					Voer hier de naam van de geregistreerde rechtspersoon in							
Documentnummer: P30					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	Clausule 8.1, Clausule 9	Gestructureerde processen voor risicobeheer en incidentrespons
ISO/IEC 27002:2022	Beheersmaatregelen 5.25–5.27	Rollen, melding, respons en verbetering voor incidenten
NIST SP 800-53 Rev.5	IR-1 tot en met IR-9	Uitgebreide incidentresponslevenscyclus
AVG	Artikel 33(1), 33(3)(a)–(d), 34(1), 34(2)(a)–(c)	Meldtermijnen voor datalekken, rapportage en communicatie met betrokkenen
EU NIS2	Artikel 23(1)–(4)	Melding aan de nationale bevoegde autoriteit en gestructureerde rapportage
EU DORA	Artikel 17(1)–(3)	Rapportage van majeure ICT-gerelateerde incidenten voor financiële entiteiten
COBIT 2019	DSS02, DSS04, MEA	Definieert, monitort en beoordeelt incidentbeheer, bedrijfscontinuïteit en evaluatie

1. Doel

1.1 Dit beleid stelt een formeel kader vast voor de identificatie, melding, analyse, indamming, respons, herstel en post-incidentevaluatie van informatiebeveiligingsincidenten die de organisatie raken.

1.2 Dit beleid waarborgt tijdige, gecoördineerde en doeltreffende responsmaatregelen om operationele verstoring, financieel verlies, reputatieschade en niet-naleving van wet- en regelgeving tot een minimum te beperken.

1.3 Dit beleid ondersteunt tevens de continue verbetering van de cyberweerbaarheid van de organisatie door geleerde lessen en bevindingen uit post-incidentevaluaties te integreren in governance, tooling en opleidingsprogramma's.

2. Reikwijdte

2.1 Dit beleid is van toepassing op:

2.1.1 alle medewerkers, met inbegrip van werknemers, contractanten, consultants en externe dienstverleners

2.1.2 alle informatiesystemen, toepassingen, infrastructuur, netwerken en gegevens, ongeacht of deze on-premises, in de cloud of hybride zijn

2.1.3 alle typen beveiligingsincidenten, met inbegrip van maar niet beperkt tot:

2.1.3.1 ongeautoriseerde toegang of privilege-escalatie

2.1.3.2 malware- en ransomwareaanvallen

2.1.3.3 denial-of-service(DoS/DDoS)-aanvallen

2.1.3.4 gegevensverlies, datalekken of data-exfiltratie

2.1.3.5 misbruik van binnenuit of beleidsovertredingen

2.1.3.6 inbreuken op fysieke beveiliging die digitale bedrijfsmiddelen raken

2.2 Het beleid omvat detectie, triage, onderzoek, escalatie, indamming, bewijsverwerking, melding, herstel en root cause analysis.

3. Doelstellingen

3.1 Het vaststellen van een herhaalbare en schaalbare incidentresponscapaciteit die snelle detectie, classificatie en mitigatie van beveiligingsincidenten mogelijk maakt.

3.2 Het minimaliseren van de bedrijfsimpact van beveiligingsgebeurtenissen door middel van gestructureerde procedures voor indamming, uitroeiing en systeemherstel.

3.3 Waarborgen dat incidentmelding en respons in lijn zijn met wettelijke, regelgevende en contractuele vereisten, in het bijzonder waar het gaat om meldtermijnen voor datalekken en bewijsverwerking.

3.4 Ondersteunen van transparantie en verantwoordingsplicht door middel van adequate auditlogging, documentatie en het monitoren van metrieken voor alle beveiligingsincidenten.

3.5 Bevorderen van continue verbetering door middel van post-incidentevaluatie, corrigerende maatregelen en training van stakeholders.

4. Rollen en verantwoordelijkheden

4.1 Chief Information Security Officer (CISO)

4.1.1 Is eigenaar van het incidentresponsraamwerk, ziet toe op de naleving van dit beleid en houdt toezicht op de organisatiebrede incidentcoördinatie.

4.1.2 Treedt tijdens majeure incidenten op als primair aanspreekpunt voor toezichthouders, het uitvoerend management en externe juridisch adviseurs.

4.2 Incident Response Coordinator

4.2.1 Coördineert multidisciplinaire responsteams, beheert werkstromen en bewaakt de status van indamming en herstel.

4.2.2 Initieert en leidt post-incidentevaluaties (PIR's) en waarborgt dat corrigerende maatregelen worden vastgelegd en uitgevoerd.

[... 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 actualisering

9.1 Dit beleid moet ten minste jaarlijks worden beoordeeld en waar nodig worden herzien om het volgende op te nemen:

9.1.1 wijzigingen in het dreigingslandschap, incidenttypen of aanvalsvectoren

9.1.2 geleerde lessen uit majeure incidenten, bijna-incidenten of bevindingen van toezichthouders

9.1.3 actualiseringen van toepasselijke wet- en regelgeving (bijvoorbeeld AVG, DORA, NIS2)

9.1.4 feedback uit incidentresponsoefeningen en post-incidentevaluaties

9.2 De CISO is verantwoordelijk voor het initiëren en coördineren van het beoordelingsproces, in overleg met:

9.2.1.1 juridisch adviseur en de FG

9.2.1.2 SOC en IT-operaties

9.2.1.3 teams voor bedrijfscontinuïteit en risicobeheer

9.2.1.4 uitvoerend management

9.3 Beleidswijzigingen moeten:

9.3.1 worden gedocumenteerd in een repository onder versiebeheer

9.3.2 worden gecommuniceerd aan alle getroffen teams en worden verwerkt in bewustwordingstrainingen

9.3.3 binnen drie maanden na goedkeuring worden gevalideerd via tabletopoefeningen of live incidentresponsoefeningen

9.4 Spoedeisende actualiseringen die worden getriggerd door opkomende dreigingen, auditbevindingen of nieuw uitgevaardigde wettelijke verplichtingen moeten onmiddellijk worden doorgevoerd en worden opgenomen in de wijzigingshistorie van het beleid.

10. Gerelateerde beleidslijnen en samenhang

10.1 Dit beleid wordt ondersteund door en is afhankelijk van de volgende organisatorische beleidslijnen:

10.1.1 P1 – Informatiebeveiligingsbeleid: stelt de overkoepelende eis vast voor risicogebaseerde en incidentbestendige bedrijfsvoering.

10.1.2 P5 – Wijzigingsbeheerbeleid: waarborgt dat indammings- en herstelactiviteiten met betrekking tot infrastructuur of diensten formele procedures volgen.

10.1.3 P13 – Beleid inzake gegevensclassificatie en etikettering: ondersteunt de ernstclassificatie van incidenten op basis van de gevoeligheid van gegevens.

10.1.4 P15 – Beleid inzake back-up en herstel: maakt herstel mogelijk na ransomware of destructieve aanvallen, met waarborging van integriteit.

10.1.5 P18 – Beleid inzake cryptografische beheersmaatregelen: definieert encryptiemaatregelen die de impact van incidenten en risico's op gegevensblootstelling verkleinen.

10.1.6 P22 – Logging- en monitoringbeleid: biedt de fundamentele zichtbaarheid van gebeurtenissen, alertering en logbewaring die vereist zijn voor doeltreffende detectie en forensisch onderzoek.

10.1.7 P29 – Beleid inzake testgegevens en testomgevingen: waarborgt dat incidenten die niet-productieomgevingen raken eveneens gestructureerd en veilig worden afgehandeld.

10.1.8 P33 – Beleid inzake audit- en nalevingsmonitoring: valideert incidentgereedheid en de doeltreffendheid van incidentrespons via gestructureerde audits en nalevingsbeoordelingen.

11. Referentienormen en -raamwerken

11.1 ISO/IEC 27001: Clausule 8.1 – Operationele planning en beheersing: gestructureerde processen voor het beheren van risico's en de planning van incidentrespons.

11.2 ISO/IEC 27002:2022 – Beheersmaatregelen 5.25–5.27: verantwoordelijkheden voor incidentbeheer, incidentmelding, respons, communicatie en verbetering.

11.3 NIST SP 800-53 Rev.5: IR-1 tot en met IR-9, AU-6, PL-2: uitgebreide vereisten voor de incidentresponslevenscyclus, audit en beveiligingsplanning.

11.4 AVG: Artikel 33/34: meldverplichtingen aan toezichthoudende autoriteiten en vereisten voor kennisgeving aan betrokkenen (met gedefinieerde uitzonderingen).

11.5 EU NIS2-richtlijn (2022/2555): Artikel 23: verplichte nationale melding, met tussentijdse en definitieve rapportageverplichtingen.

11.6 EU DORA (2022/2554): Artikel 17: vereisten voor rapportage van ICT-incidenten door financiële instellingen aan bevoegde autoriteiten.

11.7 COBIT 2019: DSS02, DSS04, MEA01: beheer van service-incidenten en bedrijfscontinuïteit, aangevuld met monitoring van prestaties en conformiteit.