09. Proces Incidentmelding

Documentcategorie	Proces
Toelichting	Het Proces Incidentmelding volgens ISO 27001 is essentieel voor het snel detecteren, effectief reageren op en leren van beveiligingsincidenten, wat bijdraagt aan continue verbetering van het informatiebeveiligingsmanagementsysteem (ISMS) en het versterken van de algehele beveiligingsposture van de organisatie.
Eigenaar proces	Security Officer
Status	In werking
Beleid	09. Incidentmanagement
Registraties <>	09. Incidentenregister
Operationele planning <>	OP-16 Beoordelen incidenten en wijzigingen, OP-20 Evaluatie verbeterkansen uit wijzigingen/incidenten/audits
HS 4-10 Clausules (ISO27001:2022)	10.2 Afwijkingen en corrigerende maatregelen
Annex A	A.6.8 Melden van informatiebeveiligingsgebeurtenissen
Uitvoering door	Security Officer, Personeel

▼ Een rootcause analyse door 5 keer waarom te vragen

De 5 Waaroms (The 5 Whys)

De "5 Waaroms" is een probleemoplossingstechniek die wordt gebruikt om de onderliggende oorzaak van een probleem te achterhalen. Deze methode werd oorspronkelijk ontwikkeld door Sakichi Toyoda en werd veel gebruikt binnen Toyota Motor Corporation.

Hoe werkt het?

1. Identificeer het probleem
2. Vraag "Waarom?" en beantwoord
3. Vraag opnieuw "Waarom?" voor het vorige antwoord
4. Herhaal dit proces vijf keer of totdat de hoofdoorzaak is gevonden
5. Wanneer je de hoofdoorzaak hebt gevonden, ontwikkel dan een oplossing

Voorbeeld

Probleem: De auto start niet.

1. *Waarom? - De accu is leeg.*
2. *Waarom? - De dynamo werkt niet goed.*
3. *Waarom? - De aandrijfriem van de dynamo is gebroken.*
4. *Waarom? - De riem was versleten en niet op tijd vervangen.*
5. *Waarom? - Het onderhoudsschema werd niet gevolgd.*

Hoofdoorzaak: Gebrek aan regelmatig onderhoud.

Processtappen

1. Rapporteren van het incident

Een incident wordt gerapporteerd bij de Security Officer en vervolgens toegevoegd aan het

2. Classificatie

In het geval bij een informatiebeveiligingsincident sprake is een 18a. Melding datalek (proces) of 09. Proces Incidentmelding , dienen de betrokken autoriteiten in kennis gesteld te worden .

3. Veiligstellen bewijsmateriaal

Het verzamelen van relevante (logboek) gegevens (van alle betrokken systemen) en veiligstellen van (forensisch) bewijs.

4. Corrigeren van het incident

Het incident wordt gecorrigeerd middels het implementeren van een patch, een tijdelijke oplossing of vervangende maatregelen.

5. Analyse onderliggende oorzaak (Root cause analysis)

De onderliggende oorzaak van het incident wordt vastgesteld op basis van de 5 why method.

6. Vaststellen van de kans op herhaling

Bepaal of de geïdentificeerde onderliggende oorzaak zich vaker kan voordoen

7. Identificeren maatregelen

Vaststellen of de impact kan worden verminderd door het aanpassen/versterken van één of meerdere maatregelen

8. Evaluatie werking

Periodiek wordt het Incidentenregister gecontroleerd ten aanzien van;:

- Voorkomende trends in incidenten (aantallen, onderwerpen/gebieden)
- Effectiviteit van correcties en verbeteringen

Proces uitgebreid

Nr.	Actie	Hoe/wat	Wie	Date	Status
Melding	Medewerker meldt een incident, integriteitsschending of fraudegeval	• Probeert het incident te stoppen indien mogelijk • Meldt het incident (via een mail of een telefoongesprek met de directie) • Legt zoveel mogelijk feiten vast (maak foto's, screenshots)	Medewerker/ incidentmelder		Not started
2 Triage	Behandeling	• Bepalen welke actie nodig is om de schade te beperken en dit uitvoeren	Security Officer		Not started
3 Impactanalyse	Analyseren en bepalen impact incident	• Analyseren informatie en identificeren schade en betrokken middelen en gegevens • Verzamelen en zorgen voor zekerstelling bewijsmateriaal voor eventueel (forensisch) onderzoek • **Bepalen ernst incident:**	Security Officer		Not started
4 Communicatie intern	Informeren directie	• Incidenten met een hoge prioriteit worden onmiddellijk onder de aandacht van de directie gebracht met de status en een advies. • Midden en laag kunnen in de reguliere overleggen worden gemeld aan directie 12a. Voortgangsoverleggen	Security Officer		Not started
5 Aanpak	Beslissen over incidentafwikkeling	• Security Officer bepaalt hoe het incident dient te worden afgewikkeld en verdeelt de rollen • Indien nodig wordt directie betrokken voor besluitvorming	Security Officer		Not started
6 Pleisters plakken?	Inperking gevolgen (directe schadebeperking)	• Beëindigen ongewenste situatie • Voorkoming verder uitbreiding	Security Officer		Not started
7 eerste oorzaakanalyse	Analyse en identificatie van de oorzaak van het incident en vaststelling vervolgstappen	• Direct overleg met betrokkenen gefaciliteerd door Compliance • Vastleggen activiteiten in actielijst • **Indien Datalek met privacy impact betrekken**	Security Officer		Not started

Nr.	Actie	Hoe/wat	Wie	Date	Status
		Directie (zie procedure datalekken)			
7a Betrekken derden	Communicatie met externen	• Communiceren met betrokken stakeholders	Security Officer Directie (hoogste management)		Not started
7b Melding datalek?	Indien noodzakelijk, binnen 24 uur rapporteren van incident en de genomen maatregelen aan klant, de desbetreffende autoriteit of toezichthouder	• **Indien nodig melding aan klant volgens afspraak overeenkomst volgens proces melding datalekken (zie volgende bijlage**) • Niet eerder tenzij vereist	Directie (hoogste management)		Not started
8 Corrigerende maatregelen vastleggen	Vaststellen corrigerende maatregelen voor acceptabel risiconiveau	• Oorzaak-gevolg analyse • Inventarisatie mitigerende maatregelen • Na goedkeuring implementeren aanpassingen	Security Officer Directie		Not started
9 communicatie intern 2	Terugkoppeling afwikkelingen incident en genomen maatregelen	• Aan melder en verdere betrokkenen terugkoppelen oorzaak gevolgen en nemen acties ter voorkoming herhaling incident	Security Officer		Not started
10. Agenda directiebeoordeling					Not started