# Afbeelding met kleding, persoon, person, schoeisel Automatisch gegenereerde beschrijvingAfbeelding met tekst, Lettertype, schermopname, Graphics Automatisch gegenereerde beschrijving

Afbeelding met Graphics, clipart, creativiteit

Automatisch gegenereerde beschrijving

Incident Response Plan

**Newmorn’**

**2024-09**

**(IRP)**

# Incident Response Plan (IRP)

## 1. Inleiding

**Doel van het IRP:**

Het doel van dit Incident Response Plan is om de impact van beveiligingsincidenten te minimaliseren, de oorzaak ervan te identificeren en de normale bedrijfsvoering van [Bedrijfsnaam] zo snel mogelijk te herstellen. Dit plan biedt een systematische aanpak om snel en effectief te reageren op verschillende soorten beveiligingsincidenten.

**Omvang:**   
*Geef aan welke systemen, processen en gegevens het IRP dekt.*

Dit IRP dekt alle IT-systemen, netwerken, en databases van [Bedrijfsnaam], inclusief interne en cloudgebaseerde systemen. Het plan is van toepassing op alle afdelingen en werknemers die toegang hebben tot gevoelige bedrijfsinformatie.

## 2. Incident Response Team (IRT)

**Teamstructuur:**  
*Lijst van teamleden met hun contactgegevens en verantwoordelijkheden voor elk lid (bijvoorbeeld IT-specialisten, juridische experts, communicatiemanagers, etc.).*

|  |  |  |  |
| --- | --- | --- | --- |
| **Naam** | **Functie/verantwoordelijkheid** | **E-mailadres** | **Telefoonnummer** |
| [Naam teamleider] |  |  |  |
| [Naam] |  |  |  |
| [Naam] |  |  |  |
| [Naam] |  |  |  |
| [Naam] |  |  |  |
| [Naam] |  |  |  |
| [Naam] |  |  |  |
| [Naam] |  |  |  |

**[Naam]** is aangewezen als hoofd van het Incident Response Team. Hij/zij is verantwoordelijk voor de coördinatie van het team en het nemen van beslissingen tijdens incidenten.

## 3. Incident Classificatie

**Type incidenten:**  
*Lijst van mogelijke beveiligingsincidenten die de organisatie kunnen treffen (bijvoorbeeld phishing, ransomware, datalekken).*

* Phishing-aanvallen
* Ransomware-infecties
* Datalekken
* Ongeautoriseerde toegang tot systemen
* Verlies van apparaten met gevoelige informatie
* Verder...

**Classificatie:**

Incidenten worden geclassificeerd op basis van ernst en impact. Incidenten met een hoog risico hebben de hoogste prioriteit en vereisen onmiddellijke actie. Incidenten met een laag risico kunnen worden behandeld met standaardprocedures.

|  |  |  |  |
| --- | --- | --- | --- |
| **Risico** | **Beschrijving** | **Voorbeelden** | **Actie/prioriteit** |
| Laag | Incidenten met minimale impact en geen gevoelige gegevens betrokken. | Kleine phishing-pogingen, verlies van niet-gevoelige informatie. | Normale actie, binnen 24 uur oplossen. |
| Middel | Incidenten met matige impact, mogelijk met betrokkenheid van gevoelige gegevens, maar beperkte schade. | Malware-infecties zonder dataverlies, ongeautoriseerde toegang zonder datalek | Verhoogde prioriteit, binnen 8 uur oplossen. |
| Hoog | Incidenten met grote impact, gevoelige gegevens betrokken, potentieel ernstige schade | Ransomware-aanvallen, grote datalekken, verlies van gevoelige persoonsgegevens. | Hoge prioriteit, onmiddellijke actie vereist. |

**Prioriteit:**  
*Richtlijnen voor het prioriteren van incidenten op basis van hun classificatie.*

## 4. Incident Response Stappenplan

**Detectie en analyse:**  
Detectie

*Procedures voor het detecteren van incidenten (bijvoorbeeld monitoring tools, meldingen van gebruikers).*

Analyse

*Richtlijnen voor de eerste analyse en beoordeling van het incident.*

**Beperking:**  
*Acties om verdere schade te voorkomen of te minimaliseren (bijvoorbeeld isoleren van geïnfecteerde systemen, blokkeren van verdachte activiteiten).*

**Oplossen:**  
*Stappen om het incident op te lossen en de oorzaak aan te pakken (bijvoorbeeld verwijderen van malware, herstellen van data).*

**Herstel:**  
*Procedures voor het herstellen van de normale bedrijfsvoering (bijvoorbeeld terugzetten van back-ups, herstarten van systemen).* *Post-incident controles om te bevestigen dat het probleem volledig is opgelost.*

**Evaluatie:**  
*Analyse van het incident na afloop.*

*Documenteren van lessen die zijn geleerd en aanbevelingen voor verbetering van het IRP.*

## 5. Communicatieplan

**Interne communicatie:**  
*Richtlijnen voor het informeren van medewerkers en management tijdens een incident.*

**Externe communicatie:**  
*Procedures voor communicatie met klanten, leveranciers en andere externe partijen.*

*Sjablonen voor persberichten en klantcommunicatie.*

**Media en PR:**  
*Aanwijzingen voor het omgaan met de media en het voorkomen van een PR-crisis.*

## 6. Documentatie en Rapportage

**Incident logboek:**

Alle incidenten worden gedocumenteerd in een centraal logboek met tijdlijnen, genomen acties, en resultaten. Dit logboek is toegankelijk voor alle leden van het Incident Response Team.

**Rapportage:**  
*Procedures voor het rapporteren van incidenten aan interne belanghebbenden en indien van toepassing aan externe toezichthouders.*

Incidenten worden gerapporteerd aan het management en, indien van toepassing, aan toezichthouders zoals de Autoriteit Persoonsgegevens.

## 7. Bijlagen

**Contactinformatie:**  
*Gedetailleerde contactinformatie van alle relevante personen en externe partijen (bijvoorbeeld leveranciers van beveiligingssoftware, juridische adviseurs).*

**Sjablonen:**  
*Voorbeelden van interne memo's, persberichten en meldingen aan klanten.*

**Beleid en procedures:**  
*Relevante beleidsdocumenten en procedures die verband houden met incident respons.*

Afbeelding met sinaasappel, Amber, goud, geel

Automatisch gegenereerde beschrijvingAfbeelding met tekst, Lettertype, schermopname, Graphics

Automatisch gegenereerde beschrijving

Flight Forum 40

5657 DB Eindhoven

+31 (0) 6 5312 8317

info@newmorn.nl

**www.newmorn.nl**