					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: P22					Dokumenttitel: **Policy för loggning och övervakning**							
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**

1. Syfte

1.1 Syftet med denna policy är att fastställa tydliga och bindande krav för generering, skydd, granskning och analys av loggar som registrerar centrala system- och säkerhetshändelser i hela organisationens IT-miljö.

1.2 Loggning och övervakning är avgörande för avvikelsedetektering, hotidentifiering, forensisk analys, revisionsberedskap och efterlevnad av rättsliga krav. Denna policy säkerställer att alla systemgenererade händelser registreras korrekt, bevaras och korreleras med tidssynkroniserad precision.

1.3 Denna policy är väsentlig för att stödja ISO/IEC 27001 klausul 8.1 och bilaga A-kontrollerna 8.15 (loggning), 8.16 (övervakning) och 8.17 (klocksynkronisering), och är direkt kopplad till regulatoriska skyldigheter enligt GDPR, NIS2, DORA och COBIT 2019.

2. Omfattning

2.1 Denna policy gäller för alla system, tjänster och miljöer som lagrar, behandlar eller överför data som omfattas av ledningssystemet för informationssäkerhet (ISMS), inklusive:

2.1.1 lokal IT-infrastruktur, molntjänster (t.ex. IaaS, PaaS, SaaS) och hybridmiljöer

2.1.2 operativsystem, databaser, applikationer och nätverksutrustning

2.1.3 säkerhetssystem såsom SIEM, brandväggar, endpointskyddsplattformar, VPN-koncentratorer och identitetsleverantörer

2.2 Följande intressenter omfattas:

2.2.1 interna användare med systembehörigheter eller administrativa privilegier

2.2.2 personal inom IT-infrastruktur och IT-drift

2.2.3 säkerhetsoperationscenter (SOC) och team för hotdetektering

2.2.4 programvaruutvecklare och applikationsägare

2.2.5 tredjepartsleverantörer som förvaltar system som genererar loggar

3. Mål

3.1 Säkerställa att alla kritiska system genererar loggar över säkerhetshändelser och systemaktiviteter som bevaras i enlighet med regulatoriska, rättsliga och avtalsmässiga krav.

3.2 Fastställa vilka minsta händelsetyper och vilket minsta loginnehåll som krävs för att upptäcka obehöriga aktiviteter, spåra användaråtgärder och stödja forensiska utredningar.

3.3 Säkerställa skydd som förhindrar manipulation av loggar, obehörig radering eller okontrollerad åtkomst till loggdata.

3.4 Etablera centraliserade system för loggning och larmhantering (t.ex. SIEM) för att aggregera, korrelera och eskalera misstänkt aktivitet i nära realtid.

3.5 Säkerställa synkronisering av systemklockor för att möjliggöra korrekt korrelation mellan system och analys av incidenter.

3.6 Möjliggöra kontinuerlig förbättring och efterlevnad genom att integrera loggövervakning med processer för revision, riskhantering och incidenthantering.

4. Roller och ansvar

4.1 Informationssäkerhetschef (CISO)

4.1.1 Äger denna policy och säkerställer att den är anpassad till organisationens riskbild, revisionskrav och skyldigheter inom ISMS.

4.1.2 Godkänner loggningsomfattningen för reglerade system eller högrisksystem och utövar tillsyn över rapportering av regelefterlevnad.

4.2 Chef för säkerhetsoperationscenter (SOC)

4.2.1 Ansvarar för drift och underhåll av centraliserade plattformar för logghantering (t.ex. SIEM).

4.2.2 Fastställer regler för loggaggregering, larmtrösklar och eskaleringsvägar för incidenttriagering.

4.2.3 Granskar dagliga rapporter och säkerställer att avvikelser analyseras, dokumenteras och eskaleras 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 Denna policy ska granskas årligen, eller tidigare till följd av:

9.1.1 större förändringar i systemarkitektur eller loggningsinfrastruktur (t.ex. migrering av SIEM)

9.1.2 ändringar i regulatoriska loggningskrav (t.ex. loggningskrav enligt NIS2 och DORA)

9.1.3 iakttagelser från revisioner eller granskningar efter incident

9.1.4 framväxande hot som kräver förstärkt övervakning (t.ex. insiderhot eller kompromettering i leverantörskedjan)

9.2 Granskningsprocessen ska ledas av chefen för säkerhetsoperationscenter (SOC) i samordning med CISO, riskhantering, regelefterlevnad och teamen för IT-infrastruktur.

9.3 Godkända ändringar ska versionshanteras i ISMS-registret för dokumentstyrning och kommuniceras till:

9.3.1 alla intressenter med ansvar för underhåll av loggningssystem

9.3.2 applikations- och systemägare

9.3.3 tredjepartsleverantörer med ansvar för telemetri eller SIEM-integration

9.4 Alla ersatta versioner ska arkiveras säkert, med åtkomst begränsad till behöriga ISMS-förvaltare för revisions- och rättsliga ändamål.

10. Relaterade policyer och kopplingar

10.1 P1 – Informationssäkerhetspolicy. Fastställer det grundläggande åtagandet att skydda system och data, där loggning och övervakning utgör centrala detekterande kontroller och stöd för incidenthantering.

10.2 P4 – Policy för åtkomstkontroll. Säkerställer att privilegierad åtkomst, användarinloggningar och auktoriseringshändelser registreras i loggar och övervakas avseende missbruk eller avvikande beteende.

10.3 P5 – Policy för ändringshantering. Kräver loggning av systemändringar, driftsättning av patchar och konfigurationsuppdateringar som kan medföra risk eller obehöriga ändringar.

10.4 P21 – Nätverkssäkerhetspolicy. Kräver loggning på nätverksnivå (t.ex. brandväggsloggar, IDS/IPS-larm, VPN-aktivitet) och integration med SIEM för insyn i trafikavvikelser och skydd av nätverksgränser.

10.5 P23 – Policy för tidssynkronisering. Säkerställer enhetlig tid mellan system, vilket är nödvändigt för tillförlitlig loggning och korrelation av säkerhetshändelser i flera miljöer.

10.6 P30 – Incidenthanteringspolicy. Bygger på loggdata och larmmekanismer för att identifiera, utreda och hantera säkerhetsincidenter samt för att bevara forensiska artefakter för efterhandsgranskning.

11. Referensstandarder och ramverk

11.1 ISO/IEC 27001

11.1.1 Klausul 8.1 – Operativ planering och styrning: Kräver kontroller för övervakning av verksamheten och skydd mot obehörig åtkomst och otillbörlig användning av system.

11.2 ISO/IEC 27002:2022 – Kontroller 8.15, 8.16, 8.17

11.2.1 Definierar detaljerade krav för loggning, inklusive vilka händelser som ska registreras, hur loggar ska skyddas och analyseras samt hur tillförlitliga tidsstämplar säkerställs mellan system.

11.3 NIST SP 800-53 Rev. 5

11.3.1 AU-2 till AU-12: Omfattar urval av händelser, loggning, skydd, granskning av revisionsspår, hantering av fel i revisionsfunktioner och bevarande av revisionsunderlag.

11.3.2 SI-4 – Systemövervakning: Kräver aktiv systemövervakning med larm baserade på avvikande aktivitet.

11.3.3 SC-45 – Synkronisering av systemtid: Förstärker kraven på tidsnoggrannhet för spårbarhet av händelser och korrelation av incidenter.

11.4 EU:s GDPR (2016/679)

11.4.1 Artikel 32 – Säkerhet i behandlingen: Kräver tekniska kontroller såsom loggning och övervakning för att säkerställa säkerhet och ansvarsskyldighet, särskilt vid åtkomst till personuppgifter.

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

11.5.1 Artikel 21.2 e: Kräver loggning av händelser och övervakningssystem för snabb upptäckt av och respons på säkerhetsincidenter.

11.6 EU:s DORA-förordning (2022/2554)

11.6.1 Artikel 9 – IKT-riskhantering: Kräver mekanismer för att upptäcka avvikande aktivitet, logga incidenter och bevara forensiska data.

11.6.2 Artikel 11 – Testning av planer för verksamhetskontinuitet för IKT: Betonar kontinuitet i övervakning och validering av tillgänglighet till loggar under operativa störningar.

11.7 COBIT 2019

11.7.1 DSS01.05 – Hantera säkerhetsloggar: Kräver införande av loggningsförmåga för all kritisk infrastruktur.

11.7.2 DSS05.04 – Övervaka säkerhetshändelser: Kräver övervakning och analys av loggar i realtid för att upptäcka och hantera händelser.

11.7.3 MEA03 – Övervaka, utvärdera och bedöma efterlevnad: Kräver regelbunden granskning av loggningspraxis och anpassning till kontrollmål.