					Indsæt navnet på den registrerede juridiske enhed her							
Dokumentnummer: P30S					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 reguleringer

Standard/regulering	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Klausul 6.1, 6.3, 8	hændelseshåndtering, løbende forbedring, operationel planlægning og styring
ISO/IEC 27002:2022	Kontrol 5.24, 5.25	hændelsesdetektion, beredskab, læring
NIST SP 800-53 Rev.5	IR-4, IR-5, IR-6	hændelseshåndtering og overvågning, hændelsesrapportering
EU GDPR	Artikel 33	krav til anmeldelse af brud på persondatasikkerheden
EU NIS2	Artikel 23	obligatorisk rapportering af cyberhændelser
EU DORA	Artikel 17	styring af IKT-hændelser
COBIT 2019	DSS02, DSS04	styring af serviceanmodninger og hændelser samt forretningskontinuitet

1. Formål

1.1. Denne politik fastlægger, hvordan organisationen detekterer, rapporterer og håndterer sikkerhedshændelser, der påvirker dens digitale systemer, data eller tjenester.

1.2. Politikken skal sætte organisationen i stand til at minimere skade, beskytte kundedata og opfylde regulatoriske forpligtelser, herunder GDPR's krav om anmeldelse af brud på persondatasikkerheden inden for 72 timer.

1.3. Politikken sikrer klare ansvarsforhold, kommunikationsveje og opfølgning efter hændelser, også i mindre organisationer uden et dedikeret sikkerhedsteam.

2. Omfang

2.1. Denne politik gælder for:

2.1.1. Alle medarbejdere, kontrahenter og eksterne IT-tjenesteudbydere

2.1.2. Alle virksomhedsadministrerede systemer og tjenester, herunder websites, cloudplatforme, mobile enheder, bærbare computere og e-mailkonti

2.1.3. Alle typer hændelser, herunder:

2.1.3.1. uautoriseret adgang til data eller systemer

2.1.3.2. malwareinfektioner eller ransomware

2.1.3.3. phishing eller forsøg på social engineering

2.1.3.4. systemnedbrud som følge af cyberangreb eller misbrug

2.1.3.5. utilsigtet videregivelse eller sletning af følsomme oplysninger

2.1.3.6. tab eller tyveri af forretningsenheder eller lagringsmedier

3. Mål

3.1. Etablere en klar proces for identifikation og eskalering af sikkerhedshændelser.

3.2. Sikre, at hændelser rapporteres, registreres og håndteres inden for på forhånd fastsatte tidsfrister.

3.3. Muliggøre hurtig inddæmning af skade, datagendannelse og genetablering af tjenester.

3.4. Sikre, at berørte parter, f.eks. kunder og tilsynsmyndigheder, underrettes, når dette følger af lovgivningen.

3.5. Forebygge gentagelser gennem rodårsagsanalyse, korrigerende handlinger og forbedring af politikken.

3.6. Sætte SMV'er i stand til at opfylde krav til ISO 27001-certificering og dokumentere ansvarlighed under revisioner.

4. Roller og ansvar

4.1. Direktør

4.1.1. Er ejer af denne politik og sikrer, at den implementeres.

4.1.2. Fører tilsyn med hændelseshåndteringsaktiviteter og godkender anmeldelser til tilsynsmyndigheder eller kunder.

4.1.3. Gennemgår rapporter efter hændelser og sikrer, at politikken opdateres efter behov.

4.1.4. Kan delegere koordineringsopgaver, men bevarer ansvaret.

4.2. IT-leverandør/systemadministrator (intern eller ekstern)

4.2.1. Detekterer og undersøger potentielle sikkerhedshændelser.

4.2.2. Iværksætter inddæmnings- og genopretningsaktiviteter, f.eks. deaktivering af adgang og gendannelse fra sikkerhedskopier.

4.2.3. Underretter direktøren om alle bekræftede eller mistænkte hændelser inden for 1 time efter opdagelse.

4.2.4. Vedligeholder en hændelseslog med tidsstempler, konsekvensvurdering og responsaktiviteter.

[... 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. Planlagt gennemgang

9.1.1. Denne politik skal gennemgås mindst én gang hver 12. måned af direktøren for at sikre:

9.1.1.1. overensstemmelse med kontroller i ISO/IEC 27001:2022

9.1.1.2. reaktionsevne over for nye trusler, risici og hændelser

9.1.1.3. fortsat efterlevelse af juridiske og kontraktlige forpligtelser, f.eks. GDPR og DORA

9.2. Udløsende hændelser

9.2.1. Politikken skal også gennemgås og opdateres efter:

9.2.1.1. enhver hændelse med høj alvorlighed eller anmeldelse til tilsynsmyndighed

9.2.1.2. indførelse af ny IT-infrastruktur eller systemændringer

9.2.1.3. ændringer i lovkrav vedrørende sikkerhedsbrud

9.3. Dokumentation for gennemgang og distribution

9.3.1. Alle gennemgange og ændringer skal dokumenteres i politikkens ændringslog.

9.3.2. Opdaterede versioner skal distribueres til alle medarbejdere, leverandører og IT-leverandører, der er involveret i sikkerhed eller systemdrift.

9.3.3. Dokumentation for medarbejdernes sikkerhedsbevidsthed, f.eks. mødereferater eller e-mailbekræftelser, skal opbevares af hensyn til revisionsberedskab.

10. Relaterede politikker og sammenhænge

10.1. Denne politik skal anvendes i sammenhæng med følgende SME-politikker:

10.1.1. P1S – Informationssikkerhedspolitik: Fastlægger de overordnede forventninger til opretholdelse af fortrolighed, integritet og tilgængelighed i driften, herunder hændelseshåndtering.

10.1.2. P2S – Politik for styringsroller og ansvarsområder: Fastlægger strukturer for beføjelser og ansvar for hændelsesdetektion, hændelsesrapportering og eskalering.

10.1.3. P4S – Politik for adgangskontrol: Muliggør øjeblikkelig tilbagekaldelse af adgangsrettigheder under hændelseshåndtering.

10.1.4. P8S – Politik for informationssikkerhedsbevidsthed og uddannelse: Sikrer, at alle medarbejdere effektivt kan identificere og rapportere sikkerhedshændelser.

10.1.5. P17S – Databeskyttelses- og privatlivspolitik: Vejleder om juridiske procedurer for anmeldelse af brud efter GDPR og understøtter efterlevelse af regulatoriske krav under hændelser.

10.1.6. P22S – Politik for logning og overvågning: Leverer de nødvendige værktøjer og den nødvendige synlighed til at detektere, analysere og revidere sikkerhedshændelser.

10.1.7. P31S – Politik for indsamling af bevismateriale og it-forensik: Understøtter undersøgelse og juridisk forsvarlighed af hændelsesrelaterede handlinger ved at vejlede om korrekt håndtering af bevismateriale.

10.2. Disse politikker udgør samlet SMV'ens operationelle ramme for at detektere, håndtere og genoprette efter sikkerhedshændelser.

11. Referencestandarder og rammeværker

11.1. ISO/IEC 27001

11.1.1. Klausul 6.1 – Kræver planlægning af risikobehandling, herunder forberedelse til hændelser.

11.1.2. Klausul 6.3 – Understøtter løbende forbedring gennem læring fra sikkerhedshændelser.

11.1.3. Klausul 8.1 – Fremhæver operationel planlægning og styring for at håndtere hændelser og driftsforstyrrelser.

11.2. ISO/IEC 27002

11.2.1. Kontrol 5.24 – Kræver en struktureret tilgang til rapportering, vurdering og håndtering af sikkerhedshændelser.

11.2.2. Kontrol 5.25 – Fokuserer på læring fra hændelser for at forbedre fremtidigt beredskab og systemernes robusthed.

11.3. NIST SP 800-53 Rev.5

11.3.1. IR-4 – Definerer procedurer for hændelseshåndtering, herunder inddæmning og genopretning.

11.3.2. IR-5 – Fastlægger krav til hændelsesovervågning og analyse.

11.3.3. IR-6 – Kræver protokoller for ekstern og intern hændelsesrapportering.

11.4. EU GDPR

11.4.1. Artikel 33 – Kræver anmeldelse af brud på persondatasikkerheden til tilsynsmyndigheder inden for 72 timer med oplysninger om omfang og afbødning.

11.5. EU NIS2-direktivet (2022/2555)

11.5.1. Artikel 23 – Kræver, at væsentlige og vigtige enheder underretter kompetente myndigheder om væsentlige hændelser ved brug af standardiserede rapporteringsformater.

11.6. EU DORA-forordningen (2022/2554)

11.6.1. Artikel 17 – Kræver, at finansielle enheder klassificerer, rapporterer og sporer IKT-relaterede hændelser og driftsforstyrrelser.

11.7. COBIT 2019

11.7.1. DSS02 – Manage Service Requests and Incidents: Vejleder om effektiv håndtering af driftsmæssige hændelser og sikkerhedshændelser i overensstemmelse med styringsmål.

11.7.2. DSS04 – Manage Continuity: Forbinder hændelseshåndtering med bredere strategier for forretningskontinuitet og genopretning.