					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: P08S					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**

Anpassad till standarder och regelverk

Standard/regelverk	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Klausul 7	
ISO/IEC 27002:2022	Kontroll 6	
NIST SP 800-53 Rev.5	AT-2, AT-4	
EU:s NIS2-direktiv	Artikel 21(2)(i)	
EU:s DORA-förordning	Artikel 13	
COBIT 2019	BAI08, DSS	
EU:s GDPR	Artikel 32, 39	

1. Syfte

1.1. Denna policy säkerställer att alla anställda, entreprenörer och tredjepartsleverantörer förstår sitt ansvar avseende informationssäkerhet.

1.2. Syftet är att minska sannolikheten för mänskliga fel, förbättra förmågan att upptäcka och rapportera incidenter samt främja en säkerhetsmedveten kultur i hela organisationen.

1.3. Policyn möjliggör efterlevnad av ISO/IEC 27001, NIS2, GDPR och DORA genom att integrera säkerhetsmedvetenhet i det dagliga arbetet och i rollbaserade förväntningar.

2. Omfattning

2.1. Denna policy gäller för alla anställda, entreprenörer, tredjepartsleverantörer, praktikanter och andra tredje parter som har åtkomst till organisationens system eller data.

2.2. Den omfattar:

2.2.1. Introduktionsutbildning i säkerhetsmedvetenhet för nyanställda

2.2.2. Årlig repetitionsutbildning i säkerhetsmedvetenhet

2.2.3. Ad hoc-insatser för säkerhetsmedvetenhet (t.ex. incidentrelaterade uppdateringar, affischer eller råd)

2.3. Policyn gäller för samtliga befattningar, avdelningar och arbetsplatser.

3. Mål

3.1. Säkerställa att all personal får utbildning i säkerhetsmedvetenhet i rätt tid, och att utbildningen är begriplig och relevant.

3.2. Ge anställda förmåga att identifiera och undvika vanliga hot såsom nätfiske, skadlig kod och dataläckage.

3.3. Upprätta dokumentation över genomförda utbildningar för att kunna visa efterlevnad av rättsliga krav, avtalskrav och revisionskrav.

3.4. Upprätthålla aktuellt utbildningsinnehåll som återspeglar organisationens policyer, hotbild och tillämpliga regelverk.

3.5. Främja ett proaktivt förhållningssätt bland personalen, där säkerhet ses som en del av det dagliga ansvaret.

4. Roller och ansvar

4.1. Verkställande direktör

4.1.1. Godkänner utbildningskrav och säkerställer att tillräckliga resurser avsätts.

4.1.2. Granskar rapporter om genomförande och eskalerar bristande efterlevnad vid behov.

4.2. Kontorschef / HR

4.2.1. Samordnar genomförandet av introduktionsutbildning för nyanställda och årliga repetitionsutbildningar.

4.2.2. Upprätthåller utbildningsregister och utbildningsloggar.

4.2.3. Säkerställer att personal bekräftar centrala informationssäkerhetspolicyer och sekretessavtal (NDA).

[... 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. Årlig granskning

9.1.1. Denna policy ska granskas årligen av verkställande direktör och HR för att säkerställa att den återspeglar aktuella risker, regelverk och verksamhetens behov.

9.2. Uppdateringar mellan ordinarie granskningar

9.2.1. Policyn och utbildningsinnehållet ska även granskas och revideras efter:

9.2.1.1. En betydande säkerhetsincident

9.2.1.2. Rättsliga eller avtalsmässiga förändringar

9.2.1.3. Omstrukturering i organisationen eller systemmigreringar

9.3. Versionshantering och distribution

9.3.1. Varje uppdatering ska omfatta:

9.3.1.1. Versionsnummer och ikraftträdandedatum

9.3.1.2. Sammanfattning av ändringar

9.3.1.3. Godkännande av verkställande direktör

9.3.1.4. Arkiv över alla tidigare versioner som bevaras i minst tre år

9.4. Kommunikation till anställda

9.4.1. Uppdateringar av policyn ska kommuniceras till all personal, och bekräftelse ska inhämtas om väsentliga ändringar görs.

10. Relaterade policyer och kopplingar

10.1. Denna policy stödjer följande:

10.1.1. P2S – Policy för styrningsroller och ansvar: Tilldelar ansvar för samordning av utbildning och tillsyn

10.1.2. P3S – Policy för godtagbar användning: Förstärker beteendeförväntningar som tas upp i utbildningen

10.1.3. P4S – Åtkomstkontrollpolicy: Säkerställer att användare förstår betydelsen av säker åtkomst

10.1.4. P7S – Policy för introduktion och avslut: Integrerar utbildning i introduktionsprocessen

10.1.5. P30S – Policy för incidenthantering (P30): Säkerställer att personal vet hur incidenter ska rapporteras korrekt och utan dröjsmål

11. Referensstandarder och ramverk

11.1. ISO/IEC 27001

11.1.1. Klausul 7.3 – Kräver att organisationer säkerställer att personal är medveten om sitt ansvar och sin påverkan på säkerheten

11.2. ISO/IEC 27002

11.2.1. Kontroll 6.3 – Anger förväntningar på säkerhetsutbildningens omfattning och genomförande

11.3. NIST SP 800-53 Rev.5

11.3.1. AT-2 – Kräver utbildning i säkerhetsmedvetenhet för användare med systemåtkomst

11.3.2. AT-4 – Omfattar rollbaserad utbildning och konsekvenser vid bristande efterlevnad

11.4. EU:s GDPR

11.4.1. Artikel 32 – Kräver säkerhetsåtgärder, inklusive utbildning av personal, för att skydda personuppgifter

11.4.2. Artikel 39 – Kräver att dataskyddsombud, där så är tillämpligt, utövar tillsyn över insatser för säkerhetsmedvetenhet och utbildning

11.5. EU:s NIS2-direktiv

11.5.1. Artikel 21(2)(i) – Kräver löpande program för säkerhetsmedvetenhet och utbildning inom cybersäkerhet

11.6. EU:s DORA-förordning

11.6.1. Artikel 13 – Kräver att finansiella entiteter genomför utbildning för all personal med ansvar kopplat till IKT-system

11.7. COBIT 2019

11.7.1. BAI08 – Hantera kunskap: Säkerställer att personal är kompetent och utbildad

11.7.2. DSS05 – Hantera säkerhetstjänster: Betonar säkerhetsmedvetenhet som en central skyddskontroll