					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: P22S					Dokumenttitel: **Loggnings- och övervakningspolicy**							
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	Klausul 8	Operativa kontroller, inklusive loggning
ISO/IEC 27002:2022	Kontroller 8.15, 8.16, 8.17	Händelseloggning, skydd av loggar och övervakning
NIST SP 800-53 Rev.5	AU-2 till AU-12, SI-4	Innehåll i revisionsloggar, granskning, logglagring, avvikelsedetektering och avisering
EU:s dataskyddsförordning (GDPR)	Artiklarna 5.1 f, 32, 33	Konfidentialitet och riktighet för uppgifter, tekniska åtgärder samt anmälan av personuppgiftsincidenter
EU:s NIS2-direktiv	Artiklarna 21.2 d, 23	Loggningsmekanismer för avvikelser och incidentrapportering inom 24 timmar
DORA-förordningen	Artiklarna 10, 15	Operativ resiliens samt övervakning och loggning av tjänsteleverantörer
COBIT 2019	DSS01.03, DSS05.02	Spårbarhet av aktiviteter samt skydd genom loggning och övervakning

1. Syfte

1.1 Denna policy fastställer obligatoriska kontroller för loggning och övervakning för att säkerställa säkerhet, ansvarsskyldighet och operativ riktighet i organisationens IT-system.

1.2 Den anger vilka typer av händelser som ska loggas, hur loggar ska lagras, hur de ska granskas samt ansvar för personal och tjänsteleverantörer.

1.3 Loggning och övervakning stödjer hotdetektering, regelefterlevnad, incidenthantering och forensisk analys.

1.4 Denna policy gör det möjligt för organisationen att uppfylla kraven på operativa kontroller enligt ISO/IEC 27001 och stödjer löpande revisionsberedskap, kundförtroende samt efterlevnad av EU:s dataskyddsförordning (GDPR), EU:s NIS2-direktiv och DORA-förordningen.

2. Omfattning

2.1 Denna policy gäller för alla system och användare inom organisationen, inklusive:

2.1.1 Arbetsstationer, bärbara datorer, servrar, brandväggar, switchar, routrar och trådlösa åtkomstpunkter

2.1.2 Molntjänster som används i verksamheten, till exempel e-post, fillagring, säkerhetskopiering och samarbetsverktyg

2.1.3 Loggningsfunktioner i antivirusprogram, applikationer, operativsystem och nätverksutrustning

2.1.4 Alla anställda, entreprenörer och tredjepartstjänsteleverantörer samt leverantörer av hanterade tjänster (MSP:er) som använder eller administrerar system

2.1.5 Alla platser där organisationens IT-system används, inklusive distansarbetsmiljöer, hybridmiljöer och Bring Your Own Device (BYOD)-miljöer

2.2 Policyn gäller även för loggar som genereras av tredjepartstjänster där organisationen har administrativ åtkomst eller revisionsrätt enligt avtal.

3. Mål

3.1 Säkerställa loggning av systemaktivitet, inklusive autentisering, konfigurationsändringar, åtkomst till känsliga uppgifter och säkerhetslarm

3.2 Upprätthålla säkra och korrekta loggar för att upptäcka policyöverträdelser, systemfel eller obehöriga åtgärder

3.3 Möjliggöra snabb granskning av loggar vid incidenter, utredningar och revisioner

3.4 Stödja tidssynkronisering för att säkerställa riktighet och korrelation av loggdata

3.5 Skydda loggar mot manipulation, förlust eller förtida radering

3.6 Uppfylla rättsliga och regulatoriska skyldigheter avseende ansvarsskyldighet i system, spårbarhet och hantering av överträdelser

4. Roller och ansvar

4.1 Verkställande direktör (GM)

4.1.1 Godkänner denna policy och säkerställer att den genomförs i samtliga verksamhetssystem

4.1.2 Granskar larm med hög allvarlighetsgrad och väsentliga revisionsiakttagelser som rapporteras av IT eller dataskyddsfunktionen

4.1.3 Godkänner undantag där loggning eller bevarande inte kan genomföras av tekniska skäl

4.2 IT-supportleverantör / intern IT-funktion

4.2.1 Implementerar och konfigurerar loggning för operativsystem, nätverksenheter, antivirusverktyg och centrala applikationer

4.2.2 Säkerställer att loggar bevaras, säkerhetskopieras och skyddas mot ändring

4.2.3 Granskar loggar enligt fastställd tidsplan och utreder misstänkt eller obehörig aktivitet

4.2.4 Upprätthåller aviseringsmekanismer som flaggar avvikande beteende eller indikatorer på intrång

[... 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 granskning

9.1.1 Denna policy ska granskas minst en gång per år av verkställande direktör med stöd av IT-supportleverantören och Integritetssamordnaren.

9.2 Utlösande faktorer för granskning

9.2.1 Granskningar utanför ordinarie plan ska genomföras som svar på:

9.2.1.1 Iakttagelser kopplade till loggning från interna eller externa revisioner

9.2.1.2 Säkerhetsincidenter där loggar saknades, var korrupta eller otillräckliga

9.2.1.3 Väsentliga förändringar i IT-infrastrukturen, till exempel migrering till molnbaserade loggningsplattformar

9.2.1.4 Uppdateringar av rättsliga eller regulatoriska skyldigheter, till exempel EU:s dataskyddsförordning (GDPR), EU:s NIS2-direktiv eller DORA-förordningen

9.3 Versionshantering

9.3.1 Alla ändringar i denna policy ska loggas med versionsnummer, datum och sammanfattning av revideringar

9.3.2 Tidigare versioner ska arkiveras och bevaras i minst 3 år

9.3.3 Uppdaterade policyer ska kommuniceras till berörda intressenter, särskilt dem med konton på systemnivå

10. Relaterade policyer och kopplingar

10.1 Denna policy stödjer direkt och stöds av följande SME-policyer inom informationssäkerhet:

10.1.1 P17S – Policy för dataskydd och integritet: Säkerställer att loggdata som innehåller personuppgifter hanteras med riktighet, bevarande och åtkomstskydd i enlighet med kraven i EU:s dataskyddsförordning (GDPR).

10.1.2 P21S – Nätverkssäkerhetspolicy: Ger grunden för att samla in loggar relaterade till brandväggar, trådlös åtkomst, VPN och övervakning av segmentering.

10.1.3 P24S – Policy för säker utveckling: Säkerställer att applikationsloggar, till exempel för inloggningsförsök, fel och undantag, byggs in i programvarans design och drift.

10.1.4 P30S – Policy för incidenthantering: Är beroende av korrekt och fullständig loggdata för att upptäcka, analysera och hantera informationssäkerhetshändelser.

10.1.5 P23S – Policy för tidssynkronisering: Säkerställer konsekventa och spårbara tidsstämplar i alla system så att loggar kan korreleras vid utredningar.

11. Referensstandarder och ramverk

11.1 ISO/IEC 27001

11.1.1 Klausul 8.1 – Kräver genomförande av operativa kontroller för att minska informationssäkerhetsrisker, inklusive loggning.

11.2 ISO/IEC 27002

11.2.1 Kontroll 8.15 – Kräver händelseloggning för att stödja avvikelsedetektering och ansvarsskyldighet.

11.2.2 Kontroll 8.16 – Kräver skydd av loggar mot manipulation och obehörig åtkomst.

11.2.3 Kontroll 8.17 – Kräver övervakning av system avseende ovanlig aktivitet samt verifiering av övervakningskontrollers effektivitet.

11.3 NIST SP 800-53 Rev.5

11.3.1 AU-2 till AU-12 – Omfattar innehåll i revisionsloggar, granskning, logglagring och automatiserad avisering.

11.3.2 SI-4 – Kräver detektering av systemavvikelser och rapportering av misstänkta händelser.

11.4 EU:s dataskyddsförordning (GDPR)

11.4.1 Artikel 5.1 f – Kräver riktighet och konfidentialitet för personuppgifter, vilket omfattar loggning av åtkomst.

11.4.2 Artikel 32 – Kräver tekniska och organisatoriska åtgärder för att säkerställa säkerhet, inklusive loggning och övervakning.

11.4.3 Artikel 33 – Kräver snabb anmälan av personuppgiftsincidenter, med stöd av loggar som möjliggör rotorsaksanalys (RCA).

11.5 EU:s NIS2-direktiv

11.5.1 Artikel 21.2 d – Kräver loggningsmekanismer som upptäcker avvikelser och ger stöd vid incidentutredningar.

11.5.2 Artikel 23 – Kräver rapportering av incidenter inom 24 timmar, vilket är beroende av korrekt och tillgänglig loggdata i rätt tid.

11.6 DORA-förordningen

11.6.1 Artikel 10 – Kräver digital operativ resiliens, inklusive spårbarhet för IKT-relaterade incidenter genom loggning.

11.6.2 Artikel 15 – Kräver övervakning av tjänsteleverantörer, inklusive åtkomst till loggar och revisionsrätt.

11.7 COBIT 2019

11.7.1 DSS01.03 – Kräver spårbarhet av systemaktivitet genom loggning och övervakning.

11.7.2 DSS05.02 – Behandlar loggning som en central kontroll för skydd mot skadlig kod och annan obehörig aktivitet.