerd en beschermd wordt.

Mapping indication

ISO 27001: A.5.9
CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 2
IEC 62443-2-1:2010, Clause 4.2.3.4 IEC 62443-3-3:2013 SR 7.8

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.

Doel

Voorkomen dat er informatiebeveiligingsincidenten optreden doordat bepaalde ICT-bedrijfsmiddelen niet geïdentificeerd zijn en geen eigenaar hebben, en daardoor onvoldoende worden beschermd.

Focuspunten

- Inventariseer alle ICT-bedrijfsmiddelen binnen de organisatie, zoals computers, servers, dataopslagsystemen en firewalls. Dit overzicht helpt bij het effectief beheren en beveiligen van alle ICT-middelen.
- Stel een inventarislijst op waarin alle ICT-bedrijfsmiddelen, inclusief hun locaties, omschrijvingen en datum van aanschaf, zijn opgenomen. Zorg ervoor dat deze lijst volledig, correct en actueel is.
- Wijs eigenaren/beheerders aan voor elk ICT-bedrijfsmiddel op de inventarislijst. Deze personen zijn verantwoordelijk voor het beheer, de beveiliging en het onderhoud van hun toegewezen ICT-middelen.
- Controleer en actualiseer de inventarislijst regelmatig om ervoor te zorgen dat deze altijd up-to-date is. Dit garandeert een betrouwbare basis voor het beheer en het veilig houden van ICT-bedrijfsmiddelen.

Mapping indication

ISO 27001: A.5.9
CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 2
IEC 62443-2-1:2010, Clause 4.2.3.4 IEC 62443-3-3:2013 SR 7.8

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.

Doel

Voorkomen dat er een informatiebeveiligingsincident optreedt doordat een bedrijfsmiddel na na het aflopen of aanpassen van een arbeidsovereenkomst in verkeerde handen valt of onveilig wordt gebruikt.

Focuspunten

- Inventariseer alle bedrijfsmiddelen die medewerkers gebruiken, zoals computers, smartphones en andere apparatuur. Dit helpt bij het beheren en terugvorderen van bedrijfsmiddelen wanneer een medewerker de organisatie verlaat.
- Stel een duidelijke procedure en checklist op voor het inleveren van bedrijfsmiddelen bij vertrek van een medewerker. Deze procedure moet stapsgewijs beschrijven wat er moet gebeuren om ervoor te zorgen dat alle middelen correct worden teruggegeven.
- Wijs een verantwoordelijke persoon of afdeling aan die toeziet op het inleverproces. Deze persoon of afdeling zorgt ervoor dat de procedure wordt gevolgd en dat alle bedrijfsmiddelen daadwerkelijk worden ingeleverd.
- Controleer en actualiseer de procedure en checklist regelmatig om ervoor te zorgen dat deze up-to-date blijft en aansluit bij de huidige bedrijfspraktijken en technologieën. Dit garandeert een effectief inleverproces en helpt bij het waarborgen van de informatiebeveiliging.

Mapping indication

ISO 27001: A.5.11

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.

Doel

Voorkomen dat er een informatiebeveiligingsincident optreedt doordat toegangsrechten onterecht of onjuist zijn toegewezen aan het account van een gebruiker.

Focuspunten

- Registreer wie toegang heeft tot welke informatie en bedrijfsmiddelen, en definieer zowel logische als fysieke toegangsrechten. Dit helpt bij het beheersen en controleren van toegangsrechten binnen de organisatie.
- Stel een procedure en checklist op voor het toekennen, wijzigen en intrekken van toegangsrechten. Dit zorgt ervoor dat toegangsrechten op een gestructureerde en consistente manier worden beheerd.
- Controleer bij beëindiging van een dienstverband of alle accounts correct worden afgesloten en alle toegangsrechten worden ingetrokken. Dit voorkomt ongeoorloofde toegang na vertrek van een medewerker.
- Stel een autorisatiematrix op die duidelijk maakt welke toegangsrechten bij welke rol horen. Evalueer en actualiseer regelmatig de autorisatiematrix om ervoor te zorgen dat deze up-to-date blijft en aansluit bij de huidige rollen en verantwoordelijkheden binnen de organisatie. Dit garandeert dat de toegangsrechten altijd correct en relevant zijn.

Mapping indication

ISO 27001: A.5.18
NIST SP 800-53: AC-2 - Account Management.

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.

Doel

Voorkomen dat bij een verstoring de hersteltijden en het dataverlies van essentiële informatiesystemen onvoldoende aansluiten bij bedrijfscontinuïteitsdoelstellingen van de organisatie.

Focuspunten

- Stel doelstellingen en continuïteitseisen op voor bedrijfscontinuïteit bij gebeurtenissen onverwachte, zoals cyberaanvallen. Dit helpt om snel weer operationeel te zijn en de impact op de bedrijfsvoering te minimaliseren.
- Ontwikkel een gedetailleerd plan voor bedrijfscontinuïteit dat onder andere back-upbeheer, noodvoorzieningen en crisisbeheer omvat. Dit plan moet duidelijk beschrijven hoe de organisatie haar activiteiten kan voortzetten tijdens en na een incident.
- Implementeer en onderhoud de ICT-gereedheid op basis van de vastgestelde doelstellingen en continuïteitseisen. Dit zorgt ervoor dat de technische infrastructuur klaar is om te reageren op verstoringen.
- Test de ICT-gereedheid regelmatig om ervoor te zorgen dat alle systemen en procedures effectief werken tijdens een incident. Dit garandeert dat de organisatie snel en efficiënt kan herstellen van onvoorziene gebeurtenissen.

Mapping indication

ISO 27001: A.5.30
NIST SP 800-53: CP-2 - Contingency Plan.

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.

Doel

Voorkomen dat er een informatiebeveiligingsincident optreedt als gevolg van het gebruik van een ondeugdelijke dienst of product van leveranciers, of van leveranciers dieper in de toeleveringsketen.

Focuspunten

- Inventariseer de risico's bij je belangrijkste leveranciers om te begrijpen welke bedreigingen er zijn voor jouw organisatie. Dit helpt bij het identificeren van zwakke punten in de toeleveringsketen.
- Maak gezamenlijke afspraken met leveranciers over digitale beveiliging. Dit zorgt ervoor dat alle partijen dezelfde normen en procedures volgen om cyberdreigingen te minimaliseren.
- Informeer ontvangers (personen of organisaties) tijdig over de beheersmaatregelen die ze kunnen nemen bij een significante cyberdreiging in de organisatie. Dit zorgt voor een gecoördineerde en effectieve reactie op mogelijke bedreigingen.
- Evalueer en actualiseer regelmatig de risico-inventarisatie en de gemaakte afspraken met leveranciers. Dit garandeert dat de beveiligingsmaatregelen up-to-date blijven en effectief zijn tegen nieuwe dreigingen.

Mapping indication

ISO 27001: A.5.21

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.

Doel

Voorkomen dat er informatiebeveiligingsincidenten optreden door een gebrek aan bewustzijn van informatiebeveiligingsrisico's, of door een gebrek aan kennis over regels en procedures van de organisatie.

Focuspunten

- Zorg dat directie en bestuurders een opleiding of cursus volgen om cyberbeveiligingsrisico's te kunnen identificeren en beoordelen. Dit versterkt hun vermogen om passende beveiligingsmaatregelen te nemen en een veilige informatieomgeving te waarborgen.
- Implementeer video-trainingsmodules en andere vormen van educatie voor medewerkers over digitale veiligheid. Dit zorgt ervoor dat alle medewerkers zich bewust zijn van de risico's van informatieverwerking en weten hoe ze deze kunnen minimaliseren.
- Organiseer opleidingen die zijn afgestemd op de specifieke functies binnen de organisatie. Hierdoor krijgt elke medewerker de juiste kennis en vaardigheden die nodig zijn voor hun rol in het beschermen van informatie.
- Test regelmatig de kennis van medewerkers en hun naleving van het beleid. Dit helpt om de opgedane kennis effectief toe te passen en dat medewerkers zich houden aan de vastgestelde beveiligingsrichtlijnen.

Mapping indication

ISO 27001: A.6.3
CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 14, 16
IEC 62443-2-1:2010, Clause 4.3.2.4.2
NIST SP 800-53: AT-3 – Role based training

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.

Doel

Voorkomen dat er informatiebeveiligingsincidenten optreden doordat medewerkers informatie op een onveilige manier openen, verwerken of opslaan tijdens werken op externe locaties.

Focuspunten

- Stel duidelijke regels op voor veilige informatieverwerking buiten de fysieke bedrijfslocatie, zoals thuis of op externe locaties. Dit helpt om gevoelige gegevens te beschermen tegen cyberincidenten.
- Implementeer beveiligingsmaatregelen specifiek gericht op thuis- en hybride werken, zoals het gebruik van VPN's, encryptie en sterke wachtwoorden. Dit zorgt ervoor dat gegevens veilig blijven, ongeacht waar medewerkers zich bevinden.
- Zorg ervoor dat alle medewerkers op de hoogte zijn van de regels en beveiligingsmaatregelen voor werken op afstand. Dit kan door middel van trainingen en regelmatige communicatie over de laatste veiligheidsrichtlijnen.
- Controleer en actualiseer regelmatig de beveiligingsmaatregelen en richtlijnen voor thuis- en hybride werken. Dit garandeert dat de maatregelen effectief blijven en inspelen op nieuwe cyberdreigingen.

Mapping indication

ISO 27001: A.6.7
CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 5, 6, 13
IEC 62443-2-1:2010, Clause 4.3.3.6.6, 4.3.3.7.4
IEC 62443-3-3:2013, SR 1.1, SR 1.13, SR 2.6
NIST SP 800-53: AC-17 - Remote Access.

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.

Doel

Voorkomen dat potentiële informatiebeveiligingsincidenten niet tijdig opgepakt of voorkomen kunnen worden doordat medewerkers waargenomen of vermoede informatiebeveiligingsgebeurtenissen niet of te laat melden.

Focuspunten

- Zorg voor een duidelijke en eenvoudige procedure voor het melden van cyberincidenten, zodat medewerkers snel en effectief bedreigingen voor de informatieveiligheid kunnen rapporteren.
- Maak afspraken over de kanalen die gebruikt moeten worden voor meldingen, zoals e-mail, WhatsApp en telefonie, om een snelle en betrouwbare respons te garanderen.
- Overweeg het gebruik van een digitaal meldsysteem of een specifieke app voor uitgebreidere en gedetailleerde rapportage van cyberincidenten. Dit kan helpen bij het systematisch vastleggen en opvolgen van meldingen.
- Zorg ervoor dat er een centraal meldpunt is binnen de organisatie, zoals de servicedesk of het IT-team, dat verantwoordelijk is voor het ontvangen en behandelen van meldingen over informatiebeveiligingsincidenten.

Mapping indication

ISO 27001: A.6.8
IEC 62443-2-1:2010, Clause 4.3.4.5.9 IEC 62443-3-3:2013, SR 6.1
NIST SP 800-53: IR-6 - Incident Reporting.

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.

Doel

Voorkomen dat er informatiebeveiligingsincidenten optreden doordat personen onnodig toegang hebben tot bepaalde informatie of andere bedrijfsmiddelen.

Focuspunten

- Stel duidelijke toegangsregels op die bepalen wie toegang heeft tot welke gevoelige informatie en bedrijfsmiddelen. Dit helpt om ongeautoriseerde toegang te voorkomen en de beveiliging te waarborgen.
- Stel een autorisatiematrix op die duidelijk maakt welke toegangsrechten bij welke rol horen. Evalueer en actualiseer regelmatig de autorisatiematrix om ervoor te zorgen dat deze up-to-date blijft en aansluit bij de huidige rollen en verantwoordelijkheden binnen de organisatie. Dit garandeert dat de toegangsrechten altijd correct en relevant zijn.
- Registreer en monitor de toegang tot gevoelige bedrijfsmiddelen, zodat je weet wie wanneer toegang heeft gehad. Dit zorgt voor een gedetailleerd overzicht en helpt bij het opsporen van ongeautoriseerde toegang.
- Evalueer en actualiseer regelmatig de toegangsregels en beveiligingsmaatregelen om ervoor te zorgen dat ze effectief blijven en aansluiten bij de veranderende bedrijfsbehoeften en dreigingslandschap.

Mapping indication

ISO 27001: A.5.15
CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 3, 4, 6, 7, 12, 13, 16
IEC 62443-2-1:2010, Clause 4.3.3.7.3
IEC 62443-3-3:2013, SR 2.1
NIST SP 800-53: AC-3 – Access enforcement.

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.

Doel

Voorkomen dat er een informatiebeveiligingsincident optreedt doordat een gebruikersapparaat onvoldoende beveiligd is, of doordat het bedrijfsnetwerk onvoldoende beveiligd is tegen onveilige gebruikersapparaten.

Focuspunten

- Stel een actuele lijst op van alle gebruikersapparaten binnen de organisatie en zorg voor continu toezicht op de beveiligingsconfiguraties. Dit helpt om altijd een stap voor te blijven op potentiële dreigingen en ervoor te zorgen dat de apparaten zo veilig mogelijk zijn.
- Implementeer maatregelen zoals laptopversleuteling, beperking van adminrechten en verplichting van sterke wachtwoorden en pincodes. Dit zorgt ervoor dat medewerkersapparaten goed beveiligd zijn tegen cyberincidenten.
- Communiceer duidelijke regels en beveiligingseisen voor het gebruik van gebruikersapparaten naar alle medewerkers. Zorg dat iedereen op de hoogte is van de procedures voor het beschermen van hun apparaten en de risico's van ongeautoriseerde toegang.
- Beheer en update regelmatig de beveiligingsinstellingen van alle apparaten, inclusief het installeren van software-updates en handhaven van beveiligingsprotocollen. Dit garandeert dat de apparaten altijd goed beschermd zijn tegen nieuwe dreigingen.

Mapping indication

ISO 27001: 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.

Doel

Voorkomen dat er een informatiebeveiligingsincident optreedt doordat malware leidt tot een aantasting van de beschikbaarheid, integriteit of vertrouwelijkheid van informatie.

Focuspunten

- Installeer en onderhoud betrouwbare anti-malware software, virusscanners en spamfilters op alle systemen binnen de organisatie. Dit helpt om de digitale omgeving te beschermen tegen kwaadaardige software en ongewenste e-mails.
- Overweeg het gebruik van encryptie voor belangrijke documenten en gevoelige informatie. Dit zorgt ervoor dat zelfs bij ongeautoriseerde toegang, de informatie niet gelezen kan worden zonder de juiste encryptiesleutels.
- Train medewerkers regelmatig op het herkennen en voorkomen van malware-aanvallen. Dit verhoogt het bewustzijn van de risico's en zorgt ervoor dat iedereen binnen de organisatie weet hoe ze veilig moeten omgaan met digitale dreigingen.
- Zorg voor een beleid en procedure voor het bestrijden van malware, inclusief het regelmatig updaten van beveiligingssoftware en het uitvoeren van systeemscans. Dit garandeert dat de bescherming tegen malware up-to-date blijft en effectief is tegen nieuwe bedreigingen.

Mapping indication

ISO 27001: A.8.7
CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 8, 10, 13
IEC 62443-2-1:2010, Clause 4.3.4.3.8
IEC 62443-3-3:2013, SR 3.2
NIST SP 800-53: SI-3 - Malicious code protection.

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.

Doel

Voorkomen dat essentiële informatie permanent niet meer beschikbaar is als gevolg van een kwaadaardige aanval, een menselijke fout, een ramp of een andere oorzaak.

Focuspunten

- Stel een uitgebreid back-up beleid op volgens de 3-2-1 systematiek, waarbij je drie kopieën van de data bewaart op twee verschillende media, waarvan één kopie offsite. Dit garandeert dat de gegevens veilig en toegankelijk blijven bij een calamiteit.
- Maak regelmatig back-ups van alle belangrijke data en systemen, zoals klantgegevens, financiële administratie en databases. Dit zorgt ervoor dat er altijd een recente kopie beschikbaar is in geval van dataverlies.
- Test de back-ups periodiek op betrouwbaarheid om er zeker van te zijn dat ze correct werken en dat de data teruggezet kan worden indien nodig. Dit voorkomt verrassingen op het moment dat een herstel noodzakelijk is.
- Communiceer duidelijk de verantwoordelijkheden binnen het back-up proces, inclusief wie verantwoordelijk is voor het uitvoeren, monitoren en testen van de back-ups. Dit zorgt voor een gestructureerde aanpak en voorkomt dataverlies door menselijke fouten.

Mapping indication

ISO 27001: A.8.13
CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 11
IEC 62443-2-1:2010, Clause 4.3.4.3.9
IEC 62443-3-3:2013, SR 7.3, SR 7.4
NIST SP 800-53: CP-9 – System backup

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.

Doel

Voorkomen dat er een informatiebeveiligingsincident optreedt als gevolg van een niet gerepareerde kwetsbaarheid in software.

Focuspunten

- Implementeer procedures voor het automatisch updaten van software op alle computers en apparaten. Dit zorgt ervoor dat updates zo snel mogelijk worden geïnstalleerd zonder dat medewerkers handmatig actie hoeven te ondernemen.
- Stel richtlijnen op voor het veilig updaten van software, inclusief de frequentie en methoden voor het installeren van updates. Dit helpt om systemen te beschermen tegen nieuwe bedreigingen en kwetsbaarheden.
- Communiceer het belang van regelmatige software-updates aan alle medewerkers en zorg ervoor dat zij op de hoogte zijn van de procedures. Dit bevordert naleving en zorgt ervoor dat alle apparaten up-to-date blijven.
- Werk samen met externe leveranciers voor het updaten van operationele systemen indien nodig, en zorg ervoor dat de integriteit en werking van de systemen gewaarborgd blijft. Dit kan de efficiëntie verbeteren en ervoor zorgen dat updates correct en tijdig worden uitgevoerd.

Mapping indication

ISO 27001: A.8.19
CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 1, 7, 4, 12
IEC 62443-2-1:2010, Clause 4.3.4.3.2, 4.3.4.3.3
IEC 62443-3-3:2013, SR 7.6

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.

Doel

Voorkomen dat er een informatiebeveiligingsincident optreedt doordat er bij het inloggen gebruik wordt gemaakt van een onveilige authenticatiemethode.

Focuspunten

- Implementeer multifactor-authenticatie (MFA) voor alle accounts met beheerdersrechten en toegang tot systemen met bedrijfsgevoelige informatie. Dit zorgt voor een extra beveiligingslaag die ongeautoriseerde toegang moeilijker maakt.
- Gebruik authenticatiemethoden die passen bij de gevoeligheid van de informatie en systemen die worden benaderd. Voorzie cruciale systemen altijd van MFA of continue-authenticatieoplossingen om de beveiliging te versterken.
- Zorg dat gebruikers die via het internet inloggen ook MFA gebruiken. Dit beschermt de systemen tegen aanvallen waarbij wachtwoorden mogelijk zijn gecompromitteerd.
- Beveilig communicatiekanalen zoals spraak-, video- en tekstcommunicatie met veilige protocollen. Zorg ervoor dat noodcommunicatiesystemen ook goed beveiligd zijn om betrouwbare communicatie tijdens incidenten te garanderen.

Mapping indication

ISO 27001: A.8.5
CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 5, 6, 13
IEC 62443-2-1:2010, Clause 4.3.3.6.6, 4.3.3.7.4
IEC 62443-3-3:2013, SR 1.1, SR 1.13, SR 2.6
NIST SP 800-53: IA-2 - Identification and authentication (organizational users).

Copyright

Toelichting op Mapping indication

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