					Indsæt navnet på den registrerede juridiske enhed her						
Dokumentnummer: P39					Dokumenttitel: **Politik for koordineret offentliggørelse af sårbarheder**						
Version: 1.0		Ikrafttrædelsesdato: 01.01.2025			Dokumentejer:						
X	Politik		Standard		Procedure		Formular		Register		Andet

Revisionshistorik				
Revisionsnummer	**Revisionsdato**	**Ændringer**	**Gennemgået af**	**Procesejer**

Godkendelser			
Navn	**Stilling**	**Dato**	**Underskrift**

Tilpasset relevante standarder og reguleringer

Standard/regulering	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 GDPR	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. Formål

1.1 At etablere en formel proces for modtagelse, håndtering og offentliggørelse af oplysninger om sårbarheder, der påvirker organisationens systemer eller tjenester, i overensstemmelse med NIS2 artikel 21(2)(e) om håndtering og offentliggørelse af sårbarheder.

1.2 At tilskynde eksterne sikkerhedsforskere, partnere og brugere til ansvarlig rapportering af sårbarheder (Coordinated Vulnerability Disclosure, CVD) samt fastlægge, hvordan organisationen kommunikerer oplysninger om sårbarheder til interessenter.

2. Omfang

2.1 Denne politik gælder for alle netværks- og informationssystemer, som ejes eller drives af organisationen, samt alle identificerede sårbarheder i disse systemer.

2.2 Politikken omfatter interne teams (informationssikkerhed, IT og udvikling) og alle eksterne parter, der rapporterer sårbarheder (f.eks. forskere, kunder og leverandører). Den regulerer også kommunikation med produktleverandører eller tjenesteudbydere, når deres komponenter indgår i den pågældende sårbarhed.

3. Mål

3.1 At identificere og afhjælpe sikkerhedssårbarheder rettidigt ved hjælp af både interne vurderinger og eksterne indberetninger.

3.2 At fastsætte klare retningslinjer for, hvordan eksterne indberettere sikkert og lovligt indsender oplysninger om sårbarheder, og hvordan organisationen responderer og afhjælper effektivt.

3.3 At sikre overensstemmelse med kravene i NIS2 og branchens bedste praksis (ISO/IEC 29147 og ISO/IEC 30111) for koordineret offentliggørelse af sårbarheder og dermed styrke den samlede sikkerhed i økosystemet.

4. Roller og ansvar

4.1 Vulnerability Response Team (VRT): Et udpeget team (ledet af CISO eller den ansvarlige for sårbarhedsstyring), som modtager og triagerer sårbarhedsrapporter, vurderer risiko og konsekvens samt koordinerer afhjælpning og offentliggørelse.

4.2 IT- og udviklingsteams: Samarbejder med VRT om at validere rapporterede sårbarheder, udvikle og teste patches eller afbødende foranstaltninger samt udrulle rettelser. Leverer tekniske detaljer til sikkerhedsmeddelelser efter behov.

[... Afsnit 4.3–8 er ikke inkluderet i denne forhåndsvisning. Køb det fulde dokument for at få adgang til det komplette indhold. ...]

9. Overvågning og revision

9.1 VRT skal vedligeholde en log over offentliggørelse af sårbarheder, som sporer hver rapport fra modtagelse til lukning. Denne log skal gennemgås månedligt for at sikre rettidig fremdrift i åbne forhold. Forhold, der overskrider fastsatte frister, skal eskaleres.

9.2 Intern revision eller en uafhængig part med ansvar for sikkerhedsvurdering skal årligt gennemgå effektiviteten af processen for håndtering af sårbarheder, f.eks. ved at kontrollere, at stikprøver af sårbarhedssager er håndteret i overensstemmelse med politikken (bekræftet, rettet og offentliggjort rettidigt). Derudover skal det verificeres, at den offentligt tilgængelige rapporteringskanal fungerer (f.eks. at test-e-mails modtages og håndteres).

9.3 Metrikker om sårbarheder (omfang efter alvorlighed, afhjælpningstider mv.) skal sammenstilles kvartalsvist og præsenteres for cybersikkerhedens styringskomité med henblik på opdatering af risikovurderinger.

10. Gennemgang og vedligeholdelse

10.1 Denne politik skal gennemgås mindst én gang årligt. Derudover skal enhver væsentlig ændring i vores IT-miljø (f.eks. idriftsættelse af en ny internetvendt tjeneste) eller relevante regulatoriske ændringer (f.eks. ny EU-lovgivning om offentliggørelse af produktsårbarheder) udløse en ekstraordinær gennemgang.

10.2 Opdateringer af politikken skal indarbejde feedback fra eksterne indberettere og læringspunkter fra interne efterhændelsesanalyser. Væsentlige ændringer skal godkendes af CISO og kommunikeres til alle medarbejdere samt offentliggøres i vores online-repositorium for sikkerhedspolitikker af hensyn til gennemsigtighed.

11. Relaterede politikker og sammenhænge

11.1 P01 – Informationssikkerhedspolitik. Ledelsesmæssigt mandat for håndtering og offentliggørelse af sårbarheder.

11.2 P19 – Politik for sårbarheds- og patchstyring. Intern afhjælpningsproces knyttet til modtagelse under CVD.

11.3 P24 – Politik for sikker udvikling. Understøtter rettelser og hærdning af SDLC på baggrund af rapporterede forhold.

11.4 P25 – Politik for krav til applikationssikkerhed. Sikrer, at produkter har sikkerhedskrav, der understøtter offentliggørelse af sårbarheder.

11.5 P30 – Politik for hændelseshåndtering. Håndterer aktiv udnyttelse af offentliggjorte sårbarheder.

11.6 P31 – Politik for indsamling af bevismateriale og digital efterforskning. Bevarer artefakter fra rapporterede eller udnyttede fejl.

11.7 P26 – Politik for tredjeparts- og leverandørsikkerhed. Koordinerer offentliggørelser, der involverer leverandørkomponenter.

11.8 P37 – Politik for juridisk og regulatorisk efterlevelse. Regulerer underretning, formulering af safe harbor og offentliggørelse.

12. Referencer

12.1 NIS2-direktivet (EU 2022/2555), artikel 21(2), litra (e) (sikkerhed i udvikling samt håndtering og offentliggørelse af sårbarheder)

12.2 Kommissionens gennemførelsesforordning (EU) 2024/2690, bilag, afsnit 6.10 (tekniske krav til processer for håndtering og offentliggørelse af sårbarheder)

12.3 ENISA Technical Guidance on Cybersecurity Risk Management Measures – afsnit om håndtering og offentliggørelse af sårbarheder

12.4 ISO/IEC 27001:2022 / ISO/IEC 27002:2022 (kontrol 5.7 om trusselsinformation og offentliggørelse af sårbarheder; kontrol 8.28 om sikker udvikling)

12.5 ISO/IEC 29147:2018 (retningslinjer for offentliggørelse af sårbarheder) og ISO/IEC 30111:2019 (retningslinjer for processer til håndtering af sårbarheder)