					Indsæt navnet på den registrerede juridiske enhed her						
Dokumentnummer: P22					Dokumenttitel: **Lognings- og overvågningspolitik**						
Version: 1.0		Ikrafttrædelsesdato: 01.01.2025			Dokumentejer:						
X	Politik		Standard		Procedure		Formular		Register		Andet

Revisionshistorik				
Revisionsnummer	**Revisionsdato**	**Ændringer**	**Gennemgået af**	**Procesejer**

Godkendelser			
Navn	**Stilling**	**Dato**	**Underskrift**

1. Formål

1.1 Formålet med denne politik er at fastsætte klare og bindende krav til generering, beskyttelse, gennemgang og analyse af logfiler, der registrerer væsentlige system- og sikkerhedshændelser på tværs af organisationens IT-miljø.

1.2 Logning og overvågning er afgørende for anomalidetektion, håndtering af sikkerhedshændelser, forensiske undersøgelser, revisionsberedskab og overholdelse af lovgivningsmæssige krav. Denne politik sikrer, at alle systemgenererede hændelser registreres korrekt, opbevares og kan korreleres med tidsmæssig nøjagtighed på grundlag af synkroniseret tid.

1.3 Denne politik er væsentlig for at understøtte ISO/IEC 27001 klausul 8.1 og bilag A, kontrollerne 8.15 (Logning), 8.16 (Overvågning) og 8.17 (Synkronisering af ure), og er direkte knyttet til regulatoriske forpligtelser efter GDPR, NIS2, DORA og COBIT 2019.

2. Omfang

2.1 Denne politik gælder for alle systemer, tjenester og miljøer, der lagrer, behandler eller overfører data omfattet af ledelsessystemet for informationssikkerhed (ISMS), herunder:

2.1.1 lokal infrastruktur, cloudbaserede tjenester (f.eks. IaaS, PaaS, SaaS) og hybride miljøer

2.1.2 operativsystemer, databaser, applikationer og netværksenheder

2.1.3 sikkerhedssystemer såsom SIEM-platforme, firewalls, endpoint detection and response (EDR)-platforme, VPN-koncentratorer og identitetsudbydere

2.2 Følgende interessenter er omfattet:

2.2.1 interne brugere med systemrettigheder eller administrative privilegier

2.2.2 infrastruktur- og driftsansvarlige i IT

2.2.3 Security Operations Center (SOC) og teams for trusselsdetektion

2.2.4 softwareudviklere og applikationsejere

2.2.5 tredjepartsleverandører, der administrerer systemer, som genererer logfiler

3. Mål

3.1 Sikre, at alle kritiske systemer genererer logfiler over sikkerhedshændelser og systemaktiviteter, som opbevares i overensstemmelse med regulatoriske, juridiske og kontraktlige krav.

3.2 Fastlægge minimumskrav til hændelsestyper og logindhold, der er nødvendige for at opdage uautoriserede aktiviteter, spore brugerhandlinger og understøtte forensiske undersøgelser.

3.3 Håndhæve beskyttelsesforanstaltninger, der forhindrer manipulation af logfiler, uautoriseret sletning eller ukontrolleret adgang til logdata.

3.4 Etablere centraliserede systemer til logning og alarmering (f.eks. SIEM) til at aggregere, korrelere og eskalere mistænkelig aktivitet nær realtid.

3.5 Sikre synkronisering af systemure for at muliggøre nøjagtig korrelation på tværs af systemer og analyse af sikkerhedshændelser.

3.6 Understøtte løbende forbedring og efterlevelse ved at integrere logovervågning med processer for revision, risikostyring og hændelseshåndtering.

4. Roller og ansvar

4.1 Chief Information Security Officer (CISO)

4.1.1 Er ansvarlig for denne politik og sikrer, at den er tilpasset organisationens risikoprofil, revisionskrav og ISMS-forpligtelser.

4.1.2 Godkender logningsomfanget for regulerede systemer eller højrisikosystemer og fører tilsyn med rapportering om efterlevelse.

4.2 Leder af Security Operations Center (SOC)

4.2.1 Driver og vedligeholder centraliserede platforme til logstyring (f.eks. SIEM).

4.2.2 Fastlægger regler for logaggregering, alarmeringstærskler og eskalationsveje for hændelsestriagering.

4.2.3 Gennemgår daglige rapporter og sikrer, at anomalier analyseres, dokumenteres og eskaleres efter behov.

[... Afsnit 4.3–8 er ikke inkluderet i denne forhåndsvisning. Køb det fulde dokument for at få adgang til det komplette indhold. ...]

9. Krav til gennemgang og opdatering

9.1 Denne politik skal gennemgås årligt eller tidligere som reaktion på:

9.1.1 væsentlige ændringer i systemarkitektur eller logningsinfrastruktur (f.eks. migrering af SIEM)

9.1.2 ændringer i regulatoriske krav til logning (f.eks. logningskrav efter NIS2 og DORA)

9.1.3 konstateringer fra revisioner eller efterhændelsesgennemgange

9.1.4 fremspirende risici, der kræver styrket overvågning (f.eks. insidertrusler eller kompromittering af forsyningskæden)

9.2 Gennemgangsprocessen skal ledes af lederen af Security Operations Center (SOC) i koordinering med CISO, risikostyring, compliance og IT-infrastrukturteams.

9.3 Godkendte ændringer skal versionsstyres i ISMS-dokumentstyringsregisteret og kommunikeres til:

9.3.1 alle interessenter med ansvar for vedligeholdelse af logningssystemer

9.3.2 applikations- og systemejere

9.3.3 tredjepartsleverandører med ansvar for telemetri eller SIEM-integration

9.4 Alle erstattede versioner skal arkiveres sikkert, og adgangen skal begrænses til autoriserede ISMS-forvaltere af hensyn til revision og juridiske formål.

10. Relaterede politikker og sammenhænge

10.1 P1 – Informationssikkerhedspolitik. Fastlægger det overordnede tilsagn om at beskytte systemer og data, hvor logning og overvågning fungerer som kritiske detekterende og responsunderstøttende mekanismer.

10.2 P4 – Politik for adgangskontrol. Sikrer, at privilegeret adgang, brugerlogin og autorisationshændelser registreres i logfiler og overvåges for misbrug eller anomal adfærd.

10.3 P5 – Politik for ændringsstyring. Kræver logning af systemændringer, patchudrulninger og konfigurationsopdateringer, som kan introducere risiko eller uautoriserede ændringer.

10.4 P21 – Politik for netværkssikkerhed. Kræver logning på netværksniveau (f.eks. firewalllogfiler, IDS/IPS-alarmer og VPN-aktivitet) samt integration med SIEM for synlighed i trafikafvigelser og beskyttelse af systemgrænser.

10.5 P23 – Politik for tidssynkronisering. Håndhæver ensartet tid på tværs af systemer, hvilket er afgørende for pålidelig logning og korrelation af sikkerhedshændelser på tværs af flere miljøer.

10.6 P30 – Politik for hændelseshåndtering. Er afhængig af logdata og alarmeringsmekanismer til at identificere, undersøge og håndtere sikkerhedshændelser, samtidig med at forensiske artefakter bevares til efterhændelsesgennemgang.

11. Referencestandarder og rammeværker

11.1 ISO/IEC 27001

11.1.1 Klausul 8.1 – operationel planlægning og styring: Kræver kontroller for overvågning af driften og beskyttelse mod uautoriseret adgang til og misbrug af systemer.

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

11.2.1 Fastlægger detaljerede krav til logning, herunder hvilke hændelser der skal registreres, hvordan logfiler skal beskyttes og analyseres, og hvordan pålideligheden af tidsstempler på tværs af systemer sikres.

11.3 NIST SP 800-53 Rev. 5

11.3.1 AU-2 til AU-12: Dækker udvælgelse af hændelser, logning, beskyttelse, revisionsgennemgang, respons på revisionsfejl og opbevaring af revisionsspor.

11.3.2 SI-4 – systemovervågning: Kræver aktiv systemovervågning med alarmer baseret på anomal adfærd.

11.3.3 SC-45 – synkronisering af systemtid: Understreger kravet om tidsmæssig nøjagtighed for sporbarhed af hændelser og korrelation ved sikkerhedshændelser.

11.4 EU GDPR (2016/679)

11.4.1 Artikel 32 – behandlingssikkerhed: Kræver tekniske kontroller såsom logning og overvågning for at sikre sikkerhed og ansvarlighed, særligt ved adgang til personoplysninger.

11.5 EU NIS2-direktivet (2022/2555)

11.5.1 Artikel 21(2)(e): Kræver systemer til logning af hændelser og overvågning til hurtig detektion af og respons på sikkerhedshændelser.

11.6 EU DORA (2022/2554)

11.6.1 Artikel 9 – styring af IKT-risiko: Kræver mekanismer til at opdage anomal aktivitet, logge hændelser og opbevare forensiske data.

11.6.2 Artikel 11 – test af planer for IKT-forretningskontinuitet: Fremhæver behovet for kontinuitet i overvågningen og validering af logtilgængelighed under driftsforstyrrelser.

11.7 COBIT 2019

11.7.1 DSS01.05 – Manage Security Logs: Kræver implementering af logningskapacitet for al kritisk infrastruktur.

11.7.2 DSS05.04 – Monitor Security Events: Kræver realtidsovervågning og analyse af logfiler for at opdage og reagere på hændelser.

11.7.3 MEA03 – Monitor, Evaluate, and Assess Compliance: Kræver regelmæssig gennemgang af logningspraksis og tilpasning til kontrolmålsætninger.