					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: P31S					Dokumenttitel: **Policy för bevisinsamling 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**

Anpassning till standarder och regelverk

Standard/regelverk	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Klausuler 6.1, 6.3, 8	Riskbaserad planering, förbättringsåtgärder och operativa kontroller för bevismaterialets integritet
ISO/IEC 27002:2022	Kontroller 5.24–5.27	Vägledning för säker hantering, efterincidentgranskningar och förbättringar baserade på bevismaterial
ISO/IEC 27035-3:2016	Klausuler 6.3, 6.4, 7	Säkerställer korrekt planering, rättsenlig insamling och säker hantering av digital bevisning med dokumenterad beviskedja
NIST SP 800-53 Rev.5	IR-07, IR-08, AU-09, AU-12, PE-18	Forensisk beredskap, skydd av revisionsloggar och effektiv integrering i incidenthanteringen
EU:s GDPR	Artiklarna 33, 34	Dokumentation och spårbarhet för personuppgiftsincidenter
EU:s NIS2-direktiv	Artikel 23	Spårbar incidentrapportering och säker hantering av bevismaterial
EU:s DORA-förordning	Artikel 17(1), 17(2)	Säkerställer insamling, lagring och bevarande av bevismaterial för IKT-relaterade incidenter, forensisk kvalitet och regulatoriska förfrågningar
COBIT 2019	DSS05.06, DSS05.07	Tillförlitlig loggning och strukturerad hantering av bevismaterial för säkra och verifierbara utredningar

1. Syfte

1.1. Denna policy definierar hur organisationen hanterar digital bevisning relaterad till säkerhetsincidenter, personuppgiftsincidenter och interna utredningar. Den säkerställer att bevismaterial samlas in, lagras och bevaras på ett rättsenligt sätt och med revisionsberedskap, som stöd för både interna beslut och eventuella externa åtgärder.

1.2. Policyn gör det möjligt för mindre organisationer att skydda integriteten hos loggar, filer och systemavbildningar samtidigt som den visar tillbörlig aktsamhet enligt ISO/IEC 27001, EU:s GDPR och relaterade standarder.

1.3. Policyn stöder forensisk beredskap utan krav på avancerade tekniska resurser eller ett heltidsbemannat IT-team genom att fastställa tydliga ansvar, processer och krav för bevarande.

2. Omfattning

2.1. Denna policy gäller för:

2.1.1. alla anställda, IT-leverantörer och externa konsulter som medverkar i incidenthantering, utredning eller analys av överträdelser

2.1.2. alla företagets system, inklusive bärbara datorer, mobila enheter, servrar, e-postkonton, SaaS-plattformar och molnlagring (t.ex. Microsoft 365, Google Workspace)

2.1.3. alla händelser som kräver bevismaterial för interna disciplinära åtgärder, rättsligt försvar, försäkringsärenden eller kontakt med tillsynsmyndighet

2.2. Detta omfattar både bekräftade och misstänkta händelser som rör:

2.2.1. dataläckage

2.2.2. insiderhot eller missbruk

2.2.3. säkerhetsincidenter (t.ex. skadlig kod, obehörig åtkomst)

2.2.4. kundklagomål som kräver digital verifiering

2.2.5. förfrågningar från tillsynsmyndigheter eller brottsbekämpande myndigheter

3. Mål

3.1. Säkerställa att allt bevismaterial samlas in och hanteras på ett sätt som upprätthåller dess integritet, autenticitet och beviskedja.

3.2. Förhindra oavsiktlig ändring, radering eller felaktig hantering av loggar, filer eller systemavbildningar som kan behövas för utredningar.

3.3. Tillhandahålla ett enhetligt och verifierbart arbetssätt för hantering av bevismaterial som uppfyller rättsliga och regulatoriska förväntningar (t.ex. anmälan av personuppgiftsincidenter enligt EU:s GDPR och spårbarhet enligt EU:s NIS2-direktiv).

3.4. Fastställa tydliga roller och ansvar för att säkerställa snabb, säker och rättsenlig insamling av bevismaterial vid säkerhetsincidenter.

3.5. Stödja forensisk beredskap anpassad för SME samtidigt som komplexitet minimeras och störningar i den dagliga verksamheten undviks.

4. Roller och ansvar

4.1. verkställande direktör (GM)

4.1.1. Godkänner alla formella utredningar som kräver bevisinsamling.

4.1.2. Granskar och godkänner incidentrapporter som omfattar potentiella rättsliga eller disciplinära åtgärder.

4.1.3. Beslutar om extern juridisk rådgivare eller tillsynsmyndighet ska underrättas.

4.1.4. Säkerställer att policyn granskas och uppdateras regelbundet.

4.2. IT-leverantör/systemadministratör

4.2.1. Samlar in och bevarar digital bevisning enligt säkra rutiner.

4.2.2. Dokumenterar tidsstämplar, systemdetaljer och hanteringssteg.

4.2.3. Säkrar allt insamlat material på en skyddad lagringsplats.

4.2.4. Stöder forensisk analys vid behov.

[... 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. Årlig policygranskning

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

9.1.1.1. efterlevnad av kontroller i bilaga A till ISO/IEC 27001

9.1.1.2. fortsatt relevans för aktuella digitala plattformar och IT-tjänster

9.1.1.3. tillräcklighet i rutiner för loggning, bevarande av bevismaterial och forensisk beredskap

9.2. Utlösande händelser för policyrevidering

9.2.1. Policyn ska också granskas och uppdateras efter:

9.2.1.1. varje större incident som kräver bevisinsamling

9.2.1.2. en underkänd revision eller en regulatorisk begäran där bevismaterialets integritet har ifrågasatts

9.2.1.3. införande av nya verktyg eller rutiner för incidenthantering eller systemövervakning

9.2.1.4. rättsliga ändringar (t.ex. uppdaterad vägledning för EU:s GDPR eller EU:s NIS2-direktiv)

9.3. Godkännande av ändringar och distribution

9.3.1. Alla ändringar ska granskas och godkännas av GM.

9.3.2. Den uppdaterade versionen ska delas med:

9.3.2.1. IT-leverantörer och konsulter som medverkar i utredningar

9.3.2.2. personal med ansvar för systemadministration

9.3.3. En uppdaterad kopia ska bevaras i företagets policyarkiv och delas med revisorer på begäran.

10. Relaterade policyer och kopplingar

10.1. Denna policy är beroende av följande policyer anpassade för SME:

10.1.1. P2S – Policy för styrningsroller och ansvar: Fastställer mandat för incidentutredningar, beslut om bevismaterial och juridisk eskalering.

10.1.2. P4S – Policy för åtkomstkontroll: Säkerställer att endast behörig personal får åtkomst till känsliga system och loggar under utredningar.

10.1.3. P22S – Policy för loggning och övervakning: Tillhandahåller de rådata som används som forensiskt bevismaterial och fastställer krav på bevarande, åtkomstkontroll och loggning.

10.1.4. P30S – Policy för incidenthantering: Utlöser behovet av bevisinsamling och definierar det operativa flödet som leder till forensiskt bevarande.

10.1.5. P17S – Policy för dataskydd och integritet: Säkerställer att personuppgifter som samlas in som bevismaterial hanteras lagenligt enligt EU:s GDPR och relaterade regelverk.

10.2. Dessa policyer samverkar för att stödja rättslig hållbarhet, utredningars integritet och full revisionsberedskap enligt ISO/IEC 27001:2022.

11. Referensstandarder och ramverk

11.1. ISO/IEC 27001

11.1.1. Klausul 6.1 – Riskbaserad planering omfattar beredskap för respons och rutiner för bevismaterial.

11.1.2. Klausul 6.3 – Stödjer förbättringsåtgärder baserade på bevismaterial från incidenter.

11.1.3. Klausul 8.1 – Kräver operativa kontroller för bevismaterialets integritet.

11.2. ISO/IEC 27002

11.2.1. Kontroller 5.24–5.27 – Vägledning för säker hantering, efterincidentgranskningar och förbättringar baserade på bevismaterial.

11.3. ISO/IEC 27035-3

11.3.1. Klausulerna 6.3, 6.4 och 7.3 säkerställer korrekt planering, rättsenlig insamling och säker hantering av digital bevisning under incidenthantering, inklusive bevarande och dokumentation av beviskedjan.

11.4. NIST SP 800-53 Rev. 5

11.4.1. IR-07, IR-08, AU-09 och AU-12 säkerställer forensisk beredskap, skydd av revisionsloggar och effektiv integrering av bevisinsamling i incidenthanteringens livscykel.

11.5. NIST SP 800-86

11.5.1. Definierar bästa praxis för inhämtning, analys och skydd av digital bevisning under incidenthantering.

11.6. EU:s GDPR

11.6.1. Artiklarna 33–34 – Kräver dokumentation och spårbarhet för incidenter och bevismaterial vid rapportering av personuppgiftsincidenter.

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

11.7.1. Artikel 23 – Kräver spårbar incidentrapportering och säker hantering av bevismaterial för väsentliga och viktiga entiteter.

11.8. EU:s DORA-förordning

11.8.1. Artikel 17(1) – Säkerställer att bevismaterial relaterat till IKT-relaterade incidenter samlas in och lagras på ett sätt som stöder forensiska utredningar.

11.8.2. Artikel 17(2) – Kräver att finansiella entiteter bevarar alla relevanta data och loggar kopplade till säkerhetshändelser, i linje med forensisk kvalitet och regulatoriska förfrågningar.

11.9. COBIT 2019

11.9.1. DSS05.06 – Övervaka, upptäcka och rapportera incidenter: Betonar tillförlitlig loggning som stöd för utredningar.

11.9.2. DSS05.07 – Utreda och agera vid incidenter: Kräver strukturerad hantering av bevismaterial för att möjliggöra säkra och verifierbara utredningar.