					Voer hier de naam van de geregistreerde rechtspersoon in						
Documentnummer: P39					Documenttitel: **Beleid inzake gecoördineerde kwetsbaarheidsmelding**						
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	6.1.3	
ISO/IEC 27002:2022	5.7, 8.8, 8.9, 8.28, 8.29	
NIST SP 800-53 Rev.5	RA-5, SI-2, PM-15, CA-8, SR-6	
AVG	Art. 32(1)(d)	
EU NIS2	Art. 21(2)(e)	
EU DORA	Art. 11(1)(d)	
COBIT 2019	DSS05.01, DSS05.07, BAI09.02, MEA02.01	

1. Doel

1.1 Het vaststellen van een formeel proces voor het ontvangen, behandelen en openbaar maken van informatie over kwetsbaarheden die van invloed zijn op de systemen of diensten van de organisatie, zoals vereist op grond van artikel 21(2)(e) van NIS2 inzake de behandeling en openbaarmaking van kwetsbaarheden.

1.2 Externe beveiligingsonderzoekers, partners en gebruikers stimuleren om kwetsbaarheden op verantwoorde wijze te melden (Coordinated Vulnerability Disclosure, CVD) en vastleggen hoe de organisatie informatie over kwetsbaarheden aan belanghebbenden communiceert.

2. Reikwijdte

2.1 Dit beleid is van toepassing op alle netwerk- en informatiesystemen die eigendom zijn van of worden beheerd door de organisatie, en op alle geïdentificeerde kwetsbaarheden in deze systemen.

2.2 Dit beleid omvat interne teams (beveiliging, IT, ontwikkeling) en alle externe partijen die kwetsbaarheden melden (bijvoorbeeld onderzoekers, klanten en leveranciers). Het regelt tevens de communicatie met productleveranciers of dienstverleners wanneer hun componenten betrokken zijn bij een kwetsbaarheid.

3. Doelstellingen

3.1 Beveiligingskwetsbaarheden tijdig detecteren en verhelpen met behulp van zowel interne beoordelingen als externe meldingen.

3.2 Duidelijke richtlijnen bieden aan externe melders voor het veilig en rechtmatig indienen van informatie over kwetsbaarheden, en aan de organisatie voor een doeltreffende respons en het treffen van herstelmaatregelen.

3.3 Waarborgen dat wordt voldaan aan de NIS2-vereisten en best practices in de sector (ISO/IEC 29147 en ISO/IEC 30111) voor gecoördineerde openbaarmaking van kwetsbaarheden, ter versterking van de algehele beveiliging van het ecosysteem.

4. Rollen en verantwoordelijkheden

4.1 Vulnerability Response Team (VRT): een aangewezen team, onder leiding van de CISO of de verantwoordelijke voor kwetsbaarhedenbeheer, dat meldingen van kwetsbaarheden ontvangt en triage uitvoert, risico en impact beoordeelt en remediatie en openbare bekendmaking coördineert.

4.2 IT- en ontwikkelingsteams: werken samen met het VRT om gemelde kwetsbaarheden te valideren, patches of mitigerende maatregelen te ontwikkelen en te testen, en oplossingen uit te rollen. Zij leveren waar nodig technische details voor beveiligingsadviezen.

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

9. Monitoring en audit

9.1 Het VRT houdt een register bij voor de openbaarmaking van kwetsbaarheden waarin elke melding van ontvangst tot afsluiting wordt gevolgd. Dit register wordt maandelijks beoordeeld om tijdige voortgang op openstaande items te waarborgen. Achterstallige items worden geëscaleerd.

9.2 De interne audit- en compliancefunctie of een onafhankelijke beveiligingsbeoordelaar beoordeelt jaarlijks de doeltreffendheid van het proces voor de behandeling van kwetsbaarheden, bijvoorbeeld door te controleren of steekproeven van kwetsbaarheidsdossiers overeenkomstig het beleid zijn afgehandeld (ontvangst bevestigd, tijdig opgelost en openbaar gemaakt). Daarbij wordt ook geverifieerd dat het publiek toegankelijke meldkanaal voor openbaarmaking functioneert, bijvoorbeeld of testmails worden ontvangen en opgevolgd.

9.3 Kengetallen over kwetsbaarheden (aantallen naar ernst, remediatietijden enzovoort) worden elk kwartaal opgesteld en voorgelegd aan de cyberbeveiligingsgovernancecommissie ter ondersteuning van actualisaties van de risicobeoordeling.

10. Herziening en onderhoud

10.1 Dit beleid wordt ten minste jaarlijks herzien. Daarnaast leidt elke significante wijziging in onze IT-omgeving, bijvoorbeeld de introductie van een nieuwe dienst die via internet bereikbaar is, of een relevante regelgevende ontwikkeling, bijvoorbeeld nieuwe EU-wetgeving inzake de openbaarmaking van productkwetsbaarheden, tot een tussentijdse herziening.

10.2 Actualisaties van dit beleid verwerken feedback van externe melders en lessen uit interne analyses na incidenten. Majeure wijzigingen worden goedgekeurd door de CISO, gecommuniceerd aan alle werknemers en ter bevordering van transparantie gepubliceerd in onze online beleidsrepository voor informatiebeveiliging.

11. Gerelateerde beleidsdocumenten en samenhang

11.1 P01 – Informatiebeveiligingsbeleid. Managementmandaat voor de behandeling en openbaarmaking van kwetsbaarheden.

11.2 P19 – Beleid inzake kwetsbaarheden- en patchbeheer. Interne remediatiepipeline gekoppeld aan de ontvangst van CVD-meldingen.

11.3 P24 – Beleid inzake veilige ontwikkeling. Borgt dat gemelde issues leiden tot oplossingen en hardening van de Software Development Life Cycle (SDLC).

11.4 P25 – Beleid inzake vereisten voor applicatiebeveiliging. Borgt dat producten beschikken over beveiligingsvereisten die gereed zijn voor openbaarmaking.

11.5 P30 – Incidentresponsbeleid. Behandelt actieve exploitatie van openbaar gemaakte kwetsbaarheden.

11.6 P31 – Beleid inzake bewijsverzameling en forensisch onderzoek. Borgt het behoud van artefacten van gemelde of geëxploiteerde kwetsbaarheden.

11.7 P26 – Leveranciers- en derdepartijbeveiligingsbeleid. Coördineert openbaarmakingen waarbij componenten van leveranciers betrokken zijn.

11.8 P37 – Beleid inzake juridische en regelgevende naleving. Regelt kennisgeving, safe-harborformuleringen en publicatie.

12. Referenties

12.1 NIS2-richtlijn (EU 2022/2555), artikel 21(2), punt (e) (beveiliging in ontwikkeling en behandeling en openbaarmaking van kwetsbaarheden)

12.2 Uitvoeringsverordening (EU) 2024/2690 van de Commissie, bijlage, paragraaf 6.10 (technische vereisten voor processen voor de behandeling en openbaarmaking van kwetsbaarheden)

12.3 ENISA Technical Guidance on Cybersecurity Risk Management Measures – paragraaf over behandeling en openbaarmaking van kwetsbaarheden

12.4 ISO/IEC 27001:2022 / ISO/IEC 27002:2022 (beheersmaatregel 5.7 inzake threat intelligence en openbaarmaking van kwetsbaarheden; beheersmaatregel 8.28 inzake veilige ontwikkeling)

12.5 ISO/IEC 29147:2018 (richtlijnen voor openbaarmaking van kwetsbaarheden) en ISO/IEC 30111:2019 (richtlijnen voor processen voor de behandeling van kwetsbaarheden)