					Indsæt navnet på den registrerede juridiske enhed her						
Dokumentnummer: P08					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 7.3, bilag A kontrol 6.3	Fastlægger krav til bevidsthed og uddannelse, som behandles i denne politik
ISO/IEC 27002:2022	Kontrol 6	Understøtter passende awareness-træning tilpasset jobroller
NIST SP 800-53 Rev.5	AT-1 til AT-5	Er tilpasset politikker og procedurer, awareness-træning, rollebaseret træning, træningsregistre og kontakt til sikkerhedsgrupper
EU GDPR	Artikel 32, 39; betragtning 78	Kræver træning for personer, der behandler personoplysninger, samt generel medarbejderbevidsthed
EU NIS2	Artikel 21(2)(a, b), 21(3)	Kræver politikker for risiko- og sikkerhedstræning samt bevidstgørelsesinitiativer
EU DORA	Artikel 5, 8, 13	Kræver bevidsthed om IKT-risici og træning som en del af robusthedskontroller
COBIT 2019	APO07, DSS05, MEA	Understreger arbejdsstyrkens bevidsthed, brugeruddannelse og overvågning af efterlevelse

1. Formål

1.1 Denne politik fastlægger de formelle rammer for at sikre, at alt personale er bekendt med deres sikkerhedsansvar og modtager den uddannelse, der er nødvendig for at beskytte informationsaktivers fortrolighed, integritet og tilgængelighed.

1.2 Den understøtter ISO/IEC 27001 klausul 7.3 og bilag A kontrol 6.3 ved at kræve et struktureret og risikobaseret program for bevidstgørelse og uddannelse, der er tilpasset organisatoriske roller og udviklingen i trusselsbilledet.

1.3 Politikken bidrager til at reducere menneskeskabte sårbarheder, fremme sikkerhedsbevidst adfærd og løbende styrke sikre arbejdsmetoder i overensstemmelse med regulatoriske og kontraktlige krav.

2. Omfang

2.1 Denne politik gælder for alle interne og eksterne personer med adgang til organisationens informationssystemer, data eller faciliteter, herunder:

2.1.1 Medarbejdere (fuldtid, deltid, midlertidigt ansatte)

2.1.2 Kontrahenter, konsulenter, leverandører og praktikanter

2.1.3 Tredjeparter med logisk eller fysisk adgang i henhold til serviceaftaler

2.2 Omfanget omfatter:

2.2.1 Indledende onboarding-træning i informationssikkerhedsbevidsthed

2.2.2 Rollespecifik uddannelse (f.eks. udviklere, økonomimedarbejdere, privilegerede brugere)

2.2.3 Periodisk genopfriskningstræning og bevidstgørelseskampagner

2.2.4 Ad hoc-træning som reaktion på hændelser eller nye trusler

2.3 Uddannelsesformer omfattet af denne politik omfatter e-læring, fysiske briefinger, simuleringer, videnstest, plakater, nyhedsbreve og obligatoriske bekræftelser.

3. Mål

3.1 At sikre, at alt personale forstår deres ansvar for at beskytte organisationens aktiver og efterleve sikkerhedspolitikkerne.

3.2 At levere løbende og målbar awareness-træning, der er tilpasset den rollebaserede risikoeksponering.

3.3 At forankre sikker adfærd i den daglige drift ved at styrke praksisser som sikker brug af adgangskoder, rapportering af hændelser og modstandsdygtighed over for phishing.

3.4 At sikre efterlevelse af regulatoriske krav og revisionsberedskab for krav til informationssikkerhedstræning på tværs af brancher og jurisdiktioner.

3.5 At reducere sikkerhedshændelser, der skyldes uagtsomhed, manglende bevidsthed eller dårlig dømmekraft, gennem adfærdspåvirkning og løbende forstærkning.

4. Roller og ansvar

4.1 Den øverste ledelse

4.1.1 Godkender organisationens strategi for informationssikkerhedstræning og sikrer, at den er tilstrækkeligt ressourceunderstøttet og integreret i virksomhedens prioriteter.

4.1.2 Overvåger efterlevelse på ledelsesniveau og sikrer overholdelse af politikker på tværs af afdelinger.

4.2 CISO / ISMS-ansvarlig

4.2.1 Ejer denne politik og fastlægger rammerne for bevidstgørelse og uddannelse i overensstemmelse med risiko, efterlevelse og forretningsbehov.

4.2.2 Fører tilsyn med udformning, levering, sporing og gennemgang af alle initiativer vedrørende sikkerhedstræning.

4.2.3 Sikrer, at uddannelsen opdateres periodisk og afspejler nye trusler og teknologier.

[... 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 Gennemgangsfrekvens

9.1.1 Denne politik og det tilknyttede træningsprogram skal gennemgås:

9.1.1.1 Årligt, eller

9.1.1.2 Efter større hændelser, der involverer menneskelige fejl eller insidertrusler

9.1.1.3 Ved indførelse af væsentlige nye teknologier eller trusler

9.1.1.4 Som reaktion på ændringer i juridiske, kontraktlige eller certificeringsmæssige forpligtelser

9.2 Gennemgangsproces

9.2.1 Gennemgangen skal ledes af CISO i koordinering med:

9.2.1.1 HR- og uddannelsesafdelinger

9.2.1.2 Juridisk afdeling og databeskyttelsesrådgivere

9.2.1.3 IT-sikkerheds- og operationelle risikofunktioner

9.2.2 Alle opdateringer skal:

9.2.2.1 Godkendes af ISMS-styregruppen

9.2.2.2 Være versionsstyrede og dokumenteret i ISMS-dokumentregistret

9.2.2.3 Kommunikeres til brugerne, hvis væsentlige ændringer påvirker træningens omfang eller ansvar

9.3 Styring af indholdsopdateringer

9.3.1 Træningsmoduler og bevidstgørelsesmateriale skal gennemgås hver 12. måned for at sikre:

9.3.1.1 Relevans i forhold til trusselslandskabet

9.3.1.2 Regulatorisk korrekthed

9.3.1.3 Formatkompatibilitet (f.eks. tilgængelighed, lokalisering)

9.3.2 Forældet eller vildledende indhold skal straks trækkes tilbage og erstattes af godkendte alternativer.

10. Relaterede politikker og sammenhænge

10.1 Denne politik understøttes af og understøtter håndhævelsen af:

10.1.1 P01 – Informationssikkerhedspolitik: Fastlægger sikkerhedsbevidsthed som en grundlæggende kontrol i organisationens ledelsessystem for informationssikkerhed (ISMS).

10.1.2 P03 – Politik for acceptabel brug: Kræver brugerbekræftelse under træning og tydeliggør ansvar knyttet til daglig brug af teknologi.

10.1.3 P07 – Politik for onboarding og fratrædelse: Sikrer, at træning er integreret ved tiltrædelse og spores gennem hele ansættelsesforholdet.

10.1.4 P06 – Risikostyringspolitik: Knytter menneskecentreret træning til trusselsmodellering og strategier for reduktion af restrisiko.

10.1.5 P33 – Politik for revisions- og complianceovervågning: Validerer, at bevidstgørelseskontroller er operationelle, målbare og effektive under revisioner.

10.2 Samlet udgør disse politikker en omfattende styringsramme for adfærdsmæssige kontroller, som integrerer bevidstgørelse, ansvarlighed og kulturel forankring.

11. Referencestandarder og rammeværk

11.1 ISO/IEC 27001

11.1.1 Klausul 7.3 – Bevidsthed: Kræver, at organisationer sikrer, at medarbejdere er bekendt med informationssikkerhedspolitikker og deres ansvar. Denne politik operationaliserer dette krav gennem struktureret onboarding, periodisk træning og målbar deltagelse i kampagner.

11.1.2 Bilag A kontrol 6.3 – Informationssikkerhedsbevidsthed, uddannelse og træning: Fuldt adresseret gennem indledende, rollebaserede og løbende træningsprogrammer, der er tilpasset brugernes risikoprofiler.

11.2 ISO/IEC 27002:2022 – Kontrol 6

11.2.1 Understøtter udvikling og levering af awareness-træning, der er passende for jobroller, med vægt på styrkelse af sikker adfærd og periodiske opdateringer baseret på trusselsintelligens og revisionsfeedback.

11.3 NIST SP 800-53 Rev.5

11.3.1 AT-1 til AT-5 (familien Awareness and Training): Denne politik er tilpasset AT-1 (politikker og procedurer), AT-2 (awareness-træning), AT-3 (rollebaseret træning), AT-4 (registreringer af sikkerhedstræning) og AT-5 (kontakt med sikkerhedsgrupper).

11.3.2 IA-5, AC-2: Styrker brugeransvaret for sikker autentifikation og acceptabel brug, som er centrale for de adfærdsmæssige resultater af bevidstgørelsesprogrammer.

11.3.3 IR-1 til IR-8: Beredskabet for hændelseshåndtering styrkes gennem målrettede bevidstgørelseskampagner og simuleringer.

11.4 EU GDPR (2016/679)

11.4.1 Artikel 32 – Behandlingssikkerhed: Kræver, at personale, der håndterer personoplysninger, er uddannet til at identificere, forebygge og rapportere risici vedrørende personoplysninger. Denne politik sikrer, at dataansvarlige roller og alle relevante funktioner uddannes i overensstemmelse hermed.

11.4.2 Artikel 39 – Opgaver for databeskyttelsesrådgiveren: Omfatter at øge bevidstheden og uddanne personale, der er involveret i behandlingsaktiviteter.

11.4.3 Betragtning 78: Tilskynder til passende bevidstgørelsestiltag for at sikre robuste sikkerhedspraksisser og efterlevelse af politikker.

11.5 EU NIS2-direktivet (2022/2555)

11.5.1 Artikel 21(2)(a, b): Kræver, at enheder vedtager politikker om risikoanalyse og sikkerhedstræning for alt relevant personale. Denne politik opfylder dette krav ved at etablere løbende og rollefølsomme træningsprocesser.

11.5.2 Artikel 21(3): Tilskynder til at fremme bevidsthed om cybersikkerhedsrisici blandt ledelse og medarbejdere gennem bevidstgørelsesinitiativer og simuleringer.

11.6 EU DORA (2022/2554)

11.6.1 Artikel 13 – Strategi for digital operationel robusthed: Kræver, at bevidsthed om IKT-risici og træning indgår i styringsmodellen. Denne politik sikrer, at menneskelige risici adresseres gennem løbende uddannelse og trusselssimulering.

11.6.2 Artikel 5 og 8: Understreger vigtigheden af interne kontrolrammer, hvor bevidstgørelse og træning er grundlæggende komponenter i IKT-robusthed og cyberhygiejne.

11.7 COBIT 2019

11.7.1 APO07 – Managed Human Resources: Understreger behovet for at udvikle bevidsthed om sikkerhedsansvar og integrere dette i arbejdsstyringsprocesser.

11.7.2 DSS05 – Managed Security Services: Etablerer kontroller for brugeruddannelse og rapportering af hændelser, som begge er integrerede dele af denne politik.

11.7.3 MEA03 – Monitor, Evaluate, and Assess Compliance: Kræver gennemgang af effektiviteten af brugeradfærd og efterlevelse af politikker, implementeret her via phishing-tests, quizzer og kampagnemålinger.