					Indsæt navnet på den registrerede juridiske enhed her							
Dokumentnummer: P30					Dokumenttitel: **Politik for hændelseshåndtering**							
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 regler

Standard/regulering	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Klausul 8.1, klausul 9	Strukturerede processer for risikostyring og hændelseshåndtering
ISO/IEC 27002:2022	Kontroller 5.25–5.27	Roller, rapportering, respons og forbedring ved hændelser
NIST SP 800-53 Rev.5	IR-1 til IR-9	Omfattende livscyklus for hændelseshåndtering
EU GDPR	Artikel 33(1), 33(3)(a)–(d), 34(1), 34(2)(a)–(c)	Frister for anmeldelse af brud, rapportering og kommunikation til registrerede
EU NIS2	Artikel 23(1)–(4)	Underretning til nationale myndigheder og struktureret rapportering
EU DORA	Artikel 17(1)–(3)	Rapportering af større IKT-relaterede hændelser for finansielle enheder
COBIT 2019	DSS02, DSS04, MEA	Definerer, overvåger og vurderer hændelseshåndtering, forretningskontinuitet og evaluering

1. Formål

1.1 Denne politik fastlægger en formel struktur for identifikation, rapportering, analyse, inddæmning, håndtering, genopretning og efterhændelsesgennemgang af informationssikkerhedshændelser, der påvirker organisationen.

1.2 Den skal sikre rettidige, koordinerede og effektive indsatser for at minimere driftsforstyrrelser, økonomiske tab, omdømmeskade og manglende efterlevelse af regulatoriske krav.

1.3 Politikken understøtter også løbende forbedring af organisationens cyberrobusthed gennem erfaringsopsamling og integration af resultater fra efterhændelsesgennemgange i styring, værktøjer og træningsprogrammer.

2. Omfang

2.1 Denne politik gælder for:

2.1.1 Alt personale, herunder medarbejdere, kontrahenter, konsulenter og tredjepartsleverandører

2.1.2 Alle informationssystemer, applikationer, infrastrukturer, netværk og data, uanset om de er on-premises, i cloudmiljøer eller i hybride miljøer

2.1.3 Alle typer sikkerhedshændelser, herunder, men ikke begrænset til:

2.1.3.1 Uautoriseret adgang eller rettighedseskalering

2.1.3.2 Malware- og ransomwareangreb

2.1.3.3 Denial-of-service-angreb (DoS/DDoS)

2.1.3.4 Datatab, datalækage eller dataeksfiltrering

2.1.3.5 Misbrug fra interne aktører eller overtrædelser af politikker

2.1.3.6 Brud på fysisk sikring, der påvirker digitale aktiver

2.2 Politikken omfatter detektion, triage, undersøgelse, eskalering, inddæmning, håndtering af bevismateriale, underretning, genopretning og rodårsagsanalyse.

3. Mål

3.1 At etablere en gentagelig og skalerbar kapacitet til hændelseshåndtering, som muliggør hurtig detektion, klassificering og afbødning af sikkerhedshændelser.

3.2 At minimere den forretningsmæssige påvirkning af sikkerhedshændelser gennem strukturerede procedurer for inddæmning, fjernelse og systemgenopretning.

3.3 At sikre, at hændelsesrapportering og hændelseshåndtering er i overensstemmelse med juridiske, regulatoriske og kontraktuelle krav, særligt krav vedrørende frister for anmeldelse af brud og håndtering af bevismateriale.

3.4 At understøtte transparens og ansvarlighed gennem korrekt logning, dokumentation og måling for alle sikkerhedshændelser.

3.5 At fremme løbende forbedring gennem efterhændelsesgennemgange, korrigerende handlinger og træning af interessenter.

4. Roller og ansvar

4.1 Chief Information Security Officer (CISO)

4.1.1 Har det overordnede ansvar for rammeværket for hændelseshåndtering, sikrer håndhævelse af politikken og fører tilsyn med koordinering af hændelser på tværs af hele organisationen.

4.1.2 Fungerer som primær kontakt til tilsynsmyndigheder, topledelse og ekstern juridisk rådgivning under større hændelser.

4.2 Hændelseskoordinator

4.2.1 Koordinerer tværgående responsteams, styrer arbejdsgange og følger status på inddæmning og genopretning.

4.2.2 Iværksætter og leder efterhændelsesgennemgange og sikrer, at korrigerende handlinger registreres og gennemføres.

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

9. Krav til gennemgang og opdatering

9.1 Denne politik skal gennemgås mindst én gang årligt og revideres efter behov for at indarbejde:

9.1.1 Ændringer i trusselslandskabet, hændelsestyper eller angrebsvektorer

9.1.2 Erfaringer fra større hændelser, nærvedhændelser eller regulatoriske konstateringer

9.1.3 Opdateringer af gældende love og regler (f.eks. GDPR, DORA, NIS2)

9.1.4 Feedback fra øvelser i hændelseshåndtering og efterhændelsesgennemgange

9.2 CISO'en er ansvarlig for at igangsætte og koordinere gennemgangsprocessen i samråd med:

9.2.1.1 Juridisk rådgivning og DPO

9.2.1.2 SOC og IT-drift

9.2.1.3 Teams for forretningskontinuitet og risikostyring

9.2.1.4 Topledelsen

9.3 Ændringer i politikken skal:

9.3.1 Dokumenteres i et versionsstyret repository

9.3.2 Kommunikeres til alle berørte teams og opdateres i awareness-træning i informationssikkerhed

9.3.3 Valideres gennem tabletop-øvelser eller liveøvelser i hændelseshåndtering inden for tre måneder efter godkendelse

9.4 Hasteopdateringer udløst af fremspirende risici, revisionskonstateringer eller nye juridiske forpligtelser skal gennemføres straks og registreres i politikkens revisionshistorik.

10. Relaterede politikker og sammenhænge

10.1 Denne politik understøttes af og er afhængig af følgende organisatoriske politikker:

10.1.1 P1 – Informationssikkerhedspolitik: Fastlægger det overordnede krav om risikobaseret drift med beredskab for hændelser.

10.1.2 P5 – Politik for ændringsstyring: Sikrer, at inddæmnings- og genopretningsaktiviteter, som involverer infrastruktur eller tjenester, følger formelle procedurer.

10.1.3 P13 – Politik for dataklassificering og mærkning: Understøtter klassificering af hændelsers alvorlighed på baggrund af datafølsomhed.

10.1.4 P15 – Politik for backup og gendannelse: Muliggør genopretning efter ransomware eller destruktive angreb med sikkerhed for integritet.

10.1.5 P18 – Politik for kryptografiske kontroller: Definerer krypteringsforanstaltninger, der reducerer hændelsers konsekvens og risikoen for dataeksponering.

10.1.6 P22 – Lognings- og overvågningspolitik: Giver den grundlæggende synlighed i hændelser, alarmering og logopbevaring, der kræves for effektiv detektion og it-forensik.

10.1.7 P29 – Politik for testdata og testmiljøer: Sikrer, at hændelser, der påvirker ikke-produktionsmiljøer, også håndteres struktureret og sikkert.

10.1.8 P33 – Politik for revisions- og efterlevelsesovervågning: Validerer beredskab og effektivitet i hændelseshåndtering gennem strukturerede revisioner og efterlevelsesvurderinger.

11. Referencestandarder og rammeværker

11.1 ISO/IEC 27001: Klausul 8.1 – operationel planlægning og styring: Strukturerede processer til styring af risici og planlægning af hændelseshåndtering.

11.2 ISO/IEC 27002:2022 – Kontroller 5.25–5.27: Ansvar for hændelseshåndtering, rapportering, håndtering, kommunikation og forbedring.

11.3 NIST SP 800-53 Rev.5: IR-1 til IR-9, AU-6, PL-2: Omfattende krav til livscyklus for hændelseshåndtering, revision og sikkerhedsplanlægning.

11.4 EU GDPR: Artikel 33/34: Rapporteringsforpligtelser over for tilsynsmyndigheder og krav til underretning af registrerede (med definerede undtagelser).

11.5 EU NIS2-direktivet (2022/2555): Artikel 23: Obligatorisk national rapportering med krav om mellemliggende og endelig rapportering.

11.6 EU DORA (2022/2554): Artikel 17: Krav til rapportering af IKT-hændelser til myndigheder for finansielle institutioner.

11.7 COBIT 2019: DSS02, DSS04, MEA01: Styring af servicehændelser og forretningskontinuitet samt overvågning af performance og overensstemmelse.