					Indsæt navnet på den registrerede juridiske enhed her							
Dokumentnummer: P22S					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**

Tilpasset relevante standarder og regler

Standard/regulering	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Klausul 8	operationelle kontroller, herunder logning
ISO/IEC 27002:2022	Kontroller 8.15, 8.16, 8.17	hændelseslogning, beskyttelse af logfiler og overvågning
NIST SP 800-53 Rev.5	AU-2 til AU-12, SI-4	indhold i revisionslogfiler/gennemgang, opbevaring, anomalidetektion, alarmering
EU GDPR	Artikel 5, stk. 1, litra f, artikel 32, artikel 33	fortrolighed og integritet af data, tekniske foranstaltninger og underretning om brud på persondatasikkerheden
EU NIS2	Artikel 21, stk. 2, litra d, artikel 23	logningsmekanismer til anomalidetektion og rapportering af hændelser inden for 24 timer
EU DORA	Artikel 10, artikel 15	operationel robusthed, overvågning og logning af tjenesteudbydere
COBIT 2019	DSS01.03, DSS05.02	sporbarhed af aktivitet og beskyttelse via logning og overvågning

1. Formål

1.1 Denne politik fastsætter obligatoriske kontroller for logning og overvågning med henblik på at sikre sikkerhed, ansvarlighed og operationel integritet i organisationens IT-systemer.

1.2 Politikken definerer, hvilke typer hændelser der skal logges, hvordan logfiler skal opbevares, hvordan de skal gennemgås, samt medarbejderes og tjenesteudbyderes ansvar.

1.3 Logning og overvågning understøtter trusselsdetektion, overholdelse af lovgivningsmæssige krav, hændelseshåndtering og retsmedicinsk analyse.

1.4 Denne politik gør det muligt for organisationen at opfylde kravene til operationelle kontroller i ISO/IEC 27001 og understøtter løbende revisionsberedskab, kundetillid samt efterlevelse af GDPR, NIS2 og DORA.

2. Omfang

2.1 Denne politik gælder for alle systemer og brugere i organisationen, herunder:

2.1.1 Arbejdsstationer, bærbare computere, servere, firewalls, switche, routere og trådløse adgangspunkter

2.1.2 Cloudtjenester, der anvendes til forretningsdrift, f.eks. e-mail, fillagring, backup-løsninger og samarbejdsværktøjer

2.1.3 Logningsfunktioner i antivirus, applikationer, operativsystemer og netværksudstyr

2.1.4 Alle medarbejdere, kontrahenter og managed service providers (MSP'er), der anvender eller administrerer systemer

2.1.5 Enhver lokation, hvor virksomhedens IT-systemer anvendes, herunder miljøer for fjernarbejde, hybride arbejdsformer eller BYOD

2.2 Politikken gælder også for logfiler genereret af tredjepartstjenester, hvor organisationen har administrativ adgang eller revisionsrettigheder i henhold til kontrakt.

3. Mål

3.1 Sikre logning af systemaktivitet, herunder autentifikation, konfigurationsændringer, adgang til følsomme data og sikkerhedsalarmer

3.2 Opretholde sikre og korrekte logfiler for at kunne opdage brud på politikken, systemfejl eller uautoriserede handlinger

3.3 Muliggøre hurtig gennemgang af logfiler i forbindelse med hændelser, undersøgelser og audits

3.4 Understøtte tidssynkronisering for at sikre integritet og korrelation af logdata

3.5 Beskytte logfiler mod manipulation, tab eller for tidlig sletning

3.6 Opfylde juridiske og regulatoriske forpligtelser vedrørende systemmæssig ansvarlighed, sporbarhed og håndtering af brud på persondatasikkerheden

4. Roller og ansvar

4.1 Direktør (GM)

4.1.1 Godkender denne politik og sikrer implementering på tværs af alle forretningssystemer

4.1.2 Gennemgår alarmer med høj alvorlighedsgrad og væsentlige revisionskonstateringer rapporteret af IT eller databeskyttelsesfunktionen

4.1.3 Godkender undtagelser, hvor logning eller opbevaring ikke kan håndhæves teknisk

4.2 IT-supportleverandør / intern IT-funktion

4.2.1 Implementerer og konfigurerer logning for operativsystemer, netværksenheder, antivirusværktøjer og centrale applikationer

4.2.2 Sikrer, at logfiler opbevares, sikkerhedskopieres og beskyttes mod ændringer

4.2.3 Gennemgår logfiler efter en fastlagt plan og undersøger mistænkelig eller uautoriseret aktivitet

4.2.4 Vedligeholder alarmeringssystemer, der identificerer anomal adfærd eller indikatorer på kompromittering

[... 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 Årlig gennemgang

9.1.1 Denne politik skal gennemgås mindst én gang årligt af direktøren med støtte fra IT-supportleverandøren og privatlivskoordinatoren.

9.2 Udløsende forhold for gennemgang

9.2.1 Ikke-planlagte gennemgange skal gennemføres som reaktion på:

9.2.1.1 Konstateringer relateret til logning fra interne eller eksterne audits

9.2.1.2 Sikkerhedshændelser, hvor logfiler manglede, var korrupte eller utilstrækkelige

9.2.1.3 Væsentlige ændringer i IT-infrastrukturen, f.eks. migrering til cloudbaserede logningsplatforme

9.2.1.4 Opdateringer af juridiske eller regulatoriske forpligtelser, f.eks. GDPR, NIS2 og DORA

9.3 Versionsstyring

9.3.1 Alle ændringer til denne politik skal registreres med versionsnummer, dato og et resumé af revisionerne

9.3.2 Tidligere versioner skal arkiveres og opbevares i mindst 3 år

9.3.3 Opdaterede politikker skal kommunikeres til berørte interessenter, især dem med konti på systemniveau

10. Relaterede politikker og sammenhænge

10.1 Denne politik understøtter direkte og understøttes af følgende SME-politikker for informationssikkerhed:

10.1.1 P17S – Databeskyttelses- og privatlivspolitik: Sikrer, at logdata, der indeholder personoplysninger, håndteres med integritet, korrekt opbevaring og adgangskontrol i overensstemmelse med GDPR-krav.

10.1.2 P21S – Politik for netværkssikkerhed: Danner grundlag for indsamling af logfiler relateret til firewalls, trådløs adgang, VPN'er og overvågning af segmentering.

10.1.3 P24S – Politik for sikker udvikling: Sikrer, at applikationslogfiler, f.eks. for loginforsøg, fejl og undtagelser, indarbejdes i softwaredesign og drift.

10.1.4 P30S – Politik for hændelseshåndtering: Er afhængig af korrekte og fuldstændige logdata til at opdage, analysere og reagere på informationssikkerhedshændelser.

10.1.5 P23S – Politik for tidssynkronisering: Sikrer ensartede og sporbare tidsstempler på tværs af alle systemer, så logfiler kan korreleres under undersøgelser.

11. Referencestandarder og rammeværker

11.1 ISO/IEC 27001

11.1.1 Klausul 8.1 – Kræver implementering af operationelle kontroller til at reducere informationssikkerhedsrisici, herunder logning.

11.2 ISO/IEC 27002

11.2.1 Kontrol 8.15 – Kræver hændelseslogning for at understøtte anomalidetektion og ansvarlighed.

11.2.2 Kontrol 8.16 – Kræver beskyttelse af logfiler mod manipulation og uautoriseret adgang.

11.2.3 Kontrol 8.17 – Kræver overvågningssystemer til usædvanlig aktivitet og bekræftelse af effektiviteten af overvågningskontroller.

11.3 NIST SP 800-53 Rev.5

11.3.1 AU-2 til AU-12 – Omfatter indhold i revisionslogfiler, gennemgang, opbevaring og automatiseret alarmering.

11.3.2 SI-4 – Kræver detektion af systemanomalier og rapportering af mistænkelige hændelser.

11.4 EU GDPR

11.4.1 Artikel 5, stk. 1, litra f – Kræver integritet og fortrolighed for personoplysninger, hvilket omfatter logning af adgang.

11.4.2 Artikel 32 – Pålægger tekniske og organisatoriske foranstaltninger for at sikre sikkerhed, herunder logning og overvågning.

11.4.3 Artikel 33 – Kræver rettidig underretning om brud på persondatasikkerheden, understøttet af logfiler, der muliggør rodårsagsanalyse.

11.5 EU NIS2-direktivet

11.5.1 Artikel 21, stk. 2, litra d – Kræver logningsmekanismer, der detekterer anomalier og understøtter undersøgelser af hændelser.

11.5.2 Artikel 23 – Pålægger rapportering af hændelser inden for 24 timer, hvilket afhænger af korrekte og rettidige logdata.

11.6 EU DORA

11.6.1 Artikel 10 – Kræver digital operationel robusthed, herunder sporbarhed af IKT-relaterede hændelser gennem logning.

11.6.2 Artikel 15 – Forpligter til overvågning af tjenesteudbydere, herunder adgang til logfiler og rettigheder til gennemgang.

11.7 COBIT 2019

11.7.1 DSS01.03 – Kræver sporbarhed af systemaktivitet gennem logning og overvågning.

11.7.2 DSS05.02 – Behandler logning som en nøglekontrol til beskyttelse mod malware og anden uautoriseret aktivitet.