					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: P08					Dokumenttitel: **Informationssäkerhetsmedvetenhets- och utbildningspolicy**							
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**

Ansluten till standarder och regelverk

Standard/regelverk	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Klausul 7.3, bilaga A kontroll 6.3	Fastställer krav på medvetenhet och utbildning som behandlas i denna policy
ISO/IEC 27002:2022	Kontroll 6	Stödjer lämplig rollbaserad medvetenhetsutbildning
NIST SP 800-53 Rev.5	AT-1 till AT-5	Överensstämmer med policy och rutiner, medvetenhetsutbildning, rollbaserad utbildning, utbildningsregister och kontakt med säkerhetsgrupper
EU:s dataskyddsförordning (GDPR)	Artiklarna 32, 39; skäl 78	Kräver utbildning för personer som hanterar personuppgifter samt allmän medvetenhet hos personal
EU:s NIS2-direktiv	Artiklarna 21(2)(a, b), 21(3)	Kräver policyer för risk- och säkerhetsutbildning samt medvetenhetsinsatser
EU:s DORA-förordning	Artiklarna 5, 8, 13	Kräver medvetenhet om IKT-risker och utbildning som en del av kontroller för digital operativ motståndskraft
COBIT 2019	APO07, DSS05, MEA	Förstärker arbetsstyrkans medvetenhet, användarutbildning och övervakning av efterlevnad

1. Syfte

1.1 Denna policy fastställer ett formellt ramverk för att säkerställa att all personal är medveten om sitt ansvar inom informationssäkerhet och får den utbildning som krävs för att skydda informationstillgångars konfidentialitet, riktighet och tillgänglighet.

1.2 Den stödjer ISO/IEC 27001 klausul 7.3 och bilaga A kontroll 6.3 genom att kräva ett strukturerat och riskbaserat program för medvetenhet och utbildning, anpassat till organisatoriska roller och föränderliga hot.

1.3 Policyn bidrar till att minska människorelaterade sårbarheter, främja säkerhetsmedvetet beteende och fortlöpande förstärka säkra arbetssätt i linje med regulatoriska skyldigheter och avtalskrav.

2. Omfattning

2.1 Denna policy gäller för alla interna och externa personer med åtkomst till organisationens informationssystem, data eller lokaler, inklusive:

2.1.1 anställda (heltid, deltid, visstidsanställda)

2.1.2 entreprenörer, tredjepartsleverantörer, konsulter och praktikanter

2.1.3 tredje parter med logisk eller fysisk åtkomst enligt tjänsteavtal

2.2 Omfattningen inkluderar:

2.2.1 introduktionsutbildning i säkerhetsmedvetenhet

2.2.2 rollspecifik utbildning (t.ex. utvecklare, ekonomi, privilegierade användare)

2.2.3 återkommande repetitionsutbildning och medvetenhetskampanjer

2.2.4 ad hoc-utbildning som svar på incidenter eller nya hot

2.3 Leveransformer för utbildning som omfattas av denna policy inkluderar e-lärande, fysiska informationsgenomgångar, simuleringar, kunskapstester, affischer, nyhetsbrev och obligatoriska bekräftelser.

3. Mål

3.1 Att säkerställa att all personal förstår sitt ansvar för att skydda organisationens tillgångar och följa säkerhetspolicyer.

3.2 Att tillhandahålla löpande och mätbar medvetenhetsutbildning anpassad till rollbaserad riskexponering.

3.3 Att integrera säkra beteenden i den dagliga verksamheten genom att förstärka arbetssätt såsom säker lösenordshantering, incidentrapportering och motståndskraft mot nätfiske.

3.4 Att säkerställa regelefterlevnad och revisionsberedskap avseende krav på informationssäkerhetsutbildning inom olika branscher och jurisdiktioner.

3.5 Att minska säkerhetsincidenter som uppstår till följd av oaktsamhet, bristande medvetenhet eller dåligt omdöme genom beteendestyrning och kontinuerlig förstärkning.

4. Roller och ansvar

4.1 Verkställande ledning

4.1.1 Godkänner organisationens strategi för informationssäkerhetsutbildning och säkerställer att den är resursförsedd och integrerad i organisationens prioriteringar.

4.1.2 Utövar tillsyn över efterlevnad på ledningsnivå och säkerställer efterlevnad av policyn i hela organisationen.

4.2 Informationssäkerhetschef (CISO) / ISMS-ansvarig

4.2.1 Är policyägare för denna policy och fastställer ramverket för medvetenhet och utbildning i linje med risk, regelefterlevnad och verksamhetens behov.

4.2.2 Utövar tillsyn över utformning, genomförande, uppföljning och granskning av alla utbildningsinsatser inom informationssäkerhet.

4.2.3 Säkerställer att utbildningen uppdateras regelbundet och avspeglar föränderliga hot och framväxande tekniker.

[... Avsnitt 4.3–8 ingår inte i denna förhandsvisning. Köp det fullständiga dokumentet för att få tillgång till hela innehållet. ...]

9. Krav på granskning och uppdatering

9.1 Granskningsfrekvens

9.1.1 Denna policy och tillhörande utbildningsprogram ska granskas:

9.1.1.1 årligen, eller

9.1.1.2 efter större incidenter som involverar mänskliga fel eller insiderhot

9.1.1.3 vid införande av betydande nya tekniker eller hot

9.1.1.4 som svar på förändringar i rättsliga, avtalsmässiga eller certifieringsrelaterade skyldigheter

9.2 Granskningsprocess

9.2.1 Granskningen ska ledas av informationssäkerhetschefen (CISO) i samordning med:

9.2.1.1 HR- och utbildningsfunktioner

9.2.1.2 juridikfunktionen och dataskyddsombudet

9.2.1.3 funktioner för IT-säkerhet och operativ risk

9.2.2 Alla uppdateringar ska:

9.2.2.1 godkännas av informationssäkerhetsstyrgruppen (ISSC)

9.2.2.2 versionshanteras och dokumenteras i ISMS-dokumentregistret

9.2.2.3 kommuniceras till användare om väsentliga förändringar påverkar utbildningens omfattning eller ansvar

9.3 Styrning av innehållsuppdateringar

9.3.1 Utbildningsmoduler och medvetenhetsmaterial ska granskas var tolfte månad för att säkerställa:

9.3.1.1 relevans i förhållande till hotlandskapet

9.3.1.2 regulatorisk korrekthet

9.3.1.3 formatkompatibilitet (t.ex. tillgänglighet, lokalisering)

9.3.2 Föråldrat eller vilseledande innehåll ska omedelbart dras tillbaka och ersättas med godkända alternativ.

10. Relaterade policyer och kopplingar

10.1 Denna policy stöds av och stödjer tillämpningen av:

10.1.1 P01 – Informationssäkerhetspolicy: Fastställer säkerhetsmedvetenhet som en grundläggande kontroll i organisationens ISMS.

10.1.2 P03 – Policy för godtagbar användning: Kräver användarbekräftelse under utbildning och tydliggör ansvar kopplat till daglig användning av teknik.

10.1.3 P07 – Policy för introduktion och avslut: Säkerställer att utbildning integreras vid inträde och följs upp under hela anställningen.

10.1.4 P06 – Riskhanteringspolicy: Kopplar människocentrerad utbildning till hotmodellering och strategier för att minska kvarstående risk.

10.1.5 P33 – Policy för övervakning av revision och regelefterlevnad: Verifierar att medvetenhetskontroller är operativa, mätbara och effektiva vid revisioner.

10.2 Tillsammans bildar dessa policyer ett heltäckande ramverk för beteendekontroller som integrerar medvetenhet, ansvarsskyldighet och kulturell förstärkning.

11. Referensstandarder och ramverk

11.1 ISO/IEC 27001

11.1.1 Klausul 7.3 – Medvetenhet: Kräver att organisationer säkerställer att arbetstagare är medvetna om informationssäkerhetspolicyer och sitt ansvar. Denna policy omsätter det kravet i praktiken genom strukturerad introduktion, periodisk utbildning och mätbart deltagande i kampanjer.

11.1.2 Bilaga A kontroll 6.3 – Medvetenhet, utbildning och träning inom informationssäkerhet: Hanteras fullt ut genom inledande, rollbaserade och löpande utbildningsprogram anpassade till användarnas riskprofiler.

11.2 ISO/IEC 27002:2022 – Kontroll 6

11.2.1 Stödjer utveckling och genomförande av medvetenhetsutbildning anpassad till arbetsroller, med betoning på förstärkning av säkert beteende och periodiska uppdateringar baserade på hotinformation och återkoppling från revision.

11.3 NIST SP 800-53 Rev.5

11.3.1 AT-1 till AT-5 (familjen Awareness and Training): Denna policy överensstämmer med AT-1 (Policy and Procedures), AT-2 (Awareness Training), AT-3 (Role-Based Training), AT-4 (Security Training Records) och AT-5 (Contact with Security Groups).

11.3.2 IA-5, AC-2: Förstärker användarens ansvar för säker autentisering och godtagbar användning, vilket är centralt för de beteendemässiga resultaten av medvetenhetsprogrammet.

11.3.3 IR-1 till IR-8: Beredskapen för incidenthantering stärks genom riktade medvetenhetskampanjer och simuleringar.

11.4 EU:s dataskyddsförordning (2016/679)

11.4.1 Artikel 32 – Säkerhet i behandlingen: Kräver att personal som hanterar personuppgifter utbildas för att identifiera, förebygga och rapportera risker för personuppgifter. Denna policy säkerställer att personer som hanterar data och alla relevanta roller utbildas i enlighet med detta.

11.4.2 Artikel 39 – Dataskyddsombudets uppgifter: Omfattar att höja medvetenheten och utbilda personal som deltar i behandlingsaktiviteter.

11.4.3 Skäl 78: Uppmuntrar lämpliga medvetenhetsåtgärder för att säkerställa robusta säkerhetsrutiner och efterlevnad av policyn.

11.5 EU:s NIS2-direktiv (2022/2555)

11.5.1 Artikel 21(2)(a, b): Kräver att verksamheter antar policyer för riskanalys och säkerhetsutbildning för all relevant personal. Denna policy uppfyller kravet genom att fastställa kontinuerliga och rollanpassade utbildningsprocesser.

11.5.2 Artikel 21(3): Uppmuntrar till att främja medvetenhet om cybersäkerhetsrisker hos ledning och personal genom medvetenhetsinsatser och simuleringar.

11.6 EU:s DORA-förordning (2022/2554)

11.6.1 Artikel 13 – Strategi för digital operativ motståndskraft: Kräver att medvetenhet om IKT-risker och utbildning ingår i styrningsmodellen. Denna policy säkerställer att mänskliga risker hanteras genom löpande utbildning och hotsimulering.

11.6.2 Artiklarna 5 och 8: Betonar vikten av ramverk för intern kontroll, där medvetenhet och utbildning är grundläggande komponenter för IKT-motståndskraft och cyberhygien.

11.7 COBIT 2019

11.7.1 APO07 – Managed Human Resources: Förstärker behovet av att utveckla medvetenhet om säkerhetsansvar och integrera detta i arbetsstyrkehanteringen.

11.7.2 DSS05 – Managed Security Services: Fastställer kontroller för användarutbildning och incidentrapportering, vilka båda är integrerade delar av denna policy.

11.7.3 MEA03 – Monitor, Evaluate, and Assess Compliance: Kräver granskning av effektivitet i användarbeteende och efterlevnad av policy, vilket här genomförs genom phishingtester, kunskapstester och mätetal för medvetenhetskampanjer.