					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: P30S					Dokumenttitel: **Policy för incidenthantering**							
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 där tillämpligt

Standard/regelverk	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Klausul 6.1, 6.3, 8	Incidenthantering, kontinuerlig förbättring, operativ styrning
ISO/IEC 27002:2022	Kontroller 5.24, 5.25	Incidentdetektering, beredskap, lärande
NIST SP 800-53 Rev. 5	IR-4, IR-5, IR-6	Incidenthantering och övervakning, rapportering
EU:s dataskyddsförordning (GDPR)	Artikel 33	Krav på anmälan av personuppgiftsincidenter
EU:s NIS2-direktiv	Artikel 23	Obligatorisk rapportering av cyberincidenter
EU:s DORA-förordning	Artikel 17	Hantering av IKT-relaterade incidenter
COBIT 2019	DSS02, DSS04	Hantering av tjänstebegäranden och incidenter samt kontinuitet

1. Syfte

1.1. Denna policy anger hur organisationen identifierar, rapporterar och hanterar informationssäkerhetsincidenter som påverkar dess digitala system, data eller tjänster.

1.2. Policyn gör det möjligt för organisationen att minimera skador, skydda kunddata och uppfylla regulatoriska skyldigheter, såsom GDPR:s krav på anmälan av personuppgiftsincidenter inom 72 timmar.

1.3. Policyn säkerställer tydliga ansvarsförhållanden, kommunikationsvägar och uppföljning efter incidenter, även i mindre organisationer utan ett dedikerat säkerhetsteam.

2. Omfattning

2.1. Denna policy gäller för:

2.1.1. alla anställda, entreprenörer och tredjepartsleverantörer

2.1.2. alla system och tjänster som företaget hanterar, inklusive webbplatser, molnplattformar, mobila enheter, bärbara datorer och e-postkonton

2.1.3. alla typer av incidenter, inklusive:

2.1.3.1. obehörig åtkomst till data eller system

2.1.3.2. skadlig kod eller ransomwareinfektioner

2.1.3.3. nätfiskeförsök eller försök till social manipulation

2.1.3.4. systemavbrott till följd av cyberattack eller felaktig användning

2.1.3.5. oavsiktligt röjande eller oavsiktlig radering av känslig information

2.1.3.6. förlust eller stöld av verksamhetsutrustning eller lagringsmedier

3. Mål

3.1. Fastställa en tydlig process för att identifiera och eskalera säkerhetsincidenter.

3.2. Säkerställa att incidenter rapporteras, loggas och hanteras inom fastställda tidsramar.

3.3. Möjliggöra snabb skadebegränsning samt återställning av data och tjänster.

3.4. Säkerställa att berörda parter, exempelvis kunder och tillsynsmyndigheter, underrättas när detta krävs enligt lag.

3.5. Förhindra upprepning genom rotorsaksanalys (RCA), korrigerande åtgärder och förbättring av policyn.

3.6. Möjliggöra att SME uppfyller krav för ISO 27001-certifiering och kan påvisa ansvarsskyldighet vid revisioner.

4. Roller och ansvar

4.1. Verkställande chef (GM)

4.1.1. Är policyägare för denna policy och säkerställer att den genomförs.

4.1.2. Utövar tillsyn över incidenthanteringsaktiviteter och godkänner anmälningar till tillsynsmyndigheter eller notifieringar till kunder.

4.1.3. Granskar rapporter efter incidenter och säkerställer att policyuppdateringar genomförs vid behov.

4.1.4. Får delegera samordningsuppgifter men behåller ansvarsskyldigheten.

4.2. IT-supportleverantör/systemadministratör (intern eller extern)

4.2.1. Identifierar och utreder potentiella säkerhetsincidenter.

4.2.2. Genomför skadebegränsande åtgärder och återställning, till exempel genom att inaktivera åtkomst eller återläsa säkerhetskopior.

4.2.3. Ska underrätta GM om alla bekräftade eller misstänkta incidenter inom en timme från upptäckt.

4.2.4. Upprätthåller en incidentlogg med tidsstämplar, konsekvensbedömning och vidtagna åtgärder.

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

9. Krav för granskning och uppdatering

9.1. Planerad granskning

9.1.1. Denna policy ska granskas minst en gång var 12:e månad av verkställande chef (GM) för att säkerställa:

9.1.1.1. anpassning till kontroller i ISO/IEC 27001:2022

9.1.1.2. förmåga att hantera nya hot, risker och incidenter

9.1.1.3. fortsatt efterlevnad av rättsliga skyldigheter och avtalskrav, till exempel enligt GDPR och DORA

9.2. Utlösande händelser

9.2.1. Policyn ska även granskas och uppdateras efter:

9.2.1.1. varje incident med hög allvarlighetsgrad eller regulatorisk anmälan/notifiering

9.2.1.2. införande av ny IT-infrastruktur eller systemändringar

9.2.1.3. ändringar i rättsliga krav avseende säkerhetsincidenter

9.3. Dokumentation av granskning och distribution

9.3.1. Alla granskningar och ändringar ska dokumenteras i policyns ändringslogg.

9.3.2. Uppdaterade versioner ska distribueras till alla anställda, leverantörer och IT-supportleverantörer som är involverade i säkerhet eller systemdrift.

9.3.3. Underlag som visar personalens medvetenhet, till exempel mötesanteckningar eller e-postbekräftelser, ska bevaras för revisionsberedskap.

10. Relaterade policyer och kopplingar

10.1. Denna policy ska tillämpas samordnat med följande SME-policyer:

10.1.1. P1S – Informationssäkerhetspolicy: Anger övergripande förväntningar för att upprätthålla konfidentialitet, riktighet och tillgänglighet i verksamheten, inklusive incidenthantering.

10.1.2. P2S – Policy för styrningsroller och ansvar: Fastställer befogenhets- och ansvarighetsstrukturer för incidentdetektering, rapportering och eskalering.

10.1.3. P4S – Policy för åtkomstkontroll: Möjliggör omedelbar återkallelse av åtkomst vid incidenthanteringsåtgärder.

10.1.4. P8S – Policy för informationssäkerhetsmedvetenhet och utbildning: Säkerställer att alla anställda effektivt kan identifiera och rapportera säkerhetsincidenter.

10.1.5. P17S – Policy för dataskydd och integritet: Vägleder rättsliga processer för incidentanmälan enligt GDPR och stödjer regelefterlevnad vid incidenter.

10.1.6. P22S – Policy för loggning och övervakning: Tillhandahåller nödvändiga verktyg och den insyn som krävs för att identifiera, analysera och granska säkerhetshändelser.

10.1.7. P31S – Policy för bevisinsamling och forensik: Stödjer utredning och rättslig hållbarhet i incidentrelaterade åtgärder genom att vägleda korrekt hantering av bevismaterial.

10.2. Dessa policyer utgör tillsammans SME:s operativa ramverk för att identifiera, hantera och återhämta sig från informationssäkerhetsincidenter.

11. Referensstandarder och ramverk

11.1. ISO/IEC 27001

11.1.1. Klausul 6.1 – Kräver planering av riskbehandling, inklusive förberedelser för incidenter.

11.1.2. Klausul 6.3 – Stödjer kontinuerlig förbättring genom lärdomar från säkerhetsincidenter.

11.1.3. Klausul 8.1 – Betonar operativ styrning för att hantera incidenter och störningar.

11.2. ISO/IEC 27002

11.2.1. Kontroll 5.24 – Kräver ett strukturerat arbetssätt för att rapportera, bedöma och hantera informationssäkerhetsincidenter.

11.2.2. Kontroll 5.25 – Fokuserar på lärande från incidenter för att förbättra framtida beredskap och systemens resiliens.

11.3. NIST SP 800-53 Rev. 5

11.3.1. IR-4 – Definierar incidenthanteringsrutiner inklusive skadebegränsning och återställning.

11.3.2. IR-5 – Fastställer krav för incidentövervakning och analys.

11.3.3. IR-6 – Kräver rutiner för extern och intern incidentrapportering.

11.4. EU:s dataskyddsförordning (GDPR)

11.4.1. Artikel 33 – Kräver anmälan av personuppgiftsincidenter till tillsynsmyndigheter inom 72 timmar, med uppgifter om omfattning och riskreducerande åtgärder.

11.5. EU:s NIS2-direktiv (2022/2555)

11.5.1. Artikel 23 – Kräver att väsentliga och viktiga entiteter anmäler betydande incidenter till behöriga myndigheter med standardiserade rapporteringsformat.

11.6. EU:s DORA-förordning (2022/2554)

11.6.1. Artikel 17 – Kräver att finansiella entiteter klassificerar, rapporterar och följer upp IKT-relaterade incidenter och störningar.

11.7. COBIT 2019

11.7.1. DSS02 – Hantera tjänstebegäranden och incidenter: Vägleder effektiv hantering av operativa incidenter och säkerhetsincidenter i linje med styrningsmålen.

11.7.2. DSS04 – Hantera kontinuitet: Kopplar incidenthantering till bredare strategier för kontinuitet och återställning.