TLP:GREEN

IR-3 IB BELEID CHECKLIST

Incident Response - Incident Response Readiness

Best Practice versie 1.1

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	16-06-2025	Initiële versie
V1.1	29-6-2026	Referenties geactualiseerd

1.2 Referenties

Document	Link
Incident Response – IB Beleid voorbeelduitwerking	Zie "IR-3, Incident Response – IB Beleid voorbeelduitwerking (pdf)" onder Incident Response Readiness
Incident Response Readiness miniproducten	Zie Incident Response Readiness op het VSSR-portaal
SOC Security Policies	IB Beleid voor Security Operations Center
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

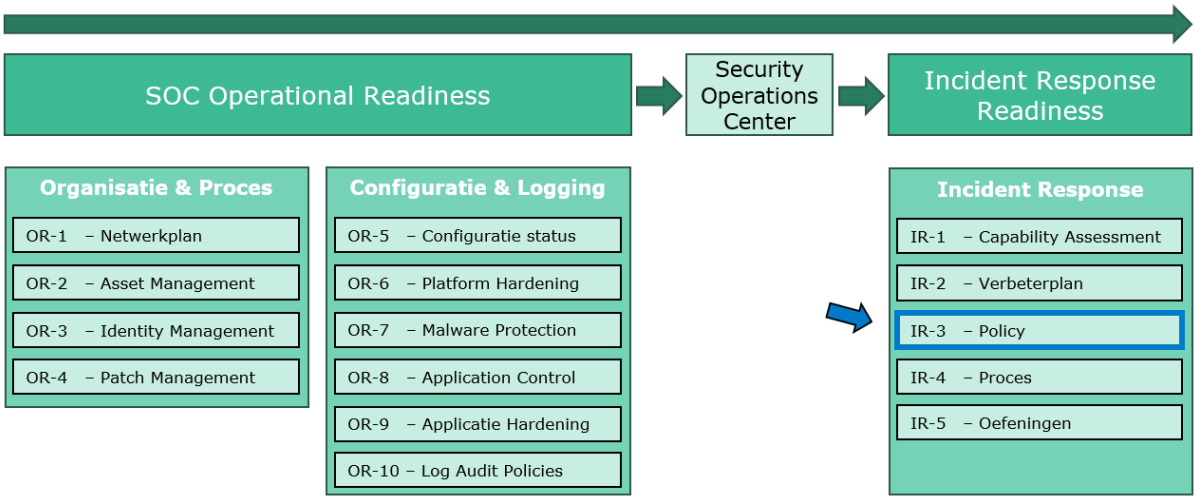
Ter verduidelijking van de terminologie en begrippen die in dit document worden gebruikt is er een verzameling van definities te vinden op Woordenboek - Cyberveilig Nederland.

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

Dit document behandelt het beleid/**policy** (IR-3), binnen de productgroep **Incident Response**.

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

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

- IB Beleid voorbeelduitwerking
  PDF document met voorbeelduitwerking IB Beleid

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, is het belangrijk dat je het 'IR1 – Capability Assessment' ten minste voor het thema beleid hebt uitgevoerd. Dit helpt om de huidige situatie van je organisatie te bepalen en de juiste verbeteracties te selecteren.

3.2 Wat is het doel van dit document?

Dit document helpt je om binnen de context van informatiebeveiliging:

- nieuw beleid op te stellen voor beveiligingsincident- en responsemanagement;
- bestaand beleid te toetsen op volledigheid en waar nodig uit te breiden;
- te voldoen aan eisen vanuit de BIO en de NIS2-richtlijn;
- de structuur en inhoud van beleidsdocumenten vast te leggen;
- beleid te koppelen aan procesdocumentatie en governance.

3.3 Gebruik van dit document

Het document bevat een checklist waarmee je kunt inventariseren welke onderdelen van het beleid al zijn ingevuld en welke nog aandacht vragen. Je kunt het document op verschillende manieren gebruiken, afhankelijk van je doel:

- Startpunt voor nieuw beleid: Gebruik hoofdstuk 5 (Checklist) om te bepalen welke onderwerpen je moet opnemen.
- Toets bestaand beleid: Gebruik de checklist om te controleren welke elementen al zijn opgenomen. Gebruik hoofdstuk 6 als leidraad voor de structuur van je beleidsdocument.
- Ondersteuning bij audits of compliance checks: Verwijs naar dit document en de bijbehorende bronnen (BIO, NIS2) om aan te tonen dat aan relevante verplichtingen wordt voldaan.

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 Kaderstelling en beleid

In dit document worden de belangrijkste richtlijnen voor het opstellen van beveiligingsincident- & responsebeleid besproken in de vorm van een checklist.

Volgens de BIO, specifiek 5.1.1 "Beleidsregels voor informatiebeveiliging", moeten organisaties beleidsregels definiëren voor informatiebeveiliging. Deze beleidsregels moeten goedgekeurd worden door de directie, gepubliceerd zijn en effectief gecommuniceerd worden aan zowel medewerkers als relevante externe partijen. Dit zorgt ervoor dat iedereen binnen de organisatie als ook externe stakeholders, op de hoogte zijn van beleid rondom informatiebeveiliging en beveiligingsincidenten. In het volgende hoofdstuk wordt een checklist gegeven van elementen die altijd in een beleid voor beveiligingsincident- & response moeten terugkomen.

Bij het gebruiken van de checklist dient er rekening te worden gehouden dat dit beleid nooit op zichzelf staat. Er wordt vanuit gegaan dat beleid ten aanzien van beveiligingsincident- & response onderdeel is van het informatiebeveiligingsbeleid van de organisatie. Een verwijzing naar dat beleid is dan ook een element van de checklist.

De checklist omvat 10 elementen die allemaal vertegenwoordigd moeten zijn in het beleidsdocument. Het is echter niet vereist om elk element volledig uit te werken; in sommige gevallen kan een verwijzing naar ander beleid, zoals het ethisch beleid, voldoende zijn. In de checklist is aangegeven bij welke elementen het voldoende is om verwijzingen naar onderliggende specifieke beleidsstukken op te nemen. Elk element in de checklist kan door de organisatie verder uitgewerkt worden.

BIO/NIS	Control	Verantwoordelijke
BIO 5.1.1	Beleidsregels voor informatiebeveiliging. Ten behoeve van informatiebeveiliging behoort een reeks beleidsregels te worden gedefinieerd, goedgekeurd door de directie, gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen.	Secretaris/algemeen directeur
NIS Art 21	Beleid inzake risicoanalyse en beveiliging van informatiesystemen	Secretaris/algemeen directeur

5 Checklist

De checklist in dit hoofdstuk is gebaseerd op de BIO-hoofdstukken 5, 16 en 17 van de BIO versie 1.04zv, en het NIS2-hoofdstuk 21. Deze hoofdstukken bevatten elementen die kunnen worden opgenomen in een beveiligingsincident- & responsebeleid.

In onderstaande tabel staat een overzicht van de elementen die minimaal opgenomen moeten worden in het beveiligingsincident- & responsemanagementbeleid. Het is niet noodzakelijk om alle onderdelen van de checklist volledig uit te werken in het beveiligingsincident- & responsemanagementbeleid, een verwijzing naar andere beleidsstukken waarin de details verder zijn uitgewerkt volstaat.

Beleid element	Doel	Omschrijving
1.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.
2.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 beveiligingsincident wordt beschouwd en hoe deze een classificatie op basis van impact en urgentie krijgt. (BIO 16.1.4) (NIS 21b) De beveiligingsincident-definitie moet hier richtinggevend zijn en is daarmee algemeen van karakter. Hier moet ook aangegeven worden hoe die voor de verschillende IT-systemen nader moet worden gespecificeerd.
3.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)
4.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)
5.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

Beleid element	Doel	Omschrijving
		opgenomen te worden. In het beleid volstaat een verwijzing naar de procesbeschrijving of een beschrijving op hoog niveau (rollen).
6.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)
7. Bedrijfscontinuïteit	Zorgen voor bedrijfscontinuïteit bij incidenten.	Afhandeling van incidenten met hoge impact en de afstemming met het bedrijfscontinuïteitsplan (BIO 17.1.1) (NIS 21c)
8.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)
9.Incidentanalyse en -Preventie	Voorkomen van toekomstige incidenten door leren van eerdere voorvallen.	Er is beleid dat voorschrijft dat er procedures zijn voor het analyseren van incidenten en het nemen van preventieve maatregelen op basis van eerdere incidenten (BIO 16.1.1) (NIS 21b en 21f)
10.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).

Let op: Het is goed om het beleid regelmatig te herzien en bij te werken om ervoor te zorgen dat deze blijft voldoen aan de organisatiedoelen en wet- en regelgeving, zoals de BIO

6 Opzet Beleidsdocument

Na het bepalen van de richtlijnen is de volgende stap het opstellen van een beleidsdocument.

U kunt hierbij gebruik maken van voorbeelden, en templates, die VSSR op het portaal beschikbaar heeft gesteld.

Zie:

- "IR-3, Incident Response – IB Beleid voorbeelduitwerking (pdf)" onder Incident Response Readiness;
- SOC Security Policies – IB Beleid voor Security Operations Center.

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