GENERIEK CYBERSECURITY INCIDENT RESPONSE PLAN

DEEL A

Incident Management – Incident Response

Template versie 1.1

Samenwerken maakt

DIGITAAL VEILIGER

VSSR

Inhoudsopgave

Voorwoord

Digitale weerbaarheid is een randvoorwaarde voor het goed functioneren van iedere organisatie binnen de overheid. Incidenten in de informatievoorziening kunnen niet alleen de continuïteit van onze dienstverlening raken, maar ook het vertrouwen van burgers, partners en medewerkers.

Het Cyber Incident Response Plan (CIRP) bestaat uit 2 delen. Met dit deel (deel A) legt de organisatie de juiste inrichting vast. Het beschrijft hoog over hoe in de organisatie gecoördineerd, transparant en doeltreffend moet worden gehandeld bij cyber security incidenten en wie daarin welke rol heeft. Het plan biedt een uniform raamwerk dat vooral bij de voorbereiding op een cyber incident zijn meerwaarde heeft. Deel B van het CIRP biedt vooral een praktisch handvat dat tijdens een cyber incident erbij kan worden gepakt en de betrokkenen begeleidt bij de te nemen acties. Dit document is generiek beschreven. Beide documenten (zowel A als B) dienen op basis van organisatie-specifieke kenmerken, wensen en eisen nog wel uniek te worden gemaakt. Het document dient als een blauwdruk op basis waarvan een eigen CIRP samengesteld kan worden. Vervang relevante secties, maak ze organisatie-specifiek waar nodig, verwijder irrelevante elementen en voeg toe wat uw organisatie nodig heeft. Beiden documenten samen vormen het volledige CIRP.

Het Cyber Incident Response Plan is bedoeld als praktisch instrument: een leidraad voor iedereen die betrokken is bij de digitale beveiliging en crisisbeheersing. Door cyber incident respons met behulp van het CIRP regelmatig te oefenen, te evalueren en te verbeteren, wordt de weerbaarheid vergroot. Waar nodig dient het CIRP n.a.v. evaluatiepunten uit de oefeningen (of incidenten) te worden aangepast.

Achtergrond

Versterken SOC Stelsel Rijk (VSSR) levert verschillende kennisproducten die betrekking hebben op Security Operations. Dit document helpt bij de prakrische kan van het beschrijven en inrichten van Incident Respons en kan worden gebruikt als voorbeeld voor de eigen organisatie.

Doelgroep

VSSR biedt met dit document handvatten voor alle vertegenwoordigers en functionarissen betrokken bij informatiebeveiliging en voornamelijk zij die betrokken zijn bij Cybersecurity Incident Response en crisisbeheersing.

1 Documentgegevens

Dit Cyber Incident Response Plan (CIRP) is een levend document dat eigendom is van de *[Rol]* van de organisatie.

[Rol] is verantwoordelijk voor het onderhoud, de actualiteit en de verspreiding van dit document. Benodigde aanpassingen worden in ieder geval jaarlijks geëvalueerd en vastgelegd in onderstaande wijzigingshistorie.

De actuele distributielijst van functionarissen en afdelingen die toegang hebben tot het IRP wordt beheerd door [Rol] en is hieronder opgenomen. Alleen geautoriseerde medewerkers mogen wijzigingen aanbrengen of goedkeuren.

1.1 Eigenaarschap

Document	Link
Auteur	
Eigenaar	
Datum gecreëerd	
Gereviewd door	
Review datum	
Goedgekeurd op	

1.2 Documenthistorie

Versie	Datum	Omschrijving
V1.0	5-3-2026	Initiële versie
V1.1	2-7-2026	Referenties geactualiseerd

1.3 Distributielijst

Versie	Datum	Gedistribueerd naar
V1.0	06-03-2026	*CIO, CISO, SOC, etc.*

1.4 Referenties

Document	Link
VSSR CIRP Deel B	Cyber Incident Response Plan - Deel B - Draaiboek

2 Inleiding

In de inleiding wordt een korte introductie gegeven op het Cyber Incident Response Plan in het licht van een bredere organisatiecontext en gaat in op het doel van dit document.

2.1 Document context

Organisaties zijn in grote mate afhankelijk van digitale processen, ketenpartners en Cloud-leveranciers. Binnen deze digitale processen treden verstoringen op. Hieruit voortvloeiende incidenten hebben niet alleen technische, maar ook juridische, organisatorische en bestuurlijke implicaties. Om verstoringen met betrekking tot cyberaanvallen en bijbehorende incidenten goed te kunnen beheersen, is dit Cyber Incident Response Plan (CIRP) opgesteld.

Het CIRP biedt een uniform handelingskader voor de voorbereiding, respons en, waar relevant, het herstel na cyberincidenten. De uitvoering van dit plan sluit aan bij nationale kaders zoals de *Baseline Informatiebeveiliging Overheid (BIO)*, de *Wet beveiliging netwerk- en informatiesystemen (Wbni)* en z'n opvolger, de *Cyberbeveiligingswet (CBW)*, en sectorale afspraken. Het plan ondersteunt tevens escalatie naar bevoegde autoriteiten zoals het NCSC of het NCTV indien noodzakelijk.

Dit plan is toepasbaar binnen alle organisatieonderdelen die betrokken zijn bij informatiebeveiliging en crisisbeheersing, waaronder:

- Operationeel/tactisch: Security Operations Centers (SOC's), Decentrale Security Teams (DST's), CISO's en ICT-beheerders;
- Organisatorisch: Informatiebeveiliging, privacy, communicatie en bedrijfscontinuïteit;
- Nationaal: NCSC (meldpunt voor ernstige incidenten), NCTV/NCC (nationale crisisstructuur, bestuurlijke coördinatie).

2.2 Doel

Het CIRP beschrijft hoe de organisatie snel, effectief en gecoördineerd reageert op Cyber beveiligingsincidenten die de beschikbaarheid, integriteit of vertrouwelijkheid van informatie kunnen aantasten.

Het doel van dit CIRP is het waarborgen van een gecoördineerde, snelle en proportionele reactie op Cyber beveiligingsincidenten, zodat schade aan dienstverlening, burgers en partners wordt beperkt en herstel efficiënt kan plaatsvinden.

Een cybersecurity-incident is elke gebeurtenis die kan leiden tot verlies van vertrouwelijkheid, integriteit of beschikbaarheid van informatie of systemen. Het plan onderscheidt:

- Standaard beveiligingsincidenten: operationele, routinematige beveiligingsincidenten die binnen reguliere IT-processen worden afgehandeld;
- Niet-standaard beveiligingsincidenten: complexe of gecoördineerde dreigingen met verhoogde impact hiervoor treedt het CIRP in werking.

Het CIRP richt zich primair op niet-standaard beveiligingsincidenten die de reguliere operationele processen overstijgen of aanzienlijke impact kunnen hebben op dienstverlening, reputatie of naleving van wet- en regelgeving. Deze afbakening helpt om incidentrespons te koppelen aan bestaande crisisstructuren, wettelijke verplichtingen (BIO, AVG, Wbni, CBW) en interne governance. Daarmee vormt dit plan een integraal onderdeel van het bredere informatiebeveiligings- en continuïteitsbeleid.

Het CIRP biedt een raamwerk voor samenwerking tussen technische teams, management, communicatie en bestuur, zodat incidenten integraal en gecontroleerd worden aangepakt.

Onder het toepassingsgebied van dit CIRP vallen onder andere:

- Cyberincidenten: aanvallen of verstoringen die voortkomen uit digitale dreigingen (bijv. malware, phishing, DDoS, ongeautoriseerde toegang);
- Datalekken: onbedoelde of onbevoegde openbaarmaking, wijziging of verlies van persoonsgegevens of vertrouwelijke informatie;

- Integrale beveiligingsincidenten met digitale component: situaties waarin fysieke, organisatorische of sociale aspecten samenkomen met digitale risico's (bijv. sabotage, interne fraude of misbruik van toegangsrechten).

De belangrijkste doelstellingen voor dit CIRP zijn:

1. Duidelijke verantwoordelijkheden: vastleggen van rollen, taken en communicatielijnen bij cyberincidenten;
2. Samenhang en samenwerking: borgen van effectieve samenwerking tussen technische, organisatorische en bestuurlijke niveaus;
3. Continu verbeteren: zorgen voor registratie, analyse, rapportage en structurele verbetering (PDCA-cyclus);
4. Naleving: bevorderen van transparantie en voldoen aan wettelijke meld- en rapportageverplichtingen (Wbni, AVG, BIO, CBW);
5. Leren & verbeteren: structureel evalueren van incidenten en toepassen van verbetermaatregelen in processen en beleid.

2.3 Leeswijzer

Dit document is in een aantal secties onderverdeeld. De verschillende hoofdstukken gaan in op:

- Hoofdstuk 3 – de organisatorische context van het CIRP;
- Hoofdstuk 4 – het incident response proces op hoofdlijnen met toelichting;
- Hoofdstuk 5 – communicatiestructuren;
- Hoofdstuk 6 – incidentmelding en rapportage.

Deel B van het CIRP gaat dieper in op de processtappen binnen het incident respons proces met de praktische handvatten om tijdens een incident te kunnen handelen.

3 Context

Dit hoofdstuk gaat in op de context en organisatie waarop het incident response proces van toepassing is. Hierbij worden een aantal zaken uiteengezet zoals: externe kaders, beleid, beleidscharter, stakeholders en scope.

3.1 Externe kaders, wet- en regelgeving

De organisatie dient rekening te houden met verschillende externe wetten, kaders en regelgeving. De onderdelen die van toepassing zijn, zijn hieronder uiteengezet.

Op hoofdlijnen sluit het plan aan op de volgende verplichtingen en richtlijnen: *[Verder aanvulen]*

- **Nationaal**: BIO2, Landelijk CrisisPlan (LCP) Digitaal, Nationaal Handboek Crisisbeheersing;
- **NCSC**: Wbni meldplicht;
- **Internationaal**: NIST SP 800-61r3, ISO/IEC 27035.

3.2 Beleid

Onderstaande informatiebeveiliging specifieke beleidsdocumenten zijn van toepassing op of liggen aan de basis van het Cyber Incident Response Plan (CIRP).

Documentnaam	Beleidsonderwerp(en)	Bestandslocatie
[Invullen]	*[Invullen]*	*[Invullen]*

Naast beleidsdocumenten die betrekking hebben op informatiebeveiliging zijn onderstaande, niet-informatiebeveiliging specifieke, beleidsdocumenten ook van toepassing.

Documentnaam	Beleidsonderwerp(en)	Bestandslocatie
[Invullen]	*[Invullen]*	*[Invullen]*

3.3 Stakeholders

Overzicht interne stakeholders

Stakeholder	Verantwoordelijkheid	Belang	Communicatiebehoefte
Directie/Management			
CISO / Security Officer			
IT-afdeling			
IT-beheer			
FG			
Medewerkers			
Eindgebruikers			
HR-afdeling			

Overzicht externe stakeholders

Stakeholder	Verantwoordelijkheid	Belang	Communicatiebehoefte
Leveranciers			
Partners			
klanten			
Toezichthouders			
Autoriteiten			

3.4 Opdracht

In deze paragraaf is de charter voor het incident response team vastgelegd samen met de communicatie interface naar buiten toe zodat het voor alle partijen duidelijk is hoe het incident response team benaderd kan worden en voor wat precies. Deze informatie is samengesteld in navolging van de internationale standaard gespecificeerd in RFC2350 en is publiek beschikbaar gesteld voor zover relevant en nodig.

Contactinformatie

Onderwerp	Informatie
Team Naam	CSIRT @Organisatie
Adres	
Tijd Zone	
Telefoon	
Fax	
Andere Communicatiemiddelen	Bijvoorbeeld: beveiligde telefoon verbindingen, chat-groepen, etc.
E-mail	
Public keys	
Team-leden	Als het privacy-technisch mogelijk is om dit op te nemen.
Openingstijden	
Additionele contact informatie	Klant/publieke contact informatie die mogelijk afwijkt van de algemene (of interne) contactinformatie

Charter

Onderwerp	Informatie
Missie	
Scope	
Sponsors	
Mandaat	

Policies

Onderwerp	Informatie
Incidenttypen en supportlevels	
Samenwerking, interactie en privacy	
Communicatie en authenticatie	

Services

Onderwerp	Informatie
Service naam	*Beschrijf hier de verschillende services die worden geleverd door het CSIRT-team. RFC2350 geeft hierin handvatten.*

Meldingsformulier

Zie Bijlage I: Incident Meldingsformulier het formulier voor het melden van incidenten. Dit dient beschikbaar gesteld te worden voor externe partijen (en kan ook in de vorm van een online-formulier beschikbaar worden gesteld op de website van de organisatie).

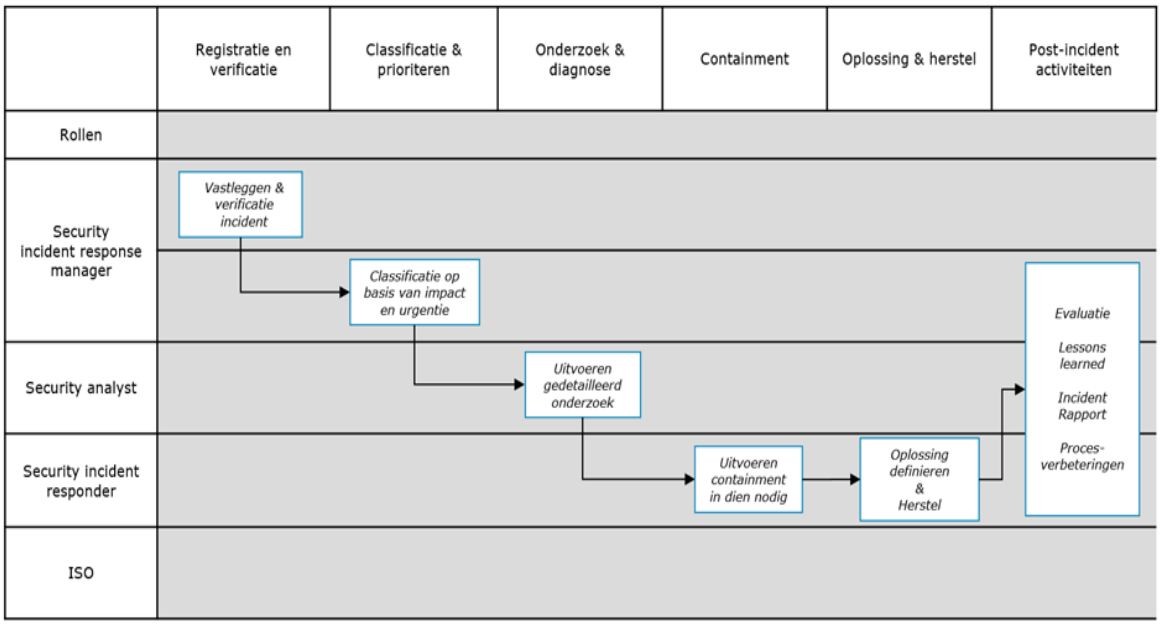
4 Cyber Security Incident Response Proces

Het incident responseproces beschrijft de hoofdactiviteiten die organisaties doorlopen bij de voorbereiding, detectie, beheersing, afhandeling en evaluatie van cyberincidenten.
Het biedt een raamwerk voor coördinatie tussen technische, organisatorische en bestuurlijke rollen. Het proces is gebaseerd op internationaal erkende richtlijnen:

- *ISO/IEC 27035 – Information Security Incident Management*
- *NIST SP 800-61v3 – Computer Security Incident Handling Guide*

4.1 Procesdiagram

Onderstaande flowchart biedt een visueel overzicht van het beveiligingsincident- & responseproces. In de rijen staan de betrokken rollen weergegeven en in de kolommen de verschillende processtappen. Het procesdiagram gaat voornamelijk in op de stappen die doorlopen moeten worden met betrekking tot een (potentieel) incident. Hieraan voorafgaand (in de pre-incident fase) gaat nog de voorbereiding. Deze is niet in het diagram opgenomen maar is in de volgende paragraaf wel vermeld en toegelicht.



4.2 Procesfasen

Het incident responseproces bestaat uit vijf kernfasen, die samen de volledige levenscyclus van incidentmanagement vormen.

Fase	Beschrijving
Voorbereiding	Plannen, oefenen, rollen, middelen en communicatiestructuren inrichten
Detectie & Analyse	• Registratie & verificatie: Vastlegging en verificatie meldingen • Classificatie & prioriteren: Prioriteren op basis van type, impact en urgentie • Onderzoek & diagnose: Identificeren en vaststellen van incidenten
Containment	Beperken van de impact en beheersen van het incident
Oplossen & Herstel	Toepassen permanente oplossingen en herstelmaatregelen
Post-incident activiteiten	Evaluatie & Verbetering door het vastleggen van Lessons Learned, proces optimalisatie en verbetermaatregelen implementeren

De verschillende fasen zijn hieronder verder toegelicht.

Pre-incident fase

1. Voorbereiding
   Inrichten van beleid, processen, rollen, middelen en communicatiestructuren om effectief te kunnen reageren.
   Dit omvat het opstellen van playbooks, definiëren van verantwoordelijkheden, testen van procedures en uitvoeren van oefeningen.

Incident fase

2. Detectie & Analyse
   Deze fase valt uiteen in:
   1. Registratie & Verificatie;
   2. Classificatie & Prioriteren; en,
   3. Onderzoek & Diagnose.

   Afwijkende zaken worden gedetecteerd (middels techniek) of gebruikers maken melding van gebeurtenissen. Geregistreerde meldingen worden gevalideerd, dan wordt een eerste classificatie met impact en ernst beoordeling gedaan. Hierna wordt onderzoek gedaan en een diagnose gesteld.

3. Containment
   In deze fase worden, waar nodig, tijdelijke maatregelen genomen om verdere schade te voorkomen of te beperken. Denk aan het isoleren van systemen, beperken van toegang of stopzetten van processen om escalatie te voorkomen.

4. Oplossen & Herstel
   In deze stap wordt gekeken naar structureel verwijderen van de oorzaak, herstellen van systemen en terugbrengen naar een veilige operationele staat. Herstel kan technisch (patchen, schoonmaken, back-up terugzetten) of organisatorisch (procesaanpassing) van aard zijn.

Post-incident fase

5. Evaluatie & Verbetering
   In deze stap gebeurt het documenteren van bevindingen, evalueren van het optreden en vastleggen van verbetermaatregelen. Lessons learned worden verwerkt in beleid, training en technische controles om herhaling te voorkomen.

4.3 Rollen en verantwoordelijkheden

In deze paragraaf worden eerst de betrokken partijen toegelicht om in een vervolgparagraaf te specificeren wat de verantwoordelijkheden van de verschillende partijen zijn middels een RACI-matrix.

4.3.1 Rollen

Onderstaande tabel voorziet in de korte rolbeschrijvingen.

Rol	Beschrijving
Security incident- en response manager (SIRM)	Verantwoordelijk voor het end-to-end coördineren, beheren en leiden van de reactie op beveiligingsincidenten binnen de organisatie
Security analist	Verantwoordelijk voor het onderzoeken van de oorzaak van beveiligingsincidenten
Security incident responder	Verantwoordelijk voor (het toezien op) de uitvoering van het herstel van IT-systemen en het verhelpen van de gevolgen van een beveiligingsincident
ISO	Verantwoordelijk voor het waarborgen van de informatiebeveiliging binnen de organisatie
CISO	Verantwoordelijke voor advies, kaderstelling en controle op beveiliging. Deze rol zorgt ervoor c.q. ziet erop toe dat het beheer op beveiligingsincidenten adequaat wordt uitgevoerd.

4.3.2 Verantwoordelijkheden

Onderstaande RACI-tabel voorziet voor iedere processtap (zie 4.1 Procesdiagram) in een overzicht met rollen verantwoordelijkheden.

	CIRM	SOC-Analist	Incident Responder	ISO	CISO
Registratie & Verificatie	A, R	I	I	I	I
Classificeren & Prioriteren	A, R	C	I	I	I
Onderzoek & diagnose	A	R	R	I	I
Containment	A	C	R	C	I
Oplossing & herstel	A	C	R	I	I
Post-incident activiteiten	A	R	R	R	I

De letters uit de RACI-tabel staan voor:

- R (Responsible): Degene die verantwoordelijk is voor de uitvoering van een taak of activiteit. Dit is de persoon die het werk uitvoert.
- A (Accountable): Degene die eindverantwoordelijk is. Deze persoon zorgt ervoor dat de taak correct en tijdig wordt uitgevoerd en geeft goedkeuring.
- C (Consulted): Personen of teams die geraadpleegd worden voor hun input of expertise. Dit zijn vaak belanghebbenden die adviseren.
- I (Informed): Personen of teams die geïnformeerd moeten worden over de voortgang of

5 Communicatie & Escalatie

Heldere en tijdige communicatie is cruciaal bij cyberincidenten. Dit hoofdstuk beschrijft wie op welk moment wordt geïnformeerd, via welke kanalen, en op welk niveau bestuurlijke afstemming plaatsvindt. Het uitgangspunt is dat communicatie altijd eenduidig, transparant en afgestemd is – zowel intern als extern.

Communicatieprincipes:

- "**Eén lijn, één boodschap**": alle externe communicatie wordt centraal afgestemd;
- Gebruik van **SitRap** als feitelijke basis voor alle interne en externe berichtgeving;
- De frequentie van communicatie neemt toe naarmate het incident-niveau stijgt;
- Bewaar altijd audit-trail van verzonden updates (voor reconstructie en evaluatie);
- NCSC verzorgt technische informatie-uitwisseling; NCTV/NCC coördineren bestuurlijke en publieke communicatie op nationaal niveau;
- Evaluatie van communicatie maakt deel uit van de *post-incident review*.

5.1 Incident niveaus en opschalingsmodel

Escalatie vindt plaats via vastgestelde lijnen; in geval van niet beschikbare communicatiemiddelen wordt overgeschakeld op de *out-of-band* (OOB) communicatiemiddelen, zoals noodtelefoons of vooraf gedefinieerde Teams/OOB-kanalen.

Algehele Incident Classificatie & Prioritering

Niveau	Ernst	Impact
L5	Kritiek	Organisatiekritieke processen, toepassingen en systemen aangetast, data lek, ransomware, voortbestaan van de organisatie komt in het gedrang of het incident kan omslaan in een nationale crisis. Interdepartementale of sectorale coördinatie
L4	Hoog	Significante impact, meerdere systemen, mogelijk data lek Departementale of organisatie brede coördinatie
L3	Midden	Beperkte impact, enkel(e) syste(e)m(en), geen data lek Coördinatie over meerdere onderdelen binnen de organisatie
L2	Laag	Minimale impact, enkel systeem of gebruiker, monitoring vereist Operationele coördinatie binnen één organisatieonderdeel
L1	Informatief	Indicatoren of niet-succesvolle aanvalspogingen

5.2 CyberSecurity Incident Response Team (CSIRT)

Het CSIRT is verantwoordelijk voor de afhandeling van incidenten. Afhankelijk van de organisatie is het CSIRT tijdelijk van aard en heeft mogelijk, naast een vast team, een flexibele schil die kan worden ingeschakeld afhankelijk van het type, omvang of ernst van een incident.

Onderstaande samenstelling is een voorbeeld, bekijk voor de organisatie wat praktisch en wenselijk is en richt hiermee het team in. Bedenk hierbij dat mogelijk niet alle rollen van toepassing zijn.

Samenstelling:

- **Incident Manager** (CISO of senior SOC-analist)
  verantwoordelijk voor coördinatie en rapportage.
- **SOC-analisten / forensisch onderzoekers**
  verantwoordelijk voor technische analyse, logging en detectie.
- **Systeem- en netwerkbeheerders**
  uitvoering containment- en herstelmaatregelen.
- **Privacy Officer / Juridisch adviseur**
  begeleiding bij datalekken, juridische duiding, AVG-meldingen.
- **Communicatieadviseur**
  interne en externe communicatie, afstemming met woordvoering / NCC indien nodig.

- **Vertegenwoordiger beveiligingsambtenaar (BVA) of Departementaal Crisiscoördinatiecentrum (DCC)**
  bij CIRP-3/4, bestuurlijke afstemming en besluitvorming.
- **Externe ondersteuning** (CSIRT-partner, leverancier of NCSC)
  bij hoog, kritische incidenten of bij crises, advies en nationale afstemming.

Taken van het CSIRT:

Taakgebied	Beschrijving	Niveau
Situatieanalyse en classificatie	In kaart brengen aard, omvang, en impact van het incident; vaststellen niveau.	L1 t/m 5
Coördinatie containment en herstel	Afstemmen technische en organisatorische maatregelen om schade te beperken.	L2 t/m 5
Communicatie en rapportage	Opstellen SitRaps, informeren CISO/BVA/DCC, coördineren externe meldingen.	L2 t/m 5
Afstemming met DCC en NCSC	Bij ernstige of ketenincidenten; delen van informatie, afstemming technische respons.	L4 t/m 5
Opschaling naar nationale structuur (NCTV/NCC)	Coördinatie bij nationale crisis of rijksbrede impact; afstemming communicatie en beleid.	L4 t/m 5
Evaluatie en lessons learned	Natraject; rapportage oorzaken, effectiviteit maatregelen, verbeterpunten.	Alle niveaus

5.3 Stakeholdercommunicatie

Bij incidenten zijn mogelijk verschillende stakeholders betrokken op verschillende momenten afhankelijk van de omvang en ernst van het incident. De verschillende groepen stakeholders zijn hier weergegeven.

Interne communicatie

- Richting SOC-team, CISO, CIO en management;
- Gebruik vaste meldstructuren (bijv. SitRap) voor updates en besluiten.

Departementale communicatie

- Afstemming met communicatieadviseur en juridische ondersteuning.

Externe communicatie

- **NCSC:** bij ernstige cyberincidenten (Wbni-meldplicht);
- **NCTV / NCC:** bij nationale of rijksbrede crisis (L4 en hoger);
- **Autoriteit Persoonsgegevens:** bij datalekken (AVG, binnen 72 uur);
- **Ketenpartners / leveranciers:** via vooraf vastgelegde contactpersonen (Zie 5.4 voor verdere details).

Publieke communicatie

- Alleen via woordvoerders, in afstemming met Communicatie;
- Persvragen of publieke statements verlopen via de centrale communicatielijn van de organisatie of departement.

5.3.1 Meldingsplicht notificatie matrix

De volgende externe partijen dienen ingelicht te worden bij de aangegeven incident typen volgens de opgenomen tijdsindicaties.

Incident type	Wie	Waarom	Wanneer
Naam	*Ontvangende organisatie*	*Waarom moet de melding plaatsvinden*	*Wat dient gerapporteerd te worden (eventueel met template link)*
Significant	NCSC	NIS2 | DORA | WBNI	Vroegtijdig (fase 1): binnen 24 uur Update (fase 2): binnen 72 uur Eindverslag: binnen 1 maand na afronding incident
Significant	NCSC	Netcode	Vroegtijdig (fase 1): binnen 4 uur
Datalek	AP	AVG	Binnen 72 uur na ontdekking (kennisname)
Datalek	Eigenaar[1]	AVG	Direct na ontdekking (kennisname)
N/A	Branch Toezichthouder	Branch voorschriften	N/A

5.3.2 Interne notificatie matrix

Afhankelijk van de ernst van de melding dienen verschillende partijen en stakeholders volgens onderstaand schema ingelicht te worden.

Ernst	Wie	Wanneer
Kritiek[2]	*CISO, CTO, CEO, Juridisch*	*Eerste melding: 15 minuten* *Status update: elke uur*
Hoog	*CISO, IT-management*	*Eerste melding: 30 minuten* *Status update: elke 2 uur*
Midden	*Security Team, IT-Ops*	*Eerste melding: 1 uur* *Status update: elke 4 uur*
Laag	*SOC*	*Eerste melding: 4 uur* *Status update: 1x per dag*
Informatief	*SOC*	*NVT*

5.3.3 Externe notificatie matrix

In een eerdere paragraaf zijn medeplichtige incidenten opgenomen. Als uitbreiding hierop wordt in deze paragraaf noodzakelijke additionele notificatie opgenomen op basis van bestaande contractuele afspraken en normen.

Bepaal of een externe notificatie matrix opgesteld dient te worden. Dit is afhankelijk van additionele verplichting bovenop de eerder genoemde meldplicht. Denk voor additionele externe communicatie aan zaken als:

- *Politie in geval van aangiften.*
- *Media response of aankondigen.*
- *Klanten/data eigenaren in geval van data lek.*
- *Investor relaties.*

[1] Een data-eigenaar kan een klant zijn, maar ook een toeleverancier of een dienstverlener.
[2] Incidenten met ernst kritiek en hoog worden gezien als significant en moeten worden gemeld.

Ernst	Wie	Wanneer
Crisis		
Kritiek[3]	*Politie, Media, Data Eigenaar, Klanten, Investeerders*	*Afhankelijk van de situatie*
Hoog	*Politie, Media, Data Eigenaar, Klanten*	*Afhankelijk van de situatie*
Midden	*Data Eigenaar*	*Afhankelijk van de situatie*
Laag	*Data Eigenaar*	*Afhankelijk van de situatie*
Informatief	*NVT*	*NVT*

5.4 Leveranciers en dienstovereenkomsten

Deze paragraaf bevat per (ICT-)leverancier welke dienst wordt geleverd en wat de contractuele overeenkomsten zijn met betrekking tot Security Incidenten. Op basis van deze informatie kan per geval worden bepaald welke leverancier betrokken dient te zijn bij het oplossen van een incident en hoe in contact te treden met de betreffende leverancier.

5.4.1 Dienstleverancier A

Dienst: Beheer desktop en laptops
Overeenkomst Security Incidenten per type:

- Kritiek: direct bellen met escalatie contactpersoon.
- Hoog: direct bellen met escalatie contactpersoon.
- Midden: direct bellen met helpdesk om een Security Incident aan te laten maken.
- Laag: notificeer de helpdesk per email met een incident rapport volgens afgesproken template.

Contactgegevens: e-mail: helpdesk@leverancier.nl, tel: 088 1234 567
Escalatie contactgegevens: manager@leverancier.nl, tel: 06 1234 5678
Locatie contractuele overeenkomst: [Link]

5.4.2 Dienstleverancier B

Dienst: Incident Response Service
Overeenkomst Security Incidenten:

- Kritiek: Direct bellen 24x7, eerste triage uitvoeren en responder laten dispatchen.
- Hoog: Direct bellen 24x7, eerste triage uitvoeren om verdere acties te bepalen.
- Medium: Bellen tijdens kantooruren als hulp bij een lopend incident gewenst is.
- Laag: NVT

Contactgegevens: tel: 088 1234 567, email: 24x7@company.com
Escalatie contactgegevens: manager@company.com
Locatie contractuele overeenkomst: [Link]

6 Incidentmelding en Rapportage

Dit hoofdstuk beschrijft hoe incidenten intern én extern worden gemeld, en hoe daarover wordt gerapporteerd. Een duidelijke meld- en rapportagestructuur voorkomt misverstanden tijdens een crisis en borgt dat wettelijke verplichtingen (zoals meldplichten) worden nageleefd.

Uitgangspunten:

- Interne meldingen volgen de escalatielijn van het CIRP-niveau: hoe ernstiger het incident, hoe korter de meldtermijnen;
- Externe meldingen zijn afgestemd op wettelijke verplichtingen (Wbni, AVG, CBW) en op nationale coördinatie (NCSC, NCTV);
- Rapportages vormen de basis voor evaluatie, verbetering en managementverantwoording.

6.1 Interne meldingen

Niveau	Wie meldt	Waar / systeem	Ontvanger	Termijn
L1	SOC 1e lijn	Ticketing / SIEM	Lokale CISO of Security Officer	Direct
L2	SOC 2e lijn / Security Manager	Meldportaal / e-mail	Centrale CISO / Crisismanager	Binnen 1 uur
L3	Centrale coördinatie (CISO / Crisismanager)	Landelijk Crisis Management Systeem (LCMS) / SitRap / crisisdashboard	Directie of bestuur	Binnen 30 minuten
L4	Organisatiebrede coördinatie (Crisismanager / CISO)	LCMS / SitRap	Sector- of ketencontact / NCSC	Binnen 30 minuten
L5	Nationaal niveau (NCTV/NCC)	LCMS / crisislijn	NCTV/NCC / Bewindspersonen	Onmiddellijk

6.2 Externe meldingen

Incidenttype	Meldinstantie	Verantwoordelijke	Termijn	Meldvorm / kanaal
Ernstig cyberincident	NCSC (Wbni)	CISO / SOC	Onmiddellijk	NCSC-portaal of meldformulier
Datalek / persoonsgegevens	Autoriteit Persoonsgegevens	Privacy Officer / CPO	Binnen 72 uur	Meldformulier AP
Ketenincident / leverancier	Leverancier / sector-CSIRT	CISO / contractbeheerder	Binnen 2 uur	Vastgestelde communicatielijn
Nationale crisis (CIRP-5)	NCTV / NCC	Crisismanager / CISO	Direct	LCMS / crisisoverleg
Internationaal incident (optioneel)	CERT-EU / sectorale CERT	CISO / liaison officer	Op afroep	Beveiligd CSIRT-kanaal

6.3 Rapportage

Rapportage	Doelgroep	Inhoud / doel	Frequentie / moment
SitRap (Situatierapportage)	CISO, Crisismanager, Managementteam	Status, impact, maatregelen, handelingsperspectief	Tijdens incident (minimaal dagelijks bij CIRP-3+)
Incidentlogboek	SOC, Security Officer, Crisismanager	Tijdlijn, acties, besluiten, verantwoordelijkheden	Continu tijdens incident
Post-incident evaluatie	Management, CISO, Security Board	Lessons learned, verbeterpunten, opvolging	Binnen 2 weken na afsluiting incident
Trendanalyse / kwartaalrapportage	Management, Audit / Risk Board	Overzicht incidenttypen, responstijden, verbetertrends	Periodiek (kwartaal / halfjaar)

Bijlage I: Incident Meldingsformulier

Gegevens van melder	
Naam melder	:
Organisatie	:
Email adres	:
Telefoonnummer	:
Relatie (klant, leverancier, …)	:

Datum & tijd van het incident	
Start van het incident	:
Ontdekking van het incident	:
Beëindiging incident	:

Beschrijving van het incident	
Gedetailleerde beschrijving	:
Wat is er gebeurd	:
Wie of wat is er betrokken	:
Waar heeft het incident plaatsgevonden (fysiek of digitaal)	:

Type incident	
Phishing of spoofing	☐
Datalek / ongeautoriseerde toegang tot personeelsgegevens	☐
Malware / ransomeware	☐
Ongeautoriseerde toegang tot ruimtes of systemen	☐
Verlies of diefstal van hardware of documenten	☐
Social engineering	☐
Verstoring dienstverlening (DoS of DDoS)	☐
Overige (toelichting)	:

Betrokken systemen of gegevens	
Welke systemen, applicaties of platforms zijn betrokken	:
Zijn er persoonsgegevens betrokken?	☐
- Zo ja, hoeveel?	:
Zijn er vertrouwelijke bedrijfsgegevens betrokken?	:

Maatregelen die al zijn genomen	
Is er al ergens anders melding gedaan?	:
Zijn er systemen afgesloten of geïsoleerd?	:
Zijn er wachtwoorden gewijzigd?	
Is er al een technisch onderzoek gestart?	

Urgentie-inschatting door melder	
Hoe ernstig schat u het incident in? *(Laag / Midden / Hoog / Kritiek)*	:
Motivatie voor deze inschatting	:

Mogelijkheid voor toevoegen bijlagen / bewijsstukken	
Screenshot	:
Emails	:
Logs	:
Rapportage	:
Overig	:

Toestemming en verwerking	
Verklaring dat het formulier naar waarheid is ingevuld	☐
Toestemming voor verwerking van persoonsgegevens	☐
Verklaring dat er contact opgenomen kan worden met de melder	☐

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)

Maart 2026