					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: P30					Dokumenttitel: **Policy för incidenthantering (P30)**							
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**

Ansluten till standarder och regelverk

Standard/regelverk	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Klausul 8.1, klausul 9	Strukturerade processer för riskhantering och incidenthantering
ISO/IEC 27002:2022	Kontroller 5.25–5.27	Roller, rapportering, respons och förbättring avseende incidenter
NIST SP 800-53 Rev.5	IR-1 till IR-9	Omfattande livscykel för incidenthantering
EU:s GDPR	Artikel 33.1, 33.3 a–d, 34.1, 34.2 a–c	Tidsfrister för anmälan av personuppgiftsincidenter, rapportering och kommunikation med registrerade
EU:s NIS2-direktiv	Artikel 23.1–23.4	Anmälan till nationell myndighet och strukturerad rapportering
EU:s DORA-förordning	Artikel 17.1–17.3	Rapportering av större IKT-relaterade incidenter för finansiella entiteter
COBIT 2019	DSS02, DSS04, MEA	Definierar, övervakar och utvärderar incidenthantering, kontinuitet och uppföljning

1. Syfte

1.1 Denna policy fastställer en formell struktur för identifiering, rapportering, analys, begränsning, respons, återställning och efterincidentgranskning av informationssäkerhetsincidenter som påverkar organisationen.

1.2 Policyn säkerställer snabba, samordnade och effektiva insatser för att minimera operativa störningar, ekonomiska förluster, anseendeskada och bristande efterlevnad av regulatoriska krav.

1.3 Policyn stödjer även kontinuerlig förbättring av organisationens cyberresiliens genom erfarenhetsåterföring och integrering av resultat från efterincidentgranskningar i styrning, verktygsstöd och utbildningsprogram.

2. Omfattning

2.1 Denna policy gäller för:

2.1.1 all personal, inklusive anställda, konsulter och tredjepartsleverantörer

2.1.2 alla informationssystem, applikationer, infrastrukturer, nätverk och data, oavsett om de finns lokalt, i molnmiljö eller i hybrida miljöer

2.1.3 alla typer av säkerhetsincidenter, inklusive men inte begränsat till:

2.1.3.1 obehörig åtkomst eller eskalering av behörigheter

2.1.3.2 attacker med skadlig kod och ransomware

2.1.3.3 överbelastningsattacker (DoS/DDoS)

2.1.3.4 dataförlust, dataläckage eller dataexfiltration

2.1.3.5 insiderrelaterat missbruk eller policyöverträdelser

2.1.3.6 fysiska säkerhetsöverträdelser som påverkar digitala tillgångar

2.2 Policyn omfattar detektering, triagering, utredning, eskalering, begränsning, hantering av bevismaterial, anmälan, återställning och rotorsaksanalys (RCA).

3. Mål

3.1 Att etablera en repeterbar och skalbar incidenthanteringsförmåga som möjliggör snabb detektering, klassificering och riskreducering av säkerhetsincidenter.

3.2 Att minimera verksamhetspåverkan från säkerhetshändelser genom strukturerade rutiner för begränsning, eliminering och återställning av system.

3.3 Att säkerställa att incidentrapportering och incidenthantering är förenliga med rättsliga, regulatoriska och avtalsmässiga krav, särskilt avseende tidsfrister för incidentanmälan och hantering av bevismaterial.

3.4 Att stödja transparens och ansvarstagande genom korrekt loggning, dokumentation och uppföljning av mätetal för alla säkerhetsincidenter.

3.5 Att främja kontinuerlig förbättring genom efterincidentgranskningar, korrigerande åtgärder och utbildning av berörda intressenter.

4. Roller och ansvar

4.1 Informationssäkerhetschef (CISO)

4.1.1 ansvarar för ramverket för incidenthantering, säkerställer efterlevnad av policyn och utövar tillsyn över incidentsamordningen i hela organisationen.

4.1.2 fungerar som primär kontaktpunkt mot tillsynsmyndigheter, verkställande ledning och extern juridisk rådgivare vid allvarliga incidenter.

4.2 Incidenthanteringskoordinator

4.2.1 samordnar tvärfunktionella responsteam, hanterar arbetsflöden och följer upp status för begränsning och återställning.

4.2.2 initierar och leder efterincidentgranskningar samt säkerställer att korrigerande åtgärder loggas och genomförs.

[... 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 Denna policy ska granskas minst årligen och revideras vid behov för att beakta:

9.1.1 förändringar i hotlandskapet, incidenttyper eller angreppsvektorer

9.1.2 erfarenheter från större incidenter, nära-händelser eller regulatoriska iakttagelser

9.1.3 uppdateringar av tillämpliga lagar och regelverk, till exempel GDPR, DORA och NIS2

9.1.4 återkoppling från incidenthanteringsövningar och efterincidentgranskningar

9.2 Informationssäkerhetschefen (CISO) ansvarar för att initiera och samordna granskningsprocessen i samråd med:

9.2.1.1 juridisk rådgivare och dataskyddsombud (DPO)

9.2.1.2 SOC och IT-drift

9.2.1.3 team för verksamhetskontinuitet och riskhantering

9.2.1.4 högsta ledningen

9.3 Ändringar i policyn ska:

9.3.1 dokumenteras i en versionshanterad lagringsplats

9.3.2 kommuniceras till alla berörda team och införas i utbildning för säkerhetsmedvetenhet

9.3.3 valideras genom skrivbordsövningar eller praktiska incidenthanteringsövningar inom tre månader från godkännande

9.4 Brådskande uppdateringar som utlöses av framväxande hot, revisionsiakttagelser eller nya rättsliga skyldigheter ska genomföras omedelbart och antecknas i policyändringshistoriken.

10. Relaterade policyer och kopplingar

10.1 Denna policy stöds av och är beroende av följande organisatoriska policyer:

10.1.1 P1 – Informationssäkerhetspolicy: Fastställer övergripande krav på riskbaserad verksamhet med beredskap för incidenthantering.

10.1.2 P5 – Ändringshanteringspolicy: Säkerställer att begränsnings- och återställningsaktiviteter som berör infrastruktur eller tjänster följer formella rutiner.

10.1.3 P13 – Policy för dataklassificering och märkning: Stödjer klassificering av incidenters allvarlighetsgrad utifrån datats känslighet.

10.1.4 P15 – Policy för säkerhetskopiering och återställning: Möjliggör återställning efter ransomware eller destruktiva angrepp med säkerställd riktighet.

10.1.5 P18 – Policy för kryptografiska kontroller: Definierar krypteringsåtgärder som minskar incidentpåverkan och risker för dataexponering.

10.1.6 P22 – Loggnings- och övervakningspolicy: Ger den grundläggande synlighet i händelser, larm och logglagring som krävs för effektiv detektering och forensik.

10.1.7 P29 – Policy för testdata och testmiljöer: Säkerställer att incidenter som påverkar icke-produktionsmiljöer också hanteras på ett strukturerat och säkert sätt.

10.1.8 P33 – Policy för revisions- och efterlevnadsövervakning: Validerar incidentberedskap och incidenthanteringens effektivitet genom strukturerade revisioner och efterlevnadsbedömningar.

11. Referensstandarder och ramverk

11.1 ISO/IEC 27001: Klausul 8.1 – Operativ planering och styrning: Strukturerade processer för att hantera risker och planering för incidenthantering.

11.2 ISO/IEC 27002:2022 – Kontroller 5.25–5.27: Ansvar för incidenthantering, rapportering, respons, kommunikation och förbättring.

11.3 NIST SP 800-53 Rev.5: IR-1 till IR-9, AU-6, PL-2: Omfattande krav för incidenthanteringens livscykel, revision och säkerhetsplanering.

11.4 GDPR: Artikel 33/34: Rapporteringsskyldigheter till tillsynsmyndigheter samt krav på information till registrerade, med definierade undantag.

11.5 NIS2-direktivet (2022/2555): Artikel 23: Obligatorisk nationell rapportering, med krav på mellanliggande och slutlig rapportering.

11.6 DORA-förordningen (2022/2554): Artikel 17: Krav på rapportering av IKT-incidenter till myndigheter för finansiella institutioner.

11.7 COBIT 2019: DSS02, DSS04, MEA01: Hantering av tjänsteincidenter och kontinuitet samt övervakning av prestanda och efterlevnad.