					Indsæt navnet på den registrerede juridiske enhed her						
Dokumentnummer: P08S					Dokumenttitel: **Politik for informationssikkerhedsbevidsthed og -uddannelse**						
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 7	
ISO/IEC 27002:2022	Kontrol 6	
NIST SP 800-53 Rev.5	AT-2, AT-4	
EU NIS2	Artikel 21(2)(i)	
EU DORA	Artikel 13	
COBIT 2019	BAI08, DSS	
EU GDPR	Artikel 32, 39	

1. Formål

1.1. Denne politik sikrer, at alle medarbejdere og kontrahenter forstår deres ansvar vedrørende informationssikkerhed.

1.2. Formålet er at reducere sandsynligheden for menneskelige fejl, forbedre evnen til at opdage og rapportere hændelser samt fremme en sikkerhedsbevidst kultur i hele organisationen.

1.3. Politikken understøtter overholdelse af ISO/IEC 27001, NIS2, GDPR og DORA ved at gøre sikkerhedsbevidsthed til en del af den daglige arbejdsadfærd og de rollebaserede forventninger.

2. Omfang

2.1. Denne politik gælder for alle medarbejdere, kontrahenter, praktikanter og tredjeparter, der har adgang til virksomhedens systemer eller data.

2.2. Den omfatter:

2.2.1. Introducerende sikkerhedsbevidsthedstræning ved onboarding for nyt personale

2.2.2. Årlig genopfriskningstræning i informationssikkerhed

2.2.3. Ad hoc-aktiviteter vedrørende sikkerhedsbevidsthed (f.eks. hændelsesrelaterede opdateringer, plakater eller vejledninger)

2.3. Politikken gælder på tværs af alle jobfunktioner, afdelinger og arbejdssteder.

3. Mål

3.1. Sikre, at alt personale modtager rettidig, forståelig og relevant træning i informationssikkerhedsbevidsthed.

3.2. Sætte medarbejdere i stand til at identificere og undgå almindelige trusler såsom phishing, malware og datalæk.

3.3. Etablere dokumentation for gennemført træning, så overholdelse af juridiske, kontraktlige og revisionsmæssige krav kan dokumenteres.

3.4. Opretholde opdateret træningsindhold, der afspejler organisationens politikker, trusler og gældende regulering.

3.5. Fremme en proaktiv tilgang blandt medarbejdere, hvor sikkerhed betragtes som en del af det daglige ansvar.

4. Roller og ansvar

4.1. Direktør

4.1.1. Godkender træningskrav og sikrer, at de nødvendige ressourcer afsættes.

4.1.2. Gennemgår rapporter om gennemført træning og eskalerer manglende efterlevelse, hvor det er nødvendigt.

4.2. Kontorleder / HR

4.2.1. Koordinerer gennemførelsen af onboarding-træning for nyansatte samt den årlige genopfriskningstræning.

4.2.2. Vedligeholder træningsregistreringer og træningslogfiler.

4.2.3. Sikrer medarbejdernes bekræftelse af centrale informationssikkerhedspolitikker og fortrolighedserklæringer.

[... 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 årligt af direktøren og HR for at sikre, at den afspejler aktuelle risici, regulatoriske krav og arbejdsstyrkens behov.

9.2. Løbende opdateringer

9.2.1. Politikken og træningsindholdet skal også gennemgås og revideres efter:

9.2.1.1. En væsentlig sikkerhedshændelse

9.2.1.2. Juridiske eller kontraktlige ændringer

9.2.1.3. Organisatoriske omstruktureringer eller systemmigreringer

9.3. Versionsstyring og distribution

9.3.1. Hver opdatering skal omfatte:

9.3.1.1. Versionsnummer og ikrafttrædelsesdato

9.3.1.2. Resumé af ændringer

9.3.1.3. Godkendelse fra direktøren

9.3.1.4. Arkiv over alle tidligere versioner, opbevaret i mindst tre år

9.4. Kommunikation til medarbejdere

9.4.1. Opdateringer af politikken skal kommunikeres til alle medarbejdere, og bekræftelse skal indhentes, hvis der foretages væsentlige ændringer.

10. Relaterede politikker og sammenhænge

10.1. Denne politik understøtter følgende:

10.1.1. P2S – Politik for styringsroller og ansvarsområder: Fastlægger ansvar for koordinering og tilsyn med træning

10.1.2. P3S – Politik for acceptabel brug: Understøtter de adfærdsforventninger, der behandles i træningen

10.1.3. P4S – Politik for adgangskontrol: Sikrer, at brugere forstår betydningen af sikker adgang

10.1.4. P7S – Politik for onboarding og fratrædelse: Integrerer træning i tiltrædelsesprocessen

10.1.5. P30S – Politik for hændelseshåndtering: Sikrer, at medarbejdere ved, hvordan hændelser rapporteres rettidigt og korrekt

11. Referencestandarder og rammeværk

11.1. ISO/IEC 27001

11.1.1. Klausul 7.3 – Kræver, at organisationer sikrer, at personale er bevidst om deres ansvar og deres sikkerhedsmæssige påvirkning

11.2. ISO/IEC 27002

11.2.1. Kontrol 6.3 – Beskriver forventninger til omfang og gennemførelse af sikkerhedstræning

11.3. NIST SP 800-53 Rev.5

11.3.1. AT-2 – Kræver træning i sikkerhedsbevidsthed for brugere med systemadgang

11.3.2. AT-4 – Omfatter rollebaseret træning og konsekvenser ved manglende efterlevelse

11.4. EU GDPR

11.4.1. Artikel 32 – Pålægger sikkerhedsforanstaltninger, herunder træning af personale, for at beskytte personoplysninger

11.4.2. Artikel 39 – Kræver, hvor relevant, at databeskyttelsesrådgivere fører tilsyn med sikkerhedsbevidsthed og træning

11.5. EU NIS2-direktivet

11.5.1. Artikel 21(2)(i) – Kræver løbende programmer for cybersikkerhedsbevidsthed og træning

11.6. EU DORA

11.6.1. Artikel 13 – Kræver, at finansielle enheder implementerer uddannelse og træning for alt personale med IKT-relaterede ansvarsområder

11.7. COBIT 2019

11.7.1. BAI08 – Manage Knowledge: Sikrer, at medarbejdere er kompetente og uddannede

11.7.2. DSS05 – Manage Security Services: Fremhæver sikkerhedsbevidsthed som en central forebyggende kontrol