					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: P31					Dokumenttitel: **Policy för bevisinhämtning och forensik**							
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	
ISO/IEC 27002:2022	Kontroller 5.25–5.27, 8	
ISO/IEC 27035:2016	Del 1 och 3	
NIST SP 800-53 Rev.5	IR-1 till IR-9, AU-6, PL-2	
NIST SP 800-101 Rev.1	Mobilforensik och medieforensik	Mobilforensik och medieforensik
NIST SP 800-86	Integrering av forensiska tekniker	Integrering av forensiska tekniker i incidenthantering
EU:s dataskyddsförordning (GDPR)	Artikel 5, 33–34	
EU:s NIS2-direktiv	Artikel 23(1)–(4)	
EU:s DORA-förordning	Artikel 17(1)–(3)	
COBIT 2019	DSS01.07, DSS05	

1. Syfte

1.1 Denna policy fastställer ett strukturerat och rättsligt hållbart ramverk för identifiering, inhämtning, bevarande, analys och avveckling av digital bevisning vid faktiska eller misstänkta säkerhetsincidenter.

1.2 Den säkerställer att processer för forensisk beredskap och bevishantering:

1.2.1 upprätthåller bevisintegritet och dokumentation av beviskedjan

1.2.2 stödjer interna utredningar, rättsprocesser eller regulatorisk rapportering

1.2.3 är anpassade till internationellt erkända forensiska standarder och krav på rättslig admissibilitet

1.3 Policyn stödjer organisationens åtagande om proaktiv incidenthantering, efterlevnad av rättsliga krav och transparens i styrningen, samtidigt som operativa störningar minimeras.

2. Omfattning

2.1 Denna policy gäller för:

2.1.1 alla anställda, uppdragstagare, leverantörer och tjänsteleverantörer som deltar i systemadministration, incidenthantering eller utredningsaktiviteter

2.1.2 alla klienter, servrar, applikationer, nätverk och molnplattformar under organisationens kontroll eller avtalsmässiga ansvar

2.1.3 varje incident eller händelse som kräver bevishantering, inklusive:

2.1.3.1 insiderhot, personuppgiftsincidenter eller bedrägeriutredningar

2.1.3.2 missbruk av system eller autentiseringsuppgifter

2.1.3.3 incidenter i OT-system eller industriella styrmiljöer

2.1.3.4 överträdelser av fysiskt tillträde som involverar digitala tillgångar

2.2 Policyn reglerar även all interaktion med externa forensiska tjänsteleverantörer eller brottsbekämpande myndigheter vid rättslig eller regulatorisk eskalering eller regulatoriska förfaranden.

3. Mål

3.1 Att möjliggöra snabb, säker och policyenlig inhämtning av bevisning vid säkerhetshändelser eller utredningar.

3.2 Att bevara riktighet, autenticitet och admissibilitet för inhämtad digital bevisning genom strikt styrning av åtkomst, loggning och verifieringsrutiner.

3.3 Att säkerställa att alla forensiska aktiviteter samordnas med rättsliga och regulatoriska skyldigheter, inklusive dataskydd, arbetsrätt och begränsningar av internationella överföringar.

3.4 Att stödja efteranalys av incidenter, fastställande av grundorsak och förbättring av kontroller genom forensiskt underlag av hög kvalitet.

3.5 Att integrera forensisk beredskap i det övergripande ledningssystemet för informationssäkerhet (LIS) för att stödja revisioner, incidentanmälningar och beslut i högsta ledningen.

4. Roller och ansvar

4.1 Informationssäkerhetschef (CISO)

4.1.1 ansvarar för denna policy och säkerställer att all forensisk verksamhet är rättsligt hållbar, granskningsbar och riskbaserad.

4.1.2 godkänner eskalering till externa juridiska aktörer och forensiska tjänsteleverantörer.

4.2 Forensiska analytiker / incidenthanterare

4.2.1 leder inhämtning, bevarande och teknisk analys av bevisning.

4.2.2 säkerställer att beviskedjan dokumenteras och upprätthålls korrekt.

4.2.3 dokumenterar alla åtgärder, iakttagelser och verktygsinställningar som används under utredningar.

[... 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 uppdateras vid behov för att återspegla:

9.1.1 förändringar i lagar, regelverk eller praxis som påverkar forensiska rutiner eller datahantering

9.1.2 uppdateringar av branschstandarder för forensik eller verktyg

9.1.3 lärdomar från efterincidentgranskningar, rättstvister eller revisionsiakttagelser

9.1.4 tekniska förändringar i plattformar, enheter eller system som omfattas av utredning

9.2 Granskningsprocessen ägs av informationssäkerhetschef (CISO) och ska omfatta samråd med:

9.2.1 juridik och regelefterlevnad

9.2.2 dataskyddsombud (DPO)

9.2.3 säkerhetsverksamheten och forensiska team

9.2.4 internrevision

9.3 Alla revideringar ska:

9.3.1 versionshanteras och lagras i policyarkivet

9.3.2 kommuniceras till berörda intressenter, inklusive forensiska team och incidenthanteringsteam

9.3.3 åtföljas av uppdateringar av relevanta operativa rutiner och utbildningsmaterial

9.4 En extra granskning ska initieras efter varje kritisk incident som innefattar felaktig hantering av bevisning, avbrott i beviskedjan eller problem med rättslig admissibilitet.

10. Relaterade policyer och kopplingar

10.1 Denna policy är anpassad till och stöds av följande organisatoriska policyer:

10.1.1 P1 – Informationssäkerhetspolicy: Fastställer grundläggande krav för utredning, bevishantering och efterlevnad av tillämpliga lagkrav.

10.1.2 P5 – Policy för ändringshantering: Säkerställer att system som är föremål för utredning inte ändras under pågående forensiska processer.

10.1.3 P14 – Policy för databevarande och bortskaffning: Reglerar säker avveckling och bevarandetider för bevisning och ärenderelaterade data.

10.1.4 P18 – Policy för kryptografiska kontroller: Anger krav på kryptering för lagring och överföring av känsliga data eller bevisdata.

10.1.5 P22 – Loggnings- och övervakningspolicy: Säkerställer tillgång till händelseloggar och telemetri för bevisinhämtning och forensisk korrelation.

10.1.6 P30 – Policy för incidenthantering: Definierar incidenttriagering och eskaleringsvägar där forensiska rutiner initieras.

10.1.7 P33 – Policy för revisions- och efterlevnadsövervakning: Verifierar efterlevnad av forensiska protokoll och krav på beviskedja genom regelbundna revisioner.

11. Referensstandarder och ramverk

11.1 Denna policy är anpassad till internationella standarder för forensik och incidenthantering för att säkerställa bevisintegritet, rättslig hållbarhet och efterlevnad i olika jurisdiktioner.

11.2 ISO/IEC 27001

11.2.1 Klausul 8.1 – Stödjer operativ styrning av forensisk beredskap och rutiner för bevishantering

11.3 ISO/IEC 27002

11.3.1 Bilaga A, kontroll 5.25 – Ansvar för incidenthantering: Kräver definierade roller för hantering av informationssäkerhetsincidenter och utredningar.

11.3.2 Bilaga A, kontroll 5.26 – Rapportering av informationssäkerhetshändelser: Stödjer insamling av händelserelaterade artefakter som bevisning.

11.3.3 Bilaga A, kontroll 5.27 – Hantering av informationssäkerhetsincidenter: Kräver strukturerad, bevisdriven åtgärdshantering och utredning.

11.3.4 Bilaga A, kontroll 8.27 – Säker utveckling och forensik (där tillämpligt): Behandlar skydd av system och verktyg under utredningar.

11.4 ISO/IEC 27035:2016 (del 1 och 3)

11.4.1 Beskriver principerna för incidentdetektering, respons och forensisk beredskap, inklusive planering, beviskedja och hantering av incidentrelaterad bevisning.

11.5 NIST SP 800-53 Rev.5

11.5.1 IR-1 till IR-9, AU-6, PL-2: Definierar strukturerade krav för planering, detektering, analys, begränsning och hantering av säkerhetsincidenter. Stödjer insamling och granskningsbarhet av bevisning (AU-6) och säkerställer anpassning till planer för systemsäkerhet och integritet (PL-2) vid forensiska utredningar.

11.6 NIST SP 800-86

11.6.1 Ger vägledning om hur forensiska processer integreras i den bredare livscykeln för incidenthantering och hur forensisk beredskap säkerställs.

11.7 NIST SP 800-101 Rev.1

11.7.1 Fokuserar på bästa praxis för att inhämta, bevara och analysera digitala medier och bevisning från mobila enheter på ett rättsligt hållbart sätt.

11.8 EU:s dataskyddsförordning (2016/679)

11.8.1 Artikel 5 – Principer för behandling av personuppgifter: Gäller för bevisning som innehåller personuppgifter eller känsliga uppgifter och säkerställer uppgiftsminimering och ändamålsbegränsning.

11.8.2 Artiklarna 33–34 – Anmälan av personuppgiftsincidenter: Forensiska data stödjer efterlevnad av skyldigheter att anmäla incidenter och rättsliga utlämningsprocesser.

11.9 EU:s NIS2-direktiv (2022/2555)

11.9.1 Artikel 23 – Rapporteringsskyldigheter: Forensisk dokumentation och iakttagelser stödjer snabb och korrekt incidentrapportering till behöriga myndigheter.

11.10 EU:s DORA-förordning (2022/2554)

11.10.1 Artikel 17 – Rapportering av IKT-incidenter: Kräver detaljerad grundorsaksanalys och bevisunderlag för större IKT-relaterade incidenter, särskilt inom finanssektorn.

11.11 COBIT 2019

11.11.1 DSS01.07 – Hantera säkerhetsincidenter: Kräver incidentdokumentation och noggrannhet i utredningar.

11.11.2 DSS05.04 – Hantera säkerhetsutredningar: Betonar bevarande av digital bevisning och stöd för disciplinära och rättsliga åtgärder.