TLP:GREEN

IR-3 IB-BELEID VOORBEELDUITWERKING

Incident Response - Incident Response Readiness

Best Practice versie 1.2

Complexiteit document

Eenvoudig

Samenwerken maakt

DIGITAAL VEILIGER

VSSR

Inhoudsopgave

Voorwoord

De Rijksoverheid verwerkt grote hoeveelheden gevoelige informatie en is daarmee een interessant en gewild doelwit. Cybercriminelen en statelijke actoren zoeken naar kwetsbaarheden om zich zo toegang te verschaffen tot de supply chain, netwerken, systemen en (gevoelige) informatie. Daarnaast hebben moderne organisaties die veel informatie verwerken een grote afhankelijkheid van digitalisering. Dat maakt dat deze organisaties kwetsbaar zijn voor verstoringen in de keten.

Om de gevolgen van cyberincidenten te beperken, is het van belang om Incident Response ingericht te hebben. Incident Response gaat over het vermogen, de processen, tools en technologieën van een organisatie die nodig zijn om te reageren op cyberdreigingen, -incidenten of -aanvallen. Het doel van Incident Response is dat de bedrijfsvoering zo min mogelijk wordt verstoord tijdens een cyberincident.

Incident Response gericht op cyberincidenten kent een aantal specifieke kenmerken en processtappen ten opzichte van regulier incidentmanagement. Regulier incidentmanagement richt zich primair op gebruikerservaring en het zo snel mogelijk oplossen van storingen om tot een optimale gebruikersbeleving te komen. Incident Response in de context van cyberincidenten richt zich op bedrijfsprocessen als geheel en het voorkomen van (verdere) schade. Incident Response in de context van cyberincidenten geeft daarom ook veel aandacht aan risicobeperkende maatregelen die uitbreiding van het beveiligingsincident – en daarmee vervolgschade - voorkomen. Deze elementen zijn in regulier incidentmanagement vaak niet of onvoldoende aanwezig.

Het programma Versterken SOC Stelsel Rijk heeft diverse producten ontwikkeld die organisaties kunnen gebruiken bij het inrichten c.q. optimaliseren van Incident Response. Dit document bevat handvatten waarmee een organisatie stapsgewijs het Incident Response kan inrichten c.q. optimaliseren.

Achtergrond

VSSR levert verschillende kennisproducten die aansluiten bij de SOC Readiness Quickscan. Dit document maakt onderdeel uit van een tiental miniproducten die rijksorganisaties helpt om een aantal operationele randvoorwaarden in te richten.

Doelgroep

Versterken SOC Stelsel Rijk (VSSR) biedt met dit document handvatten voor IT-management, IT auditor, (Security) Incidentmanager, Informatie Security Manager, CISO, Security vertegenwoordigers en functionarissen betrokken bij informatiebeveiliging.

1 Documentgegevens

1.1 Documenthistorie

Versie	Datum	Omschrijving
V1.0	28-05-2025	Initiële versie
V1.1	20-06-2025	Bijlage II vervangen door verwijzing naar SOC Security Policy Template (link)
V1.2	29-6-2026	Referenties geactualiseerd

1.2 Referenties

Document	Link
Incident Response – IB Beleid Checklist	Zie "IR-3, Incident Response – IB Beleid Checklist (pdf)" onder Incident Response Readiness
Incident Response – Policy template	Zie "IR-3, Incident Response – Policy Template (word)" onder Incident Response Readiness
SOC Security Policies & template	SOC Security Policies (met Word Policy template)
Incident Response Readiness miniproducten	Zie Incident Response Readiness op het VSSR-portaal
Baseline Informatiebeveiliging Overheid v1.04zv	https://bio-overheid.nl/media/13kduqsi/bio-versie-104zv_def.pdf
NIST-CSF 2.0	https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf
Besluit CIO-stelsel Rijksdienst 2021	https://wetten.overheid.nl/BWBR0044613/2021-01-01
Woordenboek Cyberveilig Nederland	Woordenboek - Cyberveilig Nederland
VSSR-kennisdocumenten	VSSR (ncsc.nl)

1.3 Definities

Definitie	Toelichting
Tabletop oefening	Een tabletop oefening is een gesimuleerde situatie (incident) dat in een vergaderruimte of online setting wordt besproken. De deelnemers reageren (response) op een fictief incident alsof het echt gebeurt.

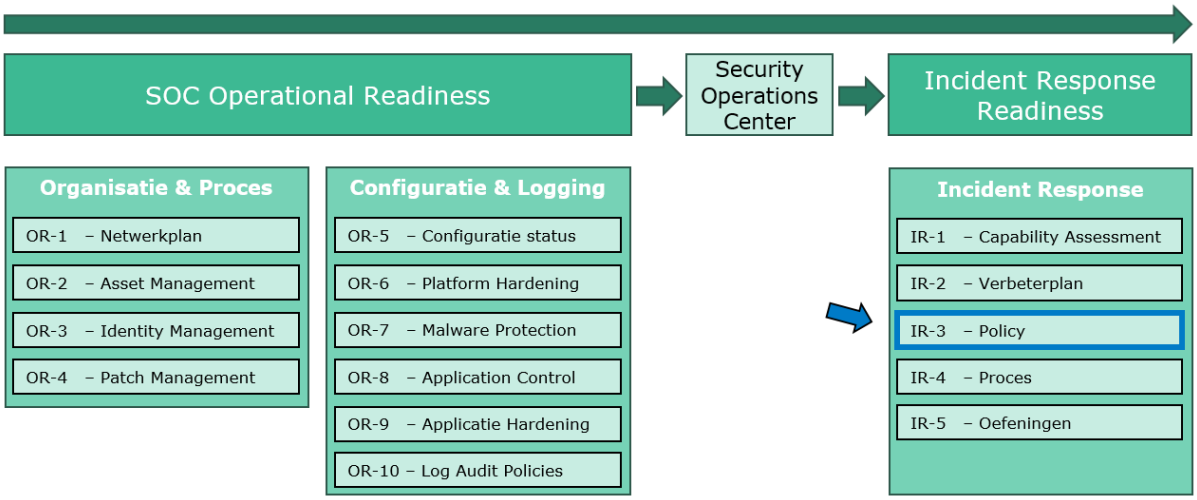
Ter verduidelijking van de terminologie en begrippen die in dit document worden gebruikt is er een verzameling van definities te vinden op Woordenboek - Cyberveilig Nederland.

2 Context miniproducten

Dit document maakt onderdeel uit van de Incident Response Readiness miniproducten. De Incident Response Readiness miniproducten ondersteunen uw organisatie bij de voorbereidingen die nodig zijn voor het optimaal benutten van een SOC(-dienst). We speken over miniproducten omdat de producten compact en overzichtelijk zijn waardoor organisaties in korte tijd en met behapbare hoeveelheden werk progressie kunnen maken. De producten hebben een samenhangende opbouw maar kunnen ook los van elkaar worden gebruikt. De producten zijn in drie groepen te verdelen:

1) **Organisatie & Proces:** Helpt bij het inrichten van processen met als doel het SOC van de juiste informatie te voorzien om goed te kunnen monitoren.
2) **Configuratie & Logging:** Helpt bij het inrichten van basisbeveiliging met als doel om beter beschermd te zijn en de juiste logdata bij een SOC aan te kunnen leveren.
3) **Incident Response:** Met behulp van monitoring & Detectie zal een SOC security melding genereren. De Incident Response producten helpen bij het inrichten van de opvolging van deze meldingen binnen uw organisatie.

Onderstaande weergave toont dit document als onderdeel van **Incident Response** in het VSSR-minipoducten raamwerk.



Figuur 1: Dit document als onderdeel van het VSSR-miniproducten raamwerk

De documenten onder IR-3 beleid/Policy bestaan uit:

- IB-Beleid Checklist
  PDF document met overzicht van de belangrijkste richtlijnen voor het opstellen van beveiligingsincident- & responsebeleid.

- IB Beleid voorbeelduitwerking (**Dit document**)
  PDF document met voorbeelduitwerking IB Beleid

    - Bijlage I Incidente Response Policy (Template)

3 Leeswijzer

Dit document ondersteunt organisaties bij het opstellen, toetsen of actualiseren van beleid voor beveiligingsincident- en responsemanagement. De inhoud is gebaseerd op relevante kaders zoals de BIO en de NIS2-richtlijn. Deze leeswijzer helpt je om het document efficiënt en doelgericht te gebruiken.

3.1 Voorbereiding

Voordat je dit document gebruikt:

- Zorg dat het IR1 – Capability Assessment is uitgevoerd, ten minste voor het thema 'Beleid';
- Gebruik eventueel het document IR3 – IB Beleid Checklist om overzicht te houden van welke beleidsonderwerpen al zijn uitgewerkt of nog ontwikkeld moeten worden.

3.2 Het doel van dit document

Dit document helpt je bij:

- het opstellen van een nieuw incident response beleid;
- het toetsen van bestaand beleid op volledigheid;
- het structureren van beleid in lijn met wet- en regelgeving (BIO/NIS2);
- het koppelen van beleid aan bijbehorende procedures, rollen en plannen;
- het benutten van een concreet beleidsvoorbeeld dat aangepast kan worden aan de eigen organisatiecontext.

3.3 Structuur van dit document

Het document bestaat uit de volgende onderdelen:

- Hoofdstuk 1 t/m 3: Algemene informatie en context
- Hoofdstuk 4: Beleidsuitwerking per beleidselement

  Elk element is volgens een vaste structuur uitgewerkt, inclusief de relatie met de BIO- en NIS2-kaders. Hierdoor is snel zichtbaar aan welke wettelijke eisen wordt voldaan. Daarnaast bevat elk onderdeel een voorbeeldtekst die gebruikt kan worden bij het opstellen van het beleidsdocument.
- Bijlage 1: Voorbeeldbeleidsdocument (Word document)

  Deze bijlage bundelt alle voorbeeldteksten uit hoofdstuk 4 tot een volledig beleidsdocument, inclusief de basiselementen van een incident response policy.

3.4 Gebruik van dit document

Bij het opstellen van nieuw beleid kun je direct beginnen bij hoofdstuk 4. Werk per beleidselement aan de hand van de toelichtingen en voorbeeldteksten.

Je kunt:

- De voorbeeldteksten gebruiken uit bijlage 1 om sneller tot een volledige tekst te komen;
- Of gebruikmaken van bijlage 2 als je een eigen opbouw of werksessie wilt faciliteren.

Het is niet vereist om elk element volledig uit te werken in het informatiebeveiligingsbeleid. In sommige gevallen is een verwijzing naar bestaand beleid voldoende. Beschikt je organisatie bijvoorbeeld al over een ethisch beleid? Dan volstaat een verwijzing daarnaar in plaats van herhaling.

4 Incidentmanagement & -response beleidsuitwerking

Dit document biedt een voorbeelduitwerking van een incidentmanagement & -response beleidsplan. De doelstelling hierbij is dat organisaties die dit plan nog niet hebben geïmplementeerd, dit voorbeeld voor ca. 80% kunnen overnemen, en het voor ca. 20% kunnen verbijzonderen naar hun eigen specifieke wensen. Bij dit document behoort het document IR-3 "IB-beleid Checklist" met de minimaal op te nemen elementen voor beleid, hetgeen als startpunt kan dienen voor het opstellen van dit beleidsplan. In de volgende hoofdstukken worden deze elementen benoemd en voorzien van toelichtingen over wat er in de tekst moet worden opgenomen. Daarnaast wordt er een voorbeeldtekst gegeven die door de organisatie kan worden aangevuld en aangepast aan de eigen specifieke situatie.

4.1 Doel, Reikwijdte en Referenties

Beleidselement	Doel	Omschrijving
Doel, Scope en verwijzingen	Het vaststellen van het doel en de reikwijdte van het beleid. Aangeven hoe het beleidsdocument moet worden gepositioneerd in het algemene beleidskader.	Beschrijving van het doel van de Incident Management policy en de scope (welke systemen, afdelingen en processen vallen onder de policy?) (BIO 5.1.1, 5.1.2) Een verwijzing naar bovenliggende beleidsdocumenten zoals ten minste het informatiebeveiligingsbeleid en het ethisch beleid van de organisatie. Tevens een verwijzing naar verplicht te beschrijven procesdocumenten die invulling moeten geven aan het gestelde beleid.

Tabel 1 – Doel, Reikwijdte en Referenties

Wat op te nemen:
In deze sectie wordt het doel en reikwijdte van het beleid gedefinieerd, inclusief een specificatie van systemen, afdelingen en processen. Ook bevat het verwijzingen naar overkoepelende beleidsstukken waaronder het Informatiebeveiligingsbeleid, Ethisch Beleid en naar verplichte procesdocumenten voor incidentafhandeling en rapportage.

Voorbeeldtekst:
"Dit beleid is bedoeld om te sturen op een proactieve aanpak voor het beheersen van beveiligingsincidenten die de beschikbaarheid, integriteit of vertrouwelijkheid van de organisatie kunnen beïnvloeden en op deze wijze negatieve gevolgen voor de organisatie te vermijden of beperken. Het beleid is van toepassing op alle werknemers, aannemers en externe dienstverleners die interactie hebben met de IT-systemen en gegevens van de organisatie. Het beslaat incidenten in alle systemen, afdelingen, processen, cyberaanvallen, gegevensverlies en pogingen tot ongeautoriseerde toegang. Dit beleid sluit aan bij het Informatiebeveiligingsbeleid (BIO 5.1.1 en 5.1.2) en het Ethisch Beleid, en volgt verplichte procesdocumenten voor incidentafhandeling en rapportage.

- *Voeg verwijzing toe naar Ethisch Beleid*
- *Voeg verwijzing toe naar procesdocumenten voor incidentafhandeling en rapportage"*

4.2 Definities en classificatie van incidenten

Beleidselement	Doel	Omschrijving
Definities en Classificatie van Incidenten	Duidelijkheid over wat als een security-incidenten wordt beschouwd en welke urgentie aan elk type security-incident wordt toegekend.	Duidelijke definitie van wat als security-incident wordt beschouwd en hoe deze een classificatie op basis van impact en urgentie krijgt. (BIO 16.1.4) (NIS 21b) De security-incidentdefinitie moet hier richtinggevend zijn en is dus algemeen van karakter. Hier moet ook aangegeven worden hoe die voor de verschillende IT-systemen nader moet worden gespecificeerd.

Tabel 2 – Definities en classificatie van incidenten

Wat op te nemen:
Deze sectie moet een duidelijke definitie geven van wat een beveiligingsincident is en beschrijven hoe deze op basis van hun impact en urgentie worden geclassificeerd.

Voorbeeldtekst:
"Een beveiligingsincident wordt gedefinieerd als elke gebeurtenis die de beschikbaarheid, integriteit of vertrouwelijkheid van de informatie-eigendommen van de organisatie bedreigt. Incidenten worden als volgt geclassificeerd:

- *Impact-bepaling:*
  - *Kritiek: Ernstige impact op bedrijfsvoering en gegevensbeveiliging en/of de organisatie is niet in staat om aan haar wettelijke taken en verplichtingen te voldoen.*
  - *Hoog: Aanzienlijke verstoring op bedrijfsvoering of gegevenscompromittering*
  - *Gemiddeld: Matige impact met beperkte gegevensblootstelling*
  - *Laag: Minimale impact op systemen of gegevens*

- *Urgentie-bepaling:*
  - *Hoog: Dit niveau van urgentie geeft aan dat er momenteel exploitatie plaatsvindt. Het incident heeft een directe en impact op de organisatie, waardoor onmiddellijke actie vereist is om verdere schade of verlies te voorkomen*
  - *Gemiddeld: verwachting van exploitatie op korte termijn. Hoewel er op dit moment geen actieve exploitatie is, zijn er aanwijzingen of kwetsbaarheden die suggereren dat een aanval waarschijnlijk is.*
  - *Laag: Dit niveau van urgentie duidt aan dat er geen indicaties zijn voor mogelijke exploitatie. De incidenten op dit niveau hebben een minimale impact op de organisatie en kunnen met minder urgentie worden behandeld.[1]"*

Opmerking:
Binnen deze policy moet specifiek worden ingegaan op de verschillende onderdelen van IT-diensten, met bijzondere aandacht voor configuratiebeheer en patchmanagement. Tabel 3 – Inschalingsmatrix kan worden gebruikt om de prioriteitscodes en de bijbehorende acties voor de verschillende prioriteiten in te vullen.

[1] *Classificatiecriteria zijn in overeenstemming met BIO 16.1.4 en NIS 21b standaarden.*

		Urgentie		
		Hoog	Gemiddeld	Laag
Impact	Kritiek	Prioriteit 1	Prioriteit 1	Prioriteit 3
	Hoog	Prioriteit 1	Prioriteit 2	Prioriteit 3
	Gemiddeld	Prioriteit 2	Prioriteit 3	Prioriteit 3
	Laag	Prioriteit 3	Prioriteit 3	Prioriteit 4

Toelichting: [Verwijs naar Annex [x] voor een gedetailleerde specificatie incl. acties per prioriteit]

Tabel 3 – Inschalingsmatrix

4.3 Incidentregistratie en -documentatie

Beleidselement	Doel	Omschrijving
Incidentregistratie en Documentatie	Het structureren van het proces van registratie en documentatie van incidenten.	Standaardprocedures voor het registreren en structureren van incidenten en de minimale vereisten voor documentatie (BIO 16.1.1) (NIS 21b)

Tabel 4 – Incidentregistratie en -documentatie

Wat op te nemen:
Deze sectie moet de standaardprocedures voor het vastleggen van beveiligingsincidenten beschrijven en de minimale documentatievereisten specificeren om traceerbaarheid en verantwoordelijkheid te waarborgen.

Voorbeeldtekst:
"Alle incidenten en beveiligingsincidenten moeten worden geregistreerd in het Incident Management Systeem (IMS), waarbij details worden vastgelegd zoals:

- *Classificatie als beveiligingsincidenten*
- *Datum en tijd van detectie.*
- *Beschrijving van het incident.*
- *Beoordeling van het risico*
- *Beoordeling van de urgentie*
- *Ondernomen acties en status van de oplossing/mitigerende maatregelen.*
- *Verantwoordelijke oplosgroep.[2]"*

[2] *Documentatie moet voldoen aan de normen zoals beschreven in BIO 16.1.1 en NIS 21b*

4.4 Incident handling- en escalatieproces

Beleidselement	Doel	Omschrijving
Incidentafhandeling en Escalatieproces	Het afhandelen en escaleren van incidenten volgens duidelijke stappen.	Gedetailleerde stappen voor het afhandelen van incidenten, inclusief technische en hiërarchische escalatieprocessen en verantwoordelijke rollen (BIO 16.1.1) (NIS 21b)

Tabel 5 – Incident handling- en escalatieproces

Wat op te nemen:
Deze sectie moet beschrijven welke stappen voor het afhandelen van incidenten minimaal aanwezig zijn. Voor elke stap zijn de technische en hiërarchische escalatieprocessen beschreven, inclusief de rollen die verantwoordelijk zijn.

Voorbeeldtekst:
"Incidentafhandeling omvat de volgende stappen:

- *Detectie en Identificatie: Het identificeren van de aard en omvang van het incident*
- *Registratie en verificatie: Validatie binnen de organisatie zelf.*
- *Triage en onderzoek: Het beoordelen van de impact en urgentie van het incident.*
- *Containment: Het isoleren van getroffen systemen om verdere schade te voorkomen.*
- *Oplossing: Het nemen van - al dan niet tijdelijke - maatregelen om het beveiligingsniveau van betreffende informatiesysteem op het vereiste niveau te brengen. (bijv. malwareverwijdering)*
- *Evaluatie: Het uitvoeren van een oorzaak-analyse.*

Escalatie naar hoger management of externe autoriteiten zal volgen volgens vooraf gedefinieerde protocollen. Deze protocollen worden vastgelegd en jaarlijks geëvalueerd en vastgesteld."

Incident handeling	**Actie**	**Technisch escalatie**	**Hiërarchische escalatie**
Detectie en identificatie	*Eerste niveau analyse en meldingen.*	2de lijn	*nvt*
Registratie en verificatie	*Validatie binnen de organisatie zelf.*	2de lijn	*nvt*
Triage en onderzoek	Bepaal de impact en urgentie en evalueer of escalatie naar technische experts nodig is	*2de lijn*	*nvt*
Containment	*Samenwerking met betrokken teams om verdere schade te minimaliseren; doorverwijzing naar senior responders indien nodig.*	*3de lijn / CSIRT*	*CISO*
Oplossing	*Maatregelen nemen om het vereiste niveau van beveiliging te herstellen*	*3de lijn / CSIRT*	*CISO/ hoger management*
Evaluatie	*Onderzoek naar de oorzaak en rapportage aan management*	*ISO*	*CISO/ hoger management*

Toelichting: [Verwijs naar Annex [x] voor een gedetailleerde specificatie per type escalatie].

Tabel 6 - Incident escalatieproces

4.5 Taakverdeling en verantwoordelijkheden

Beleidselement	Doel	Omschrijving
Taakverdeling en Verantwoordelijkheden	Duidelijkheid over wie welke rol en verantwoordelijkheid heeft.	Toewijzing van rollen binnen de incident response organisaties en de taken en verantwoordelijkheden van het incident response team (BIO 6.1.1). Belangrijk: de gedetailleerde uitwerking van rolverdeling en taakbeschrijving dient minimaal in de procesbeschrijving opgenomen te worden. In de policy volstaat een verwijzing naar de procesbeschrijving of een beschrijving op hoog niveau (rollen).

Tabel 7 – Taakvedeling en verantwoordelijkheden

Wat op te nemen:
Deze sectie moet de rollen binnen het incidentresponseteam definiëren en de taken, verantwoordelijkheden en bevoegdheden beschrijven die bij elke rol horen.

Voorbeeldtekst:
"Rollen en verantwoordelijkheden binnen het Incident Response Team (IRT) omvatten:

- *Security incident- en responsemanager: verantwoordelijk voor het end-to-end coördineren, beheren en leiden van de response op beveiligingsincidenten*
- *Security analist: Is een specialist die de oorzaak van beveiligingsincidenten onderzoekt en ondersteunt bij het oplossen ervan.*
- *Security incident responder: Is verantwoordelijk voor de uitvoering van het herstel van IT-systemen en het verhelpen van de gevolgen van een incident*
- *CISO: Is de hoogst verantwoordelijke voor advies, kaderstelling en controle op informatiebeveiliging*
- *ISO: Is verantwoordelijk voor het waarborgen van de informatiebeveiliging middels toezicht op het ontwikkelen, implementeren en onderhouden van het beleid en procedures.*

Conform BIO 6.1.1 zijn de verantwoordelijkheden van elke rol gedefinieerd. Het Incident Response Plan (IRP) is een logische plaats om deze verantwoordelijkheden vast te leggen."

4.6 Communicatie en rapportageverplichtingen

Beleidselement	Doel	Omschrijving
Communicatie- en Rapportageverplichtingen	Zorgen voor heldere communicatie tijdens en na incidenten.	Interne en externe communicatievereisten voor incidenten, evenals rapportageverplichtingen naar toezichthouders, klanten en andere belanghebbenden (BIO 16.1.2/16.1.3)

Tabel 8 – Communicatie en rapportageverplichtingen

Wat op te nemen:
Deze sectie moet de interne en externe communicatieprotocollen beschrijven, inclusief meldingsverplichtingen aan regelgevers en belanghebbenden. Leg ook afspraken vast wanneer communicatieafdelingen betrokken moeten worden, bijvoorbeeld voor communicatie richting burgers, bedrijven en politiek.

Voorbeeldtekst:
"Communicatieprotocollen omvatten: Kennisgeving aan belanghebbenden op basis van een stakeholderanalyse. De belanghebbenden zijn minimaal:

- *Management*
- *Securityfuncties*
- *Betrokkenen bij de afhandeling van incidenten*
- *IT-afdeling*
- *Klanten c.q burgers/bedrijven en partners: die mogelijk worden beïnvloed door incidenten en informatie nodig hebben over de impact en maatregelen die worden genomen[3].”*

Beschrijf wie verantwoordelijk is voor welke communicatie. Dit kan bijvoorbeeld ook onder taakverdeling en verantwoordelijkheden worden opgenomen.

Tabel 9 - Communicatiematrix geeft een overzicht van de tijdslimieten waarin communicatie met interne en externe belanghebbenden moet plaatsvinden.

	Communicatietijd (intern)	Communicatietijd (extern)*
Prioriteit 1	Binnen 60 minuten melding bij [x]	Binnen 24 uur melding bij [x]
Prioriteit 2	Binnen 120 minuten melding bij [x]	Binnen 72 uur melding bij [x]
Prioriteit 3	Binnen 48 uur melding bij [x]	Binnen 5 werkdagen melding bij [x]
Prioriteit 4	Binnen 72 uur melding bij [x]	Binnen 30 werkdagen melding bij [x]

Toelichting: tabel heeft betrekking op tijdige communicatie naar belanghebbende waarbij onderscheid is gemaakt tussen belanghebbende binnen de organisatie (intern) en belanghebbende buiten de organisatie (extern).
* Meldplicht verplicht volgens NIS2.

Tabel 9 - Communicatiematrix

[3] Naleving van BIO 16.1.2 en 16.1.3 is verplicht

4.7 Bedrijfscontinuïteit

Beleidselement	Doel	Omschrijving
Bedrijfscontinuïteit	Zorgen voor bedrijfscontinuïteit bij incidenten.	Afhandeling van incidenten met hoge impact en de afstemming met het bedrijfscontinuïteitsplan (BIO 17.1.1) (NIS 21c)

Tabel 10 - Bedrijfscontinuïteit

Wat op te nemen:
Deze sectie moet beschrijven hoe incidentafhandeling is afgestemd op het bedrijfscontinuïteitsplan om kritieke diensten te handhaven tijdens incidenten met grote impact.

Opmerking:
In het incident- en responsebeleid is een uitgebreide beschrijving van de bedrijfscontinuïteit niet noodzakelijk. Echter, de voorbeeldtekst bevat een korte sectie over dit onderwerp, waarbij het van belang is om te verwijzen naar het Business Continuïteit Plan of Policy.

Voorbeeldtekst:
"Incidentresponse-activiteiten worden afgestemd op het Business Continuïteit Plan (BCP) om te waarborgen dat:

- *Back-ups beschikbaar zijn.*
- *Restores binnen de vereiste tijden mogelijk zijn*
- *Kritieke diensten operationeel blijven.*
- *Alternatieve communicatiekanalen worden opgezet.*

Daarnaast is er integratie met crisismanagement als onderdeel van het bedrijfscontinuïteitsmanagement, waarbij incidentresponse-activiteiten worden afgestemd op de processen van crisismanagement. Dit houdt in dat er samenwerking is met het crisismanagementteam om te zorgen voor een gezamenlijke aanpak. Hierbij wordt aandacht besteed aan het ontwikkelen van mogelijke scenario's, het uitvoeren van oefening en het regelmatig bekijken van hoe de incidentresponse past binnen het crisismanagementplan[4]

- *Voeg hier de verwijzing toe naar Business Continuïteit Plan en crisismanagement plan."*

4.8 Forensisch onderzoek en bewijsbeheer

Beleidselement	Doel	Omschrijving
Forensisch Onderzoek en Bewijsbeheer	Bewijs veiligstellen en forensisch onderzoek uitvoeren.	Er is beleid dat voorschrijft dat er procedures zijn voor digitaal forensisch onderzoek en de bewaring van bewijs, inclusief de keten van bewijslast (BIO 16.1.7) (NIS 21b)

Tabel 11 – Forensisch onderzoek en bewijsbeheer

Wat op te nemen:
Deze sectie moet procedures specificeren voor digitaal forensisch onderzoek en het behoud van bewijsmateriaal, inclusief de keten van bewaring.

Opmerking:
In het incident- en responsebeleid is een uitgebreide beschrijving van forensisch onderzoek en bewijsbeheer niet nodig. Binnen het incident- en responseproces is in het kader van forensisch

[4] Dit proces voldoet aan BIO 17.1.1 en NIS 21c.

onderzoek vooral van belang dat forensisch onderzoekers tijdig worden betrokken. Het te laat inschakelen van forensisch onderzoekers resulteert in het risico dat bewijsmateriaal onbedoeld verloren gaat. De voorbeeldtekst bevat een korte sectie over dit onderwerp, waarin het belangrijk is om te verwijzen naar het Forensisch Onderzoek- en Bewijsbeheerplan of -beleid van de organisatie.

Voorbeeldtekst:
"Forensische procedures omvatten:

- *De situaties waarin forensisch onderzoek noodzakelijk is, inclusief specifieke incidenttypes;*
- *De afspraken en procedures voor het tijdig inschakelen van externe partijen voor het uitvoeren van forensisch onderzoek;*
- *Richtlijnen voor het behoud en de integriteit van bewijsmateriaal;*
- *Documentatie van de keten van bewaring, met aandacht voor de traceerbaarheid en naleving van juridische vereisten met betrekking tot bewijsmateriaal;*
- *Richtlijnen voor het gebruik van forensische tools voor malware-analyse[5].*

Alle betrokkenen bij de incidentresponse moeten zich houden aan de richtlijnen, die zijn vastgelegd in het beleid voor Forensisch Onderzoek- en Bewijsbeheerplan, van de organisatie om de integriteit van digitaal bewijs te waarborgen.

- *Voeg hier de verwijzing toe naar policy voor Forensisch Onderzoek en Bewijsbeheer."*

4.9 Incidentanalyse en preventie

Beleidselement	Doel	Omschrijving
Incidentanalyse en Preventie	Voorkomen van toekomstige incidenten door leren van eerdere voorvallen.	Er is beleid dat voorschrijft dat er procedures zijn voor analyse van incidenten en het nemen van preventieve maatregelen op basis van eerdere incidenten (BIO 16.1.1) (NIS 21b en 21f)

Tabel 12 – Incidentanalyse en preventie

Wat op te nemen:
Deze sectie moet zich richten op het omschrijven van processen met betrekking tot het analyseren van incidenten en het implementeren van preventieve maatregelen om toekomstige voorvallen te voorkomen.

Voorbeeldtekst:
"Er worden procedures opgesteld voor het systematisch analyseren van alle beveiligingsincidenten. Deze analyses omvatten het identificeren van oorzaken, gevolgen en mitigerende maatregelen. Na elk incident wordt er een gedetailleerd rapport opgesteld, waarin de bevindingen van de analyse worden vastgelegd. Dit rapport wordt gedeeld met de relevante belanghebbenden[6]. Op basis van de analyses van eerdere incidenten worden er preventieve maatregelen ontwikkeld en geïmplementeerd. Deze maatregelen zijn gericht op het verminderen van de kans op herhaling van soortgelijke incidenten in de toekomst. De effectiviteit van de genomen preventieve maatregelen wordt minimaal 1 keer per jaar geëvalueerd en indien nodig bijgesteld[7]."

[5] Het proces voldoet aan BIO 16.1.7 en NIS 21b
[6] Management, Security functies, Betrokkenen bij de afhandeling van incidenten, Klanten en partners die mogelijk worden beïnvloed door incidenten en informatie nodig hebben over de impact en maatregelen die worden genomen
[7] Naleving van BIO 16.1.1 en NIS 21b is gewaarborgd

4.10 Scenario- en Risicoanalyse

Beleidselement	Doel	Omschrijving
Scenario- en Risicoanalyse	Het gebruik maken van het risicobeeld van de organisatie in het voorbereiden op mogelijke incidenten.	Risicoanalyse en de identificatie van scenario's voor incidenten; proactieve maatregelen voor risicobeperking (BIO 16.1.1) (NIS 21a).

Tabel 13 – Scenario- en Risicoanalyse

Wat op te nemen:
Deze sectie moet de richting geven en kaders stellen aan het uitvoeren van risicoanalyses. Verder moet deze sectie richting geven en kaders stellen aan het identificeren van potentiële incidentscenario's.

Voorbeeldtekst:
"De organisatie voert periodiek een risicoanalyse uit om potentiële risico's te identificeren, waarbij kwetsbaarheden en bedreigingen voor de informatiebeveiliging in kaart worden gebracht, met aandacht voor technische, organisatorische en menselijke factoren. Op basis van deze analyses worden specifieke scenario's voor incidenten ontwikkeld, die helpen bij het begrijpen van mogelijke incidenten en hun impact, en worden geclassificeerd op urgentie en impact om prioriteiten voor verdere acties te bepalen. Daarnaast is de organisatie gericht op het verkrijgen van informatie over informatiebeveiligingsrisico's door middel van continue monitoring, rapportages en feedback van medewerkers. Deze informatie ondersteunt de verbetering van incident response plannen en processen[8]."

[8] Deze aanpak voldoet aan BIO 16.1.1 en NIS 21a

Bijlage I

Download: Incident Response Policy template voor het opstellen van specifiek beleid ten aanzien van Incident Respons.

Of maak gebruik van het SOC Security Policy template (Word document). Deze blanco template biedt een format voor organisaties die het SOC beleid stap voor stap zelf willen opstellen of aanpassen. Deze template moet apart worden gedownload en is onderdeel van bijbehorende kennisdocument SOC Security Policies.

Uitgave

Versterken SOC Stelsel Rijk (VSSR)

Postbus 117, 2501 CC Den Haag

Turfmarkt 147, 2511 DP Den Haag

070 751 5555

Meer informatie

https://www.ncsc.nl/vssr

info@ncsc.nl

vssr.info@minjenv.nl (Rijksoverheid)

Juni 2025