					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: P39					Dokumenttitel: **Policy för samordnad sårbarhetsrapportering**							
Version: 1.0		Ikraftträdandedatum: 01.01.2025			Dokumentägare:							
X	Policy		Standard		Rutin		Formulär		Register		Övrigt	

Revisionshistorik				
Revisionsnummer	**Revisionsdatum**	**Ändringar**	**Granskad av**	**Processägare**

Godkännanden			
Namn	**Titel**	**Datum**	**Underskrift**

Anpassning till standarder och regelverk

Standard/förordning	Klausul/artikel	Kommentar
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	
EU:s GDPR	Art. 32(1)(d)	
EU:s NIS2-direktiv	Art. 21(2)(e)	
EU:s DORA-förordning	Art. 11(1)(d)	
COBIT 2019	DSS05.01, DSS05.07, BAI09.02, MEA02.01	

1. Syfte

1.1 Fastställa en formell process för att ta emot, hantera och lämna information om sårbarheter som påverkar organisationens system eller tjänster, i enlighet med artikel 21.2 e i EU:s NIS2-direktiv avseende hantering och rapportering av sårbarheter.

1.2 Uppmuntra externa säkerhetsforskare, partner och användare att rapportera sårbarheter på ett ansvarsfullt sätt genom samordnad sårbarhetsrapportering (Coordinated Vulnerability Disclosure, CVD) samt definiera hur organisationen kommunicerar sårbarhetsinformation till berörda intressenter.

2. Omfattning

2.1 Denna policy gäller för alla nätverks- och informationssystem som ägs eller drivs av organisationen samt för alla identifierade sårbarheter i dessa system.

2.2 Policyn omfattar interna team inom informationssäkerhet, IT och utveckling samt externa parter som rapporterar sårbarheter, exempelvis forskare, kunder och leverantörer. Den reglerar även kommunikationen med produktleverantörer eller tjänsteleverantörer om deras komponenter påverkas av sårbarheten.

3. Mål

3.1 Upptäcka och åtgärda säkerhetssårbarheter i rätt tid genom att använda både interna bedömningar och externa rapporter.

3.2 Ge tydlig vägledning till externa rapportörer om hur sårbarhetsinformation ska lämnas på ett säkert och rättsenligt sätt samt hur organisationen ska svara och vidta åtgärder effektivt.

3.3 Säkerställa efterlevnad av kraven i EU:s NIS2-direktiv och bästa branschpraxis enligt ISO/IEC 29147 och ISO/IEC 30111 för samordnad sårbarhetsrapportering, för att stärka säkerheten i det övergripande ekosystemet.

4. Roller och ansvar

4.1 Vulnerability Response Team (VRT): Ett utsett team, lett av informationssäkerhetschefen (CISO) eller den som ansvarar för sårbarhetshantering, som tar emot och triagerar sårbarhetsrapporter, bedömer risk och konsekvens samt samordnar åtgärdande och offentliggörande.

4.2 IT- och utvecklingsteam: Samverkar med VRT för att validera rapporterade sårbarheter, utveckla och testa patchar eller riskreducerande åtgärder samt driftsätta korrigeringar. Tillhandahåller vid behov tekniska detaljer till säkerhetsmeddelanden.

[... Avsnitt 4.3–8 ingår inte i denna förhandsvisning. Köp det fullständiga dokumentet för att få tillgång till hela innehållet. ...]

9. Övervakning och revision

9.1 VRT ska upprätthålla en logg över sårbarhetsrapportering som följer varje rapport från mottagande till stängning. Loggen ska granskas månadsvis för att säkerställa att öppna ärenden drivs framåt i rätt tid. Försenade ärenden ska eskaleras.

9.2 Internrevision eller en oberoende säkerhetsbedömare ska årligen granska effektiviteten i processen för sårbarhetshantering, exempelvis genom att kontrollera att ett urval av sårbarhetsärenden har hanterats enligt policyn med bekräftelse, åtgärd och offentliggörande inom rätt tid. De ska även verifiera att den publika rapporteringskanalen fungerar, exempelvis att testmeddelanden tas emot och hanteras.

9.3 Mätetal för sårbarheter, såsom volym per allvarlighetsgrad och åtgärdstider, ska sammanställas kvartalsvis och presenteras för organisationens styrkommitté för cybersäkerhet som underlag för uppdateringar av riskbedömningar.

10. Granskning och underhåll

10.1 Denna policy ska granskas minst årligen. Därutöver ska varje betydande förändring i vår IT-miljö, exempelvis lansering av en ny internetexponerad tjänst, eller relevanta regulatoriska förändringar, exempelvis nya EU-regler om rapportering av produktsårbarheter, föranleda en extra granskning.

10.2 Uppdateringar av policyn ska beakta återkoppling från externa rapportörer och erfarenheter från interna efterincidentanalyser. Väsentliga ändringar ska godkännas av informationssäkerhetschefen (CISO), kommuniceras till samtliga anställda och publiceras i vårt policycenter online för transparens.

11. Relaterade policyer och kopplingar

11.1 P01 – Informationssäkerhetspolicy. Ledningens mandat för hantering och rapportering av sårbarheter.

11.2 P19 – Policy för sårbarhets- och patchhantering. Intern process för åtgärdande kopplad till mottagande genom CVD.

11.3 P24 – Policy för säker utveckling. Tillför korrigeringar och förstärkning av SDLC utifrån rapporterade brister.

11.4 P25 – Policy för applikationssäkerhetskrav. Säkerställer att produkter har säkerhetskrav som möjliggör sårbarhetsrapportering.

11.5 P30 – Policy för incidenthantering. Hanterar aktivt utnyttjande av rapporterade sårbarheter.

11.6 P31 – Policy för bevisinsamling och forensik. Bevarar artefakter från rapporterade eller utnyttjade brister.

11.7 P26 – Policy för leverantörssäkerhet och tredjepartssäkerhet. Samordnar rapporteringar som rör leverantörskomponenter.

11.8 P37 – Policy för rättslig och regulatorisk efterlevnad. Reglerar avisering, safe-harbor-formuleringar och publicering.

12. Referenser

12.1 NIS2-direktivet (EU 2022/2555), artikel 21.2 e (säkerhet i utveckling samt hantering och rapportering av sårbarheter)

12.2 Kommissionens genomförandeförordning (EU) 2024/2690, bilaga avsnitt 6.10 (tekniska krav för processer för hantering och rapportering av sårbarheter)

12.3 ENISA:s tekniska vägledning om åtgärder för cybersäkerhetsriskhantering – avsnitt om hantering och rapportering av sårbarheter

12.4 ISO/IEC 27001:2022 / ISO/IEC 27002:2022 (kontroll 5.7 om hotinformation och sårbarhetsrapportering samt kontroll 8.28 om säker utveckling)

12.5 ISO/IEC 29147:2018 (riktlinjer för sårbarhetsrapportering) och ISO/IEC 30111:2019 (riktlinjer för processer för sårbarhetshantering)