Bijlagen
Bijlage 1: Prioritering van incidenten

De incidenten moeten worden geprioriteerd zodat het makkelijker wordt om de geschikte maatregelen voor het incident te activeren. De incidentprioritering wordt herleid uit een tweetal factoren: urgentie en impact. Het toewijzen van de juiste prioriteit aan een incident is essentieel voor het activeren van de geschikte incident maatregelen.

De prioriteit van een incident wordt meestal bepaald door de beoordeling van de impact en urgentie, waarbij:

- Urgentie de maat is voor hoe snel de oplossing van het incident vereist is.
- Impact de maat is voor de omvang van het incident en van de mogelijke schade als gevolg van het incident voordat het kan worden opgelost.

Incident urgentie

In deze paragraaf worden urgentiecategorieën verder uitgewerkt. Om de urgentie van een incident te bepalen, kies je altijd uit de hoogste waarde van de desbetreffende categorie. LET OP: de tabel bevat slechts voorbeelden.

Categorie Urgentie	Omschrijving
Hoog (H)	▪ De schade veroorzaakt door het incident neemt snel toe. ▪ Werk dat moet worden hersteld door personeel is zeer arbeidsintensief. ▪ Een groot incident kan worden voorkomen door bij een klein incident onmiddellijk te handelen. ▪ Het incident leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen voor de bescherming van persoonsgegevens
Medium (M)	▪ De schade veroorzaakt door het incident neemt in de tijd aanzienlijk toe. ▪ Er gaat werk verloren, maar dit is relatief snel te herstellen.
Laag (L)	▪ De schade veroorzaakt door het incident neemt in de tijd maar weinig toe. ▪ Het werk dat blijft liggen is niet tijdsintensief.

Incident impact
In deze paragraaf worden de impact categorieën uitgewerkt, ook hier is de tabel slechts een voorbeeld.
Om de impact van het incident vast te stellen, kies je de hoogste desbetreffende categorie.

Categorie Impact	Omschrijving
Hoog (H)	▪ Relatief veel personeel is geraakt door het incident en/of kan zijn/haar werk niet meer doen. Meerdere afdelingen zijn geraakt, de publieksbalie moet gesloten worden. ▪ Inwoners zijn geraakt en/of lijden schade, op welke wijze dan ook, als gevolg van het incident. Persoonsgegevens zijn gecompromitteerd. ▪ De financiële impact van het incident is (bijvoorbeeld) hoger dan €10.000,-. ▪ Het incident leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel heeft ernstige nadelige gevolgen voor de bescherming van persoonsgegevens. Bij de beoordeling van de impact van het datalek zijn van belang: ▪ de aard en de omvang van het datalek ▪ de aard van de gelekte persoonsgegevens ▪ de mate waarin technische beschermingsmaatregelen zijn getroffen ▪ de gevolgen voor de persoonlijke levenssfeer van de getroffen personen

	▪ Er is reputatieschade, de krant wordt gehaald. ▪ Er zijn lichamelijk gewonden.
Medium (M)	▪ Enig personeel is geraakt door het incident en/of kan zijn/haar werk niet meer doen, bijvoorbeeld een afdeling. ▪ Enkele inwoners zijn geraakt en/of lijden schade, op welke wijze dan ook, als gevolg van het incident. Persoonsgegevens zijn gecompromitteerd. ▪ De financiële impact van het incident is (bijvoorbeeld) hoger dan €1.000,- en lager dan €10.000,-. ▪ Er is kans op reputatieschade.
Laag (L)	▪ Enkele personeelsleden zijn geraakt door het incident en/of kunnen niet meer hun werk doen. ▪ Enkele inwoners zijn geraakt en/of lijden schade, maar dit is zeer minimaal. Persoonsgegevens zijn gecompromitteerd. ▪ De financiële impact van het incident is (bijvoorbeeld) lager dan €1.000,- ▪ Er is geen kans op reputatieschade.

Incident Prioriteringsklassen
De Incident Prioriteit wordt verkregen door urgentie en impact tegen elkaar af te zetten. Voortvloeiend hieruit ontstaat de Incident Prioriteiten Matrix.

		Impact		
		Hoog	Midden	Laag
Urgentie	Hoog	1	2	3
	Midden	2	3	4
	Laag	3	4	5

Incident Prioriteiten Matrix
Als er klassen zijn gedefinieerd om urgentie en impact in te schalen, dan kan een Incident Prioriteit Matrix gebruikt worden om prioriteringsklassen te herleiden. In het onderstaande voorbeeld zijn de klassen uitgewerkt met een code en kleuren.

Code/kleur	**Omschrijving**	**Reactietijd**	**Oplossingstijd**
1	Kritiek	Onmiddellijk	1 uur
2	Hoog	10 minuten	4 uur
3	Medium	1 uur	8 uur
4	Laag	4 uur	24 uur
5	Zeer laag	1 dag	1 week

Het identificeren van kritische incidenten
Het blijft moeilijk om een eenduidige definitie van het begrip kritisch beveiligingsincident te geven. Daarom is het beter om de definitie zo ruim mogelijk te interpreteren.

Een kritisch beveiligingsincident wordt meestal getypeerd door zijn impact, vooral de impact op de organisatie en de privacy van betrokkenen speelt hierbij een belangrijke rol. Enkele voorbeelden:

- Een deel van de datacommunicatie van en naar de organisatie ligt plat door een storing in het netwerk.

- Een belangrijke database blijkt corrupt te zijn.
- Meerdere servers worden geïnfecteerd door een ‘worm’.
- Persoonsgegevens en vertrouwelijke informatie van burgers worden per ongeluk op een publiek toegankelijk forum geplaatst.

Bedenk ook dat alle rampen zoals onderkend in een (nader te ontwikkelen) continuïteitsplan, kritische incidenten zijn en ook dat kleinere incidenten door een niet afdoende afhandeling, zich tot kritische incidenten kunnen ontwikkelen.

Enkele belangrijke gevolgen van kritische incidenten zijn:

- Een groot aantal gebruikers/klanten of enkele belangrijke gebruikers/klanten kunnen mogelijk geen gebruik maken van diensten of systemen.
- Een aantal systemen die belangrijk zijn voor de uitvoering van rampenbestrijding en crisisbeheersing vallen uit of zijn niet benaderbaar.
- De kosten (inclusief gevolgschade) voor gebruikers/klanten of voor de organisatie zijn aanzienlijk of kunnen aanzienlijk worden.
- Het incident leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen voor de bescherming van persoonsgegevens. De organisatie zou reputatieschade kunnen oplopen.
- De tijd en moeite die nodig zijn om het incident op te lossen zijn waarschijnlijk groot en het is zeer waarschijnlijk dat afspraken die zijn vastgelegd in de SLA niet kunnen worden nagekomen.

Bijlage 2: Stappenplan procedure informatiebeveiligingsincidenten

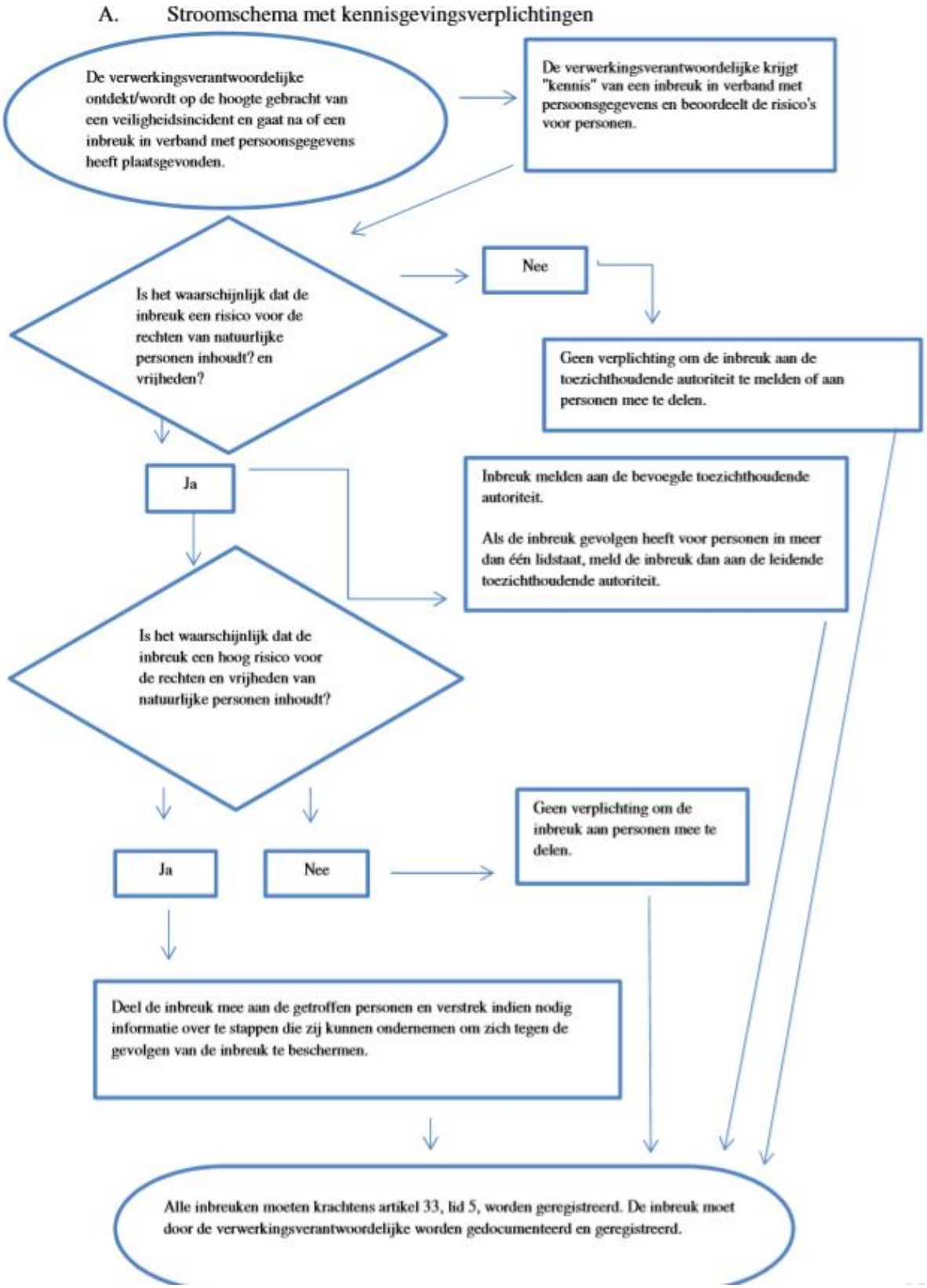
Processtappen	Activiteit	Verantwoordelijke persoon
1. Melding (vermoedelijke) incident	- Maak altijd en direct intern melding van het (vermoedelijk) incident via de daarvoor aangewezen tooling. - Informeer hiernaast direct de beveiligingsfunctionaris en leidinggevende als het gaat om incidenten met een hoge prioriteit	Medewerker die het ontdekt Medewerker die het ontdekt
2. Identificatie	- Onderzoek het incident en leg alle acties hierbij vast in de registratie in de tooling. - Beoordeel wie of welke teams binnen de organisatie hierbij betrokken zijn. - Beoordeel of er een verwerker betrokken is bij het incident. Zo ja, dan dient bepaald te worden wie de verwerkersverantwoordelijke is. Indien de betrokken partij verwerkersverantwoordelijke is, moet zij de mogelijkheid krijgen mee te beslissen over vervolgstappen. Als de betrokken partij verwerker is, is het van belang deze partij te informeren over het incident. - Onderzoek of er persoonsgegevens verloren zijn gegaan of onrechtmatig gebruikt kunnen worden.	Beveiligingsfunctionaris ICT Manager van het team waar het incident heeft plaatsgevonden Beveiligingsfunctionaris Privacy Officer
3. Schade indamming	- Stop het incident als het nog kan - Neem maatregelen om het incident en de daaruit voortvloeiende schade te beperken - De Informatiebeveiligingsdienst kan adviseren - Leg de acties van de genomen maatregelen vast in de tooling	Beveiligingsfunctionaris ICT ICT Manager van waar het incident heeft plaatsgevonden CISO ICT Beveiligingsfunctionaris ICT
4.Vaststellen impact incident	- Onderzoek het incident en de gevolgen daarvan (persoonsniveau en/of organisatieniveau) en stel deze vast. Hiermee kan de urgentie worden bepaald. - Onderzoek het incident en de gevolgen daarvan voor de betrokkene(n). - Onderzoek de omvang van het incident. Hiermee kan de impact worden bepaald.	Manager en/of een ondergeschikte Beveiligingsfunctionarissen Functionaris Gegevensbescherming (beoordeling impact en advies wel/niet melden) Manager en/of een ondergeschikte

	- Beoordeel welke impact het incident kan hebben op de betrokken personen en de organisatie. - Bijlage 1: prioriteren van incidenten op basis van urgentie en impact.	Beveiligingsfunctionarissen Beveiligingsfunctionaris Manager
5. Remediatie en herstel	- Eventueel herstarten van de bedrijfsprocessen als deze gestopt waren als gevolg van het incident. - Een manager kan ervoor kiezen om het risico n.a.v. een incident te accepteren. Dit moet schriftelijk worden vastgelegd. - Als de manager het risico niet accepteert moeten er maatregelen worden geformuleerd en worden geïmplementeerd. - Als een manager niet betrokken is bij het formuleren van de maatregel wordt deze gevraagd of hij of zij akkoord gaat met de maatregel. Na akkoord wordt er overgegaan tot implementatie van deze maatregel. - Beoordelen of de maatregel adequaat genoeg is. Indien dit niet het geval is, is er sprake van een restrisico. - Ook hier kan de manager ervoor kiezen om dit restrisico te accepteren. Ook dit moet worden vastgelegd. - Als de manager het restrisico niet accepteert moeten er aanvullende of andere maatregelen worden geformuleerd en worden geïmplementeerd. - Als een manager niet betrokken is bij het formuleren van de maatregel wordt deze gevraagd of hij of zij akkoord gaat met de maatregel. Na akkoord wordt er overgegaan tot implementatie van deze maatregel.	Manager ICT Manager Beveiligingsfunctionaris Dit is een samenwerking tussen de beveiligingsfunctionarissen, manager en eventueel een ondergeschikte van de manager en/of ICT. Dit is een samenwerking tussen de beveiligingsfunctionarissen, manager en eventueel een ondergeschikte van de manager en/of ICT. Manager Beveiligingsfunctionaris Manager Beveiligingsfunctionaris Dit is een samenwerking tussen de beveiligingsfunctionarissen, manager en eventueel een ondergeschikte van de manager en/of ICT. Dit is een samenwerking tussen de beveiligingsfunctionarissen, manager en eventueel een ondergeschikte van de manager en/of ICT.

6a. Kennisgeving: (eventueel) Melden AP[1]	- Bepaal aanpak/melden AP - Indien besloten wordt om AP te informeren dan moet dat binnen 72 uur (72 uur nadat de verwerkingsverantwoordelijke "kennis" van een inbreuk in verband met persoonsgegevens krijgt) (Zie bijlage 3: stroomschema uit guidelines meldplicht datalekken) - Melding via de website van het AP	Privacy Officer (beoordeling) Manager Functionaris Gegevensbescherming (doen van melding)
6b. Kennisgeving: Melden betrokkenen	- Bepaal aanpak/informeren betrokkenen Melding via bijvoorbeeld brief - Meedelen wat er is gebeurd, welke persoonsgegevens getroffen zijn en wat de mogelijke gevolgen van het datalek kunnen zijn. - Informeren over de maatregelen die de organisatie neemt en die de betrokkene zelf kan nemen om schade te voorkomen	Manager waar het datalek heeft plaatsgevonden (informeren betrokkenen) PO (beoordeling) Functionaris Gegevensbescherming (advies) Marketing/communicatie (advies) Jurist (beperking aansprakelijkheid)
7. Registratie, rapportage en evaluatie	- Registreer, rapporteer en evalueer over het incident. - Terugkoppeling aan de melder	Beveiligingsfunctionarissen (registratie) PO of Functionaris Gegevensbescherming Bestuur (evaluatie) Manager van het team die verantwoordelijk is voor de beveiligingsincidenten (bijvoorbeeld IT) (rapportage)

[1] Een hulpmiddel bij deze beoordeling is de 'voorbeeldlijst wel/niet melden aan AP en betrokkenen' van de Autoriteit Persoonsgegevens:

Bijlage 3: stroomschema guidelines meldplicht datalekken



Bijlage 4: Controls en maatregelen vanuit de BIO aangaande incidenten

- **6.1.3.1** Er is door de organisatie uitgewerkt wie met welke (overheids)instanties en toezichthouders contact heeft ten aanzien van informatiebeveiligingsaangelegenheden (vergunningen/incidenten/ calamiteiten) en welke eisen voor deze aangelegenheden relevant zijn.
- **9.2.5.2** De opvolging van bevindingen is gedocumenteerd en wordt behandeld als beveiligingsincident
- **12.3.1.2** Op basis van een expliciete risicoafweging is bepaald wat het maximaal toegestane dataverlies is en wat de maximale hersteltijd is na een incident.
- **12.3.1.3** In het back-upbeleid staan minimaal de volgende eisen:
    - Dataverlies bedraagt maximaal 28 uur.
    - Hersteltijd in geval van incidenten is maximaal 16 werkuren (twee dagen van 8 uur) in 85% van de gevallen.
- **12.3.1.4** Het back-upproces voorziet in opslag van de back-up op een locatie, waarbij een incident op de ene locatie niet kan leiden tot schade op de andere.
- **12.4.1.1** Een logregel bevat minimaal: de gebeurtenis; de benodigde informatie die nodig is om het incident met hoge mate van zekerheid te herleiden tot een natuurlijk persoon; het gebruikte apparaat; het resultaat van de handeling; een datum en tijdstip van de gebeurtenis.
- **12.4.1.5** De SIEM en/of SOC hebben heldere regels over wanneer een incident moet worden gerapporteerd aan het verantwoordelijk management.
- **12.4.2.4** Oneigenlijk wijzigen of verwijderen van loggegevens of pogingen daartoe worden zo snel mogelijk gemeld als beveiligingsincident via de procedure voor informatiebeveiligingsincidenten conform hoofdstuk 16.
- **16.1.1** Directieverantwoordelijkheden en -procedures behoren te worden vastgesteld om een snelle, doeltreffende en ordelijke respons op informatiebeveiligingsincidenten te bewerkstelligen.
- **16.1.2.1** Er is een meldloket waar beveiligingsincidenten kunnen worden gemeld.
- **16.1.2.2** Er is een meldprocedure waarin de taken en verantwoordelijkheden van het meldloket staan beschreven.
- **16.1.2.3** Alle medewerkers en contractanten hebben aantoonbaar kennisgenomen van de meldingsprocedure van incidenten.
- **16.1.2.4** Incidenten worden zo snel mogelijk, maar in ieder geval binnen 24 uur na bekendwording, intern gemeld.
- **16.1.2.5** De proceseigenaar is verantwoordelijk voor het oplossen van beveiligingsincidenten.
- **16.1.2.6** De opvolging van incidenten wordt maandelijks gerapporteerd aan de verantwoordelijke.
- **16.1.2.7** Informatie afkomstig uit de Coordinated Vulnerability Disclosure (CVD) procedure is onderdeel van de incidentrapportage.
- **16.1.4.1** Informatiebeveiligingsincidenten die hebben geleid tot een vermoedelijk of mogelijk opzettelijke inbreuk op de beschikbaarheid, vertrouwelijkheid of integriteit van informatieverwerkende systemen, behoren zo snel mogelijk (binnen 72 uur) al dan niet geautomatiseerd te worden gemeld aan het NCSC (alleen voor rijksoverheidsorganisaties) of de sectorale CERT.
- **16.1.5** Op informatiebeveiligingsincidenten behoort te worden gereageerd in overeenstemming met de gedocumenteerde procedures.
- **16.1.6** Kennis die is verkregen door informatiebeveiligingsincidenten te analyseren en op te lossen behoort te worden gebruikt om de waarschijnlijkheid of impact van toekomstige incidenten te verkleinen.
- **16.1.6.1** Beveiligingsincidenten worden geanalyseerd met als doel te leren en toekomstige beveiligingsincidenten te voorkomen.
- **16.1.6.2** De analyses van de beveiligingsincidenten worden gedeeld met de relevante partners om herhaling en toekomstige incidenten te voorkomen.
- **16.1.7.1** In geval van een (vermoed) informatiebeveiligingsincident is de bewaartermijn van de gelogde incidentinformatie minimaal drie jaar.