[logo organisatie]

[naam organisatie]

Comment [DK1]: Alle velden in dit document gemarkeerd met spekhaken [ ] moeten worden ingevuld.

PROCEDURE VOOR INCIDENTBEHEER

Code:	
Versie:	
Versiedatum	
Gemaakt door:	
Goedgekeurd door:	
Classificatie:	

Comment [DK2]: De documentcodering moet in overeenstemming zijn met het bestaande organisatiecoderingssysteem; indien een dergelijk systeem niet is geïmplementeerd, dan kan deze regel worden verwijderd.

Versieblad

Datum	Versie	Gemaakt door	Omschrijving van de aanpassing
DD/MM/JJJJ	0.1	Dejan Kosutic	Concept Basisdocument

Inhoudsopgave

1. Doel, toepassingsgebied en gebruikers

Het doel van doel van dit document is een snelle detectie van beveiligingsgebeurtenissen en –zwakheden te waarborgen, en snelle reactie en antwoord te hebben op beveiligingsincidenten.

Dit document is van toepassing op het hele toepassingsgebied van het Managementsysteem voor Informatiebeveiliging (ISMS), d.w.z. voor zowel alle werknemers en andere gebruikte bedrijfsmiddelen binnen het ISMS-toepassingsgebied, als ook voor leveranciers en andere personen buiten de organisatie die in contact komen met systemen en informatie binnen het ISMS-toepassingsgebied.

Gebruikers van dit document zijn zowel alle werknemers van [naam organisatie], als ook de bovengenoemde personen.

2. Gerefereerde documenten

- ISO/IEC 27001 norm, clausule A.7.2.3, A.16.1.1, A.16.1.2, A.16.1.3, A.16.1.4, A.16.1.5, A.16.1.6, A.16.1.7
- Informatiebeveiligingsbeleid
- [Lijst van Wet-, Regelgeving, Contractuele en Andere Verplichtingen]

Comment [DK3]: Indien u niet over een dergelijke lijst beschikt, vermeld dan in deze bullets de wetgeving en contracten die worden vereist zijn gerelateerd door incidentmanagement.

3. Incidentbeheer

Een informatiebeveiligingsincident is "een enkele of een serie van ongewilde of onverwachte informatiebeveiligingsgebeurtenissen die een significante waarschijnlijkheid van compromitterende bedrijfsoperaties en de informatiebeveiliging bedreigd" (ISO/IEC 27000:2009).

3.1. Ontvangst en classificatie van incidenten, zwakheden en gebeurtenissen

Elke werknemer, leverancier of een andere derde partij die in contact komt met informatie en/of systemen van [naam organisatie] dient elke bedreiging, incident of gebeurtenis aan een systeem die zou kunnen leiden tot een mogelijk incident op de volgende wijze moeten behandelen:

1. alle aan informatie- en communicatietechnologie gerelateerde gebeurtenissen dienen te worden gerapporteerd [functie als contactpunt]
2. alle andere gebeurtenissen dienen te worden gerapporteerd [functie als contactpunt]

Incidenten, bedreigingen en gebeurtenissen dienen zo snel mogelijk te worden gemeld, per telefoon of in persoon.

Comment [DK4]: Andere in gebruik zijnde incidentmeldingsystemen kunnen worden toegevoegd. Bijv. Incidentmeldsystemen, etc.).

De persoon die de informatie ontvangt dient het als volgt te classificeren:

a) beveiligingsbedreiging of gebeurtenis – geen incident trad op, maar de opgemerkte gebeurtenis of eigenschap van een gerelateerd aan een systeem, proces of organisatie kan leiden tot het optreden van een incident in de nabije of verdere toekomst

b) klein incident een incident die geen significante impact op de vertrouwelijkheid of integriteit van de informatie heeft, en niet kan leiden uitval op langere termijn
c) groot incident een incident dat tot significante schade kan leiden door verlies van vertrouwelijkheid of integriteit van informatie, of een onderbreking in de beschikbaarheid van informatie en/of proces voor een onacceptabele periode

3.2. Behandelingsproces voor bedreigingen en gebeurtenissen mbt beveiliging

De persoon die de informatie over een bedreiging of gebeurtenis met betrekking tot de beveiliging heeft ontvangen, analyseert de informatie, stelt de oorzaak vast en stel indien nodig preventieve en corrigerende maatregelen voor.

3.3. Behandeling van kleine incidenten

Indien een klein incident werd gemeld, dan dient de persoon die de informatie ontving de volgende stappen te nemen:

1. maatregelen nemen om het incident te isoleren
2. de oorzaak van het incident analyseren
3. corrigerende te nemen om de oorzaak van het incident weg te nemen
4. zowel personen informeren die bij het incident betrokken waren, als ook [functie] over het incidentbehandelingsproces

De persoon die de informatie over een klein incident ontvangt dient het incident te loggen [beschrijf de manier van het vastleggen handmatig, elektronisch of geautomatiseerd (bijv. door helpdesk applicatie)].

3.4. Behandeling van grote incidenten

In geval van grote incidenten die activiteiten kunnen verstoren voor een onacceptabele periode van tijd dient een Incidentenspoorgang als onderdeel van het Bedrijfscontinuïteitsplan) te worden ingeroepen.

Comment [DK5]: Indien een dergelijk document r[illegible] geval van een majeur incident.

3.5. Leren van incidenten

Comment [DK6]: Verwijder dit item indien beheersmaatregel A.16.1.6 als niet van toepassing in de Verklaring door Toepasselijkheid.

[Functie] dient alle kleine incidenten elke drie maanden te beoordelen en repeterende incidenten of die tot bij de volgende gelegenheid een groot incident kunnen uitgroeien in het Incidentenlogboek in te voeren.

[Functie] dient elk geregistreerd incident in het Incidentenlogboek te analyseren (identificatie type, verbanden, en kosten van het incident) en indien noodzakelijk preventieve of corrigerende maatregelen voor te stellen.

3.6. Disciplinaire maatregelen

Comment [DK7]: Verwijder dit item indien beheersmaatregel A.7.2.3 als niet van toepassing is aangegeven in de Verklaring door Toepasselijkheid.

[Functie] dient een disciplinair proces in te stellen bij elke overtreding van de beveiligingsregels.

Indien een incident een verzameling van bewijs voor juridische maatregelen vereist, dan is [functie]verantwoordelijk voor het verzamelen van dergelijk bewijs in een acceptabel format.

Comment [DK8]: Verwijder dit hele item indien beheersmaatregel A.16.1.7 is als niet van toepassing is aangegeven in de Verklaring van Toepasselijkheid.

3.7. Verzamelen van bewijs

[Functie} zal de regels bepalen over hoe bewijs te identificeren, verzamelen en bewaren dat geaccepteerd zal worden als bewijs in wettelijke en andere handelingen.

4. Registratiebeheer op basis van dit document

Naam registratie	*Opslaglocatie*	*Persoon verantwoordelijk voor opslag*	*Beveiligingsmaatregelen voor registraties*	*Bewaartermijn*
Incidentenlogboek	Gedeelde map op het internet	[functie]	Alleen [functie] heft het recht om het logboek te bewerken	3 jaar
Regels voor identificatie, verzameling en bewaren bewijs	Gedeelde map op het intranet	[functie]	Alleen [functie] heeft het recht om de regels te wijzigen en te publiceren	

Alleen [functie] kan andere werknemers toegang tot de registraties verlenen.

5. Geldigheid en documentbeheer

Dit document is geldig vanaf [datum].

De eigenaar van dit document is [functie]. Hij/zij dient het document te controleren en indien nodig het minstens eens per 6 maanden bij te werken.

Comment [DK9]: Dit is slechts een aanbeveling, pas de frequentie zo nodig aan.

Wanneer de doeltreffendheid en toereikendheid van dit document wordt beoordeeld, dan dienen de volgende criteria in ogenschouw te worden genomen:

- aantal bedreigingen of incidenten die niet aan de geautoriseerde personen zijn gemeld
- aantal incidenten die niet op een toereikende manier zijn behandeld
- aantal incidenten die niet werden geregistreerd in het incidentenlogboek
- aantal incidenten waarvoor het bewijs voor juridische maatregelen ontoereikend was
- aantal overtredingen van beveiligingseisen waar geen disciplinaire proces voor werden opgestart

6. Bijlage

- Incidentenlogboek

[functie]
[naam]

_____
[handtekening]

Comment [DK10]: Alleen noodzakelijk indien de Procedure voor Beheersing voor Documenten en Registraties een ondertekening voorschrijft.