					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: P13S					Dokumenttitel: **Policy för informationsklassificering och märkning**							
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**

I linje med standarder och regelverk

Standard/regelverk	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Klausul 5.3, 8	
ISO/IEC 27002:2022	Kontroller 5.12, 5	
NIST SP 800-53 Rev.5	AC-16, MP-3, MP-5	
EU:s NIS2-direktiv	Artikel 21.2 a	
EU:s DORA-förordning	Artikel 5.8	
COBIT 2019	BAI03.05, DSS05	
EU:s GDPR	Artikel 5, 32	

1. Syfte

1.1 Denna policy anger hur all information som hanteras av organisationen ska klassificeras och märkas för att säkerställa att konfidentialitet, riktighet och tillgänglighet upprätthålls under hela informationens livscykel.

1.2 Policyn möjliggör en enhetlig informationshantering genom att tilldela information lämpliga skyddsnivåer utifrån känslighet, verksamhetspåverkan eller rättsliga skyldigheter.

1.3 Klassificering och märkning bidrar till att minska risken för oavsiktligt röjande, obehörig åtkomst eller felaktig hantering av känsliga uppgifter, särskilt i små och medelstora företag som kan vara beroende av enklare system och färre formaliserade kontroller.

1.4 Denna policy är viktig för certifiering enligt ISO/IEC 27001 och för regelefterlevnad, särskilt i förhållande till dataskyddslagstiftning såsom GDPR och cybersäkerhetsramverk såsom NIS2 och DORA.

2. Omfattning

2.1 Denna policy gäller för all organisationsinformation, oavsett format eller lagringsplats, inklusive:

2.1.1 Elektroniska dokument, kalkylblad, e-postmeddelanden, formulär, bilder och skannade filer

2.1.2 Fysiska dokument såsom utskrivna handlingar, rapporter, fakturor och anteckningar

2.1.3 Uppgifter som lagras eller behandlas i molntjänster, på lokala servrar, flyttbara medier eller personliga enheter som används i arbetet

2.1.4 Tillfälliga eller flyktiga uppgifter som genereras under verksamheten, till exempel loggar, cachefiler och e-postmeddelanden

2.2 Samtliga medarbetare, entreprenörer, tillfälligt anställda, externa leverantörer och tredjepartstjänsteleverantörer med åtkomst till organisationens information ska följa denna policy.

2.3 Policyn gäller under hela informationens livscykel – från skapande och lagring, via åtkomst och överföring, till arkivering eller radering.

3. Mål

3.1 Fastställa ett enkelt och tillämpbart klassificeringsschema som lätt kan förstås och användas i hela organisationen.

3.2 Kräva att varje informationstillgång klassificeras utifrån sin känslighet och märks i enlighet därmed för att styra korrekt hantering, lagring och åtkomst.

3.3 Säkerställa att praxis för informationsmärkning integreras i verksamhetsprocesser såsom introduktion, projektstart och systemkonfiguration.

3.4 Minska risken för dataintrång genom att tillämpa hanteringskontroller, till exempel kryptering och åtkomstbegränsning, utifrån klassificeringsnivå.

3.5 Säkerställa efterlevnad av dataskydds- och informationssäkerhetskrav genom att visa att känsliga uppgifter, till exempel personuppgifter, finansiella register eller proprietär information, märks och hanteras korrekt.

3.6 Etablera ansvar för klassificeringsbeslut och säkerställa periodisk granskning och uppdatering utifrån förändrade verksamhetsbehov och rättsliga krav.

4. Roller och ansvar

4.1 Verkställande direktör (VD)

4.1.1 Är policyägare för denna policy och godkänner klassificeringsschemat.

4.1.2 Utövar tillsyn för att säkerställa att ansvar för klassificering delegeras och efterlevs.

4.1.3 Ska granska och godkänna eventuella undantag från kraven på klassificering eller märkning.

4.1.4 Säkerställer att informationshanteringspraxis uppfyller krav på regelefterlevnad enligt lagstiftning såsom GDPR och DORA.

4.2 Informationsägare / dataansvarig

4.2.1 Tilldelar en initial klassificering till varje ny datamängd eller informationstillgång vid skapande eller förvärv.

4.2.2 Säkerställer att synlig märkning, till exempel sidhuvuden, sidfötter, vattenstämplar och mappnamn, används där så är tillämpligt.

4.2.3 Granskar klassificeringar periodiskt för att verifiera relevans, korrekthet och behov av ändringar, till exempel efter nedklassificering eller publicering.

4.2.4 Samarbetar med IT-chef för att genomföra tekniska skyddsåtgärder utifrån klassificering, till exempel behörighetsstyrning och kryptering.

[... 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 Denna policy ska granskas årligen av VD och dataansvarig för att säkerställa att den återspeglar:

9.1.1 Förändringar i verksamheten eller i typer av information

9.1.2 Nya regulatoriska krav, till exempel avseende dataskydd eller finansiell tillsyn

9.1.3 Teknikförändringar som påverkar möjligheterna till märkning eller klassificering

9.2 Granskningen ska omfatta uppdateringar av klassificeringskategorier, märkningsverktyg eller märkningspraxis samt innehåll i informations- och utbildningsinsatser.

9.3 Revideringar av policyn ska godkännas av VD och kommuniceras till samtliga medarbetare. En versionshistorik ska bevaras för revisionsändamål.

10. Relaterade policyer och kopplingar

10.1 P2S – Policy för styrningsroller och ansvar: Fastställer ansvar för policyägarskap och tillämpning.

10.2 P4S – Policy för åtkomstkontroll: Anpassar systemåtkomst till informationens klassificeringsnivåer.

10.3 P12S – Policy för tillgångshantering: Omfattar spårning av fysiska och digitala tillgångar som lagrar klassificerad information.

10.4 P17S – Policy för dataskydd och integritet: Reglerar skydd av personuppgifter, varav en stor del klassificeras som konfidentiell.

10.5 P30S – Policy för incidenthantering: Definierar eskaleringsvägar och hanteringsrutiner vid klassificeringsöverträdelser eller dataexponering.

11. Referensstandarder och ramverk

11.1 ISO/IEC 27001

11.1.1 Klausul 5.3: Kräver tydligt definierat ansvar för informationshantering och skydd.

11.1.2 Klausul 8.1: Kräver operativ planering och kontroller, inklusive sådana som är kopplade till informationsklassificering.

11.2 ISO/IEC 27002

11.2.1 Kontroll 5.12: Ger vägledning om informationsklassificering utifrån risk och regulatoriska krav.

11.2.2 Kontroll 5.13: Beskriver praktiska mekanismer för märkning och tillhörande hanteringsregler.

11.3 NIST SP 800-53 Rev.5

11.3.1 AC-16: Kräver märkning av information för att säkerställa att skyddsåtgärder överensstämmer med klassificeringen.

11.3.2 MP-3 / MP-5: Ger vägledning om märkning och kontroll av medier och utdata.

11.4 EU:s GDPR

11.4.1 Artiklarna 5 och 32: Kräver uppgiftsminimering och riktighet genom lämplig klassificering och lämpliga skyddsåtgärder för hantering.

11.5 EU:s NIS2-direktiv

11.5.1 Artikel 21.2 a: Kräver tekniska och organisatoriska kontroller för riskbaserat skydd av information.

11.6 EU:s DORA-förordning

11.6.1 Artikel 5.8: Kräver att företag klassificerar datatillgångar som en del av sitt ramverk för IKT-riskhantering.

11.7 COBIT 2019

11.7.1 BAI03.05: Kräver informationsklassificering och riskanpassat skydd.

11.7.2 DSS05.02: Avser införande av klassificeringsbaserade kontroller och övervakning.