					Voer hier de naam van de geregistreerde rechtspersoon in							
Documentnummer: P30S					Documenttitel: **Incidentresponsbeleid**							
Versie: 1.0		Ingangsdatum: 01.01.2025			Documenteigenaar:							
X	Beleid		Standaard		Procedure		Formulier		Register		Overig	

Revisiegeschiedenis				
Revisienummer	**Revisiedatum**	**Wijzigingen**	**Beoordeeld door**	**Proceseigenaar**

Goedkeuringen			
Naam	**Functie**	**Datum**	**Handtekening**

Afgestemd op normen en regelgeving

Norm/regelgeving	Clausule/artikel	Opmerking
ISO/IEC 27001:2022	Clausules 6.1, 6.3, 8	Incidentbeheer, continue verbetering, operationele beheersing
ISO/IEC 27002:2022	Beheersmaatregelen 5.24, 5.25	Incidentdetectie, paraatheid, lering trekken
NIST SP 800-53 Rev.5	IR-4, IR-5, IR-6	Incidentafhandeling en monitoring, rapportage
AVG	Artikel 33	Vereisten voor het melden van datalekken
NIS2	Artikel 23	Verplichte melding van cyberincidenten
DORA	Artikel 17	ICT-incidentbeheer
COBIT 2019	DSS02, DSS04	Beheer van serviceverzoeken en incidenten, en continuïteit

1. Doel

1.1. Dit beleid bepaalt hoe de organisatie informatiebeveiligingsincidenten detecteert, meldt en afhandelt die gevolgen hebben voor haar digitale systemen, gegevens of diensten.

1.2. Dit beleid stelt de organisatie in staat schade te beperken, klantgegevens te beschermen en te voldoen aan wettelijke verplichtingen, zoals de meldplicht binnen 72 uur op grond van de AVG.

1.3. Dit beleid waarborgt duidelijke verantwoordelijkheden, communicatiestappen en opvolging na incidenten, ook in kleine organisaties zonder een eigen informatiebeveiligingsteam.

2. Reikwijdte

2.1. Dit beleid is van toepassing op:

2.1.1. alle medewerkers, contractanten en externe IT-dienstverleners

2.1.2. alle door de organisatie beheerde systemen en diensten, waaronder websites, cloudplatformen, mobiele apparaten, laptops en e-mailaccounts

2.1.3. alle typen incidenten, waaronder:

2.1.3.1. ongeautoriseerde toegang tot gegevens of systemen

2.1.3.2. malware-infecties of ransomware

2.1.3.3. phishing- of social-engineeringaanvallen

2.1.3.4. systeemuitval als gevolg van een cyberaanval of misbruik

2.1.3.5. onbedoelde openbaarmaking of verwijdering van gevoelige informatie

2.1.3.6. verlies of diefstal van bedrijfsapparatuur of opslagmedia

3. Doelstellingen

3.1. Een duidelijk proces vaststellen voor het herkennen en escaleren van beveiligingsincidenten.

3.2. Waarborgen dat incidenten binnen vooraf vastgestelde termijnen worden gemeld, geregistreerd en opgevolgd.

3.3. Snelle indamming van schade, herstel van gegevens en herstel van dienstverlening mogelijk maken.

3.4. Waarborgen dat getroffen partijen, zoals klanten en toezichthouders, worden geïnformeerd wanneer dit wettelijk vereist is.

3.5. Herhaling voorkomen door middel van oorzaakanalyse, corrigerende maatregelen en beleidsverbetering.

3.6. Het mkb in staat stellen te voldoen aan de vereisten voor ISO/IEC 27001-certificering en verantwoordingsplicht aan te tonen tijdens audits.

4. Rollen en verantwoordelijkheden

4.1. Algemeen directeur

4.1.1. Is eigenaar van dit beleid en waarborgt de implementatie ervan.

4.1.2. Houdt toezicht op incidentresponsactiviteiten en keurt meldingen aan toezichthouders of klanten goed.

4.1.3. Beoordeelt rapportages na incidenten en zorgt ervoor dat het beleid waar nodig wordt geactualiseerd.

4.1.4. Mag coördinatietaken delegeren, maar behoudt de eindverantwoordelijkheid.

4.2. IT-dienstverlener / systeembeheerder (intern of extern)

4.2.1. Detecteert en onderzoekt potentiële beveiligingsincidenten.

4.2.2. Voert indammings- en herstelmaatregelen uit, zoals het intrekken van toegang of het terugzetten van back-ups.

4.2.3. Meldt alle bevestigde of vermoedelijke incidenten binnen 1 uur na constatering aan de algemeen directeur.

4.2.4. Houdt een incidentlogboek bij met tijdstempels, impactbeoordeling en responsmaatregelen.

[... Secties 4.3–8 zijn niet opgenomen in dit voorbeeld. Koop het volledige document voor toegang tot de volledige inhoud. ...]

9. Eisen voor herziening en actualisatie

9.1. Geplande herziening

9.1.1. Dit beleid moet ten minste eenmaal per 12 maanden door de algemeen directeur worden beoordeeld om te waarborgen dat:

9.1.1.1. het aansluit op de beheersmaatregelen van ISO/IEC 27001:2022

9.1.1.2. het inspeelt op nieuwe dreigingen, risico's en incidenten

9.1.1.3. het blijvend voldoet aan wettelijke en contractuele verplichtingen, zoals onder de AVG en DORA

9.2. Triggergebeurtenissen

9.2.1. Het beleid moet ook worden beoordeeld en bijgewerkt na:

9.2.1.1. elk incident met hoge ernst of elke melding aan een toezichthouder

9.2.1.2. de invoering van nieuwe IT-infrastructuur of systeemwijzigingen

9.2.1.3. wijzigingen in wettelijke vereisten met betrekking tot beveiligingsincidenten

9.3. Documentatie en distributie van beoordelingen

9.3.1. Alle beoordelingen en wijzigingen moeten worden vastgelegd in het wijzigingslogboek van het beleid.

9.3.2. Bijgewerkte versies moeten worden verspreid onder alle medewerkers, leveranciers en IT-dienstverleners die betrokken zijn bij beveiliging of systeembeheer.

9.3.3. Bewijsmateriaal van bewustwording bij medewerkers, zoals vergadernotities of bevestigingen per e-mail, moet worden bewaard om naleving tijdens audits aan te tonen.

10. Gerelateerde beleidsdocumenten en samenhang

10.1. Dit beleid moet in samenhang worden toegepast met de volgende mkb-beleidsdocumenten:

10.1.1. P1S – Informatiebeveiligingsbeleid: stelt de algemene verwachtingen vast voor het waarborgen van vertrouwelijkheid, integriteit en beschikbaarheid tijdens de uitvoering van activiteiten, met inbegrip van incidentafhandeling.

10.1.2. P2S – Beleid inzake governancerollen en -verantwoordelijkheden: legt bevoegdheden en verantwoordingsstructuren vast voor incidentdetectie, incidentrapportage en escalatie.

10.1.3. P4S – Toegangscontrolebeleid: maakt onmiddellijke intrekking van toegangsrechten mogelijk tijdens incidentresponsactiviteiten.

10.1.4. P8S – Beleid voor bewustwording en opleiding op het gebied van informatiebeveiliging: waarborgt dat alle medewerkers beveiligingsincidenten effectief kunnen herkennen en melden.

10.1.5. P17S – Beleid inzake gegevensbescherming en privacy: geeft richting aan wettelijke meldingsprocedures voor datalekken onder de AVG en ondersteunt naleving van regelgeving tijdens incidenten.

10.1.6. P22S – Logging- en monitoringbeleid: biedt de benodigde hulpmiddelen en zichtbaarheid voor het detecteren, analyseren en auditen van beveiligingsgebeurtenissen.

10.1.7. P31S – Beleid inzake bewijsverzameling en forensisch onderzoek: ondersteunt onderzoek en juridische verdedigbaarheid van incidentgerelateerde handelingen door richting te geven aan de juiste omgang met bewijsmateriaal.

10.2. Deze beleidsdocumenten vormen gezamenlijk het operationele kader van het mkb voor het detecteren van, reageren op en herstellen van informatiebeveiligingsincidenten.

11. Referentienormen en -raamwerken

11.1. ISO/IEC 27001

11.1.1. Clausule 6.1 – Vereist planning van risicobehandeling, waaronder voorbereiding op incidenten.

11.1.2. Clausule 6.3 – Ondersteunt continue verbetering door lessen te trekken uit beveiligingsgebeurtenissen.

11.1.3. Clausule 8.1 – Benadrukt operationele beheersing voor het beheren van incidenten en verstoringen.

11.2. ISO/IEC 27002

11.2.1. Beheersmaatregel 5.24 – Vereist een gestructureerde aanpak voor het melden, beoordelen en afhandelen van informatiebeveiligingsincidenten.

11.2.2. Beheersmaatregel 5.25 – Richt zich op het leren van incidenten om toekomstige paraatheid en systeemweerbaarheid te verbeteren.

11.3. NIST SP 800-53 Rev.5

11.3.1. IR-4 – Definieert incidentafhandelingsprocedures, waaronder indamming en herstel.

11.3.2. IR-5 – Stelt vereisten vast voor monitoring en analyse van incidenten.

11.3.3. IR-6 – Verplicht protocollen voor externe en interne incidentmelding.

11.4. AVG

11.4.1. Artikel 33 – Verplicht melding van inbreuken in verband met persoonsgegevens aan toezichthouders binnen 72 uur, met informatie over omvang en mitigerende maatregelen.

11.5. NIS2-richtlijn (2022/2555)

11.5.1. Artikel 23 – Verplicht essentiële en belangrijke entiteiten om significante incidenten te melden aan bevoegde autoriteiten met gebruik van gestandaardiseerde meldingsformats.

11.6. DORA-verordening (2022/2554)

11.6.1. Artikel 17 – Verplicht financiële entiteiten om ICT-gerelateerde incidenten en verstoringen te classificeren, te melden en op te volgen.

11.7. COBIT 2019

11.7.1. DSS02 – Serviceverzoeken en incidenten beheren: biedt richting voor doeltreffende afhandeling van operationele incidenten en beveiligingsincidenten in lijn met governancedoelstellingen.

11.7.2. DSS04 – Continuïteit beheren: verbindt incidentrespons met bredere strategieën voor continuïteit en herstel.