					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: P13					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**

1. Syfte

1.1 Denna policy fastställer det formella ramverket för klassificering och märkning av organisationens informationstillgångar utifrån känslighet, riskexponering och regulatoriska skyldigheter.

1.2 Den säkerställer att all information – oavsett om den lagras, överförs eller behandlas – tydligt kategoriseras och märks på ett sätt som anger vilken skyddsnivå och vilka hanteringskrav som gäller.

1.3 Policyn säkerställer en strukturerad klassificering i linje med organisationens riskhanteringspraxis och stödjer mål avseende konfidentialitet, riktighet och tillgänglighet för såväl digital som fysisk information.

1.4 Denna kontroll är väsentlig för att möjliggöra rollbaserad åtkomst, revisionsberedskap, lämplig datadelning samt effektiv implementering av tekniska skyddsåtgärder såsom kryptering, säkerhetskopiering och övervakning.

2. Omfattning

2.1 Denna policy gäller för:

2.1.1 Samtliga informationstillgångar i organisationen, inklusive dokument, databaser, register och kommunikation

2.1.2 Alla dataformat, inklusive digitala, tryckta, skriftliga och muntliga

2.1.3 Samtliga miljöer: lokala miljöer, fjärrmiljöer, mobila miljöer och molnmiljöer

2.1.4 Samtliga anställda, entreprenörer, tredjepartstjänsteleverantörer och personuppgiftsbiträden som skapar, hanterar eller lagrar organisationens information

2.2 Omfattningen inkluderar internt utvecklat innehåll, externt inhämtade data, personuppgifter som omfattas av rättsliga skyldigheter enligt dataskyddslagstiftning (t.ex. GDPR) samt information som utbyts med kunder, partner och tillsynsmyndigheter.

2.3 Policyn gäller för alla system som används för att lagra eller överföra data, inklusive verksamhetsapplikationer, filservrar, e-postsystem, molnplattformar och säkerhetskopieringsarkiv.

3. Mål

3.1 Att etablera en standardiserad klassificeringsmodell för hela organisationen baserad på konsekvenserna av exponering eller kompromettering av data.

3.2 Att säkerställa att all information märks synligt och beständigt så att dess klassificeringsnivå och hanteringskrav framgår.

3.3 Att säkerställa datahantering och åtkomstkontroller i enlighet med klassificering, inklusive kryptering, loggning, skydd vid överföring och schemaläggning av bevarande.

3.4 Att stödja efterlevnad av internationella standarder (ISO/IEC 27001, 27002), rättsliga ramverk (GDPR, NIS2, DORA) och interna riskpolicyer.

3.5 Att säkerställa att alla användare förstår sitt ansvar för att skydda data, tillämpa märkning och hantera klassificerad information korrekt.

3.6 Att upprätthålla spårbarhet mellan klassificeringsstatus, tillhörande kontroller och organisationens tillgångsförteckning för revisions- och regelefterlevnadsändamål.

4. Roller och ansvar

4.1 Informationssäkerhetschef (CISO)

4.1.1 Äger policyn för informationsklassificering och märkning och säkerställer att den är anpassad till regulatoriska, avtalsmässiga och operativa krav.

4.1.2 Godkänner klassificeringsnivåer, märkningsstandarder och revideringar av policyn.

4.1.3 Utövar tillsyn över efterlevnaden genom revisioner, mätetal och granskning av undantag.

4.1.4 Samordnar tvärfunktionell styrning med juridik-, dataskydds- och riskfunktionerna.

4.2 Informationsägare

4.2.1 Ansvarar för att klassificera informationstillgångar inom sitt ansvarsområde enligt organisationens klassificeringsmodell.

4.2.2 Ska tillämpa klassificeringsmärkning vid skapande, uppdatering eller mottagande.

4.2.3 Granskar regelbundet klassificeringen av tillgångar, särskilt vid förändringar i känslighet, regulatorisk omfattning eller verksamhetsvärde.

4.2.4 Säkerställer att känsliga data hanteras och märks korrekt under hela livscykeln.

[... 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 minst årligen för att säkerställa anpassning till:

9.1.1 Föränderliga regulatoriska krav (t.ex. GDPR, NIS2, DORA)

9.1.2 Uppdateringar av vägledning om klassificering i ISO/IEC 27001 eller ISO/IEC 27002

9.1.3 Organisatoriska förändringar som påverkar datakänslighet eller ägarskap

9.1.4 Tekniska förändringar, inklusive nya plattformar för dokument- eller datahantering

9.2 Informationssäkerhetschefen (CISO) ska initiera granskningen i samverkan med informationssäkerhetskommittén, juridisk funktion och berörda verksamhetsenheter.

9.3 Granskningar ska omfatta:

9.3.1 Effektiviteten i tillämpningen av klassificering och användarnas efterlevnad

9.3.2 Analys av incidenter eller undantag kopplade till felklassificering

9.3.3 Användaråterkoppling om märkningsverktyg eller vägledningsmaterial

9.3.4 Benchmarking mot branschpraxis för klassificering

9.4 Uppdateringar av policyn ska versionshanteras, dokumenteras i ISMS dokumentregister och kommuniceras till all relevant personal med betoning på nya ansvar eller förändringar i verktyg.

9.5 Nyanställda ska introduceras till den aktuella versionen av policyn i samband med introduktion. Alla anställda ska genomföra repetitionsutbildning efter väsentliga ändringar i policyn.

10. Relaterade policyer och kopplingar

10.1 Denna policy stöds direkt av och upprätthåller kontroller som beskrivs i följande relaterade policyer:

10.1.1 P4 - Åtkomstkontrollpolicy: Åtkomst till information styrs av klassificeringsnivåer; mer känsliga data kräver striktare åtkomstkontroller och behörighetsmekanismer.

10.1.2 P11 - Policy för hantering av användarkonton och privilegier: Förstärker tilldelning av privilegier utifrån need-to-know-principen, som styrs av klassificeringsnivåer.

10.1.3 P12 - Policy för tillgångshantering: Säkerställer att varje tillgång i förteckningen har angiven klassificering och märkning, vilket stödjer spårbarhet och ansvarsskyldighet.

10.1.4 P14 - Policy för bevarande och bortskaffande av data: Regler för bortskaffande och bevarande avgörs av datats klassificeringsnivå och regulatoriska bevarandekrav.

10.1.5 P18 - Policy för kryptografiska kontroller: Tillämpar lämpliga krypteringsstandarder utifrån informationstillgångens klassificering.

10.1.6 P22 - Loggnings- och övervakningspolicy: Möjliggör övervakning av åtkomst till och förflyttning av klassificerad information och säkerställer revisionsbarhet samt detektering av felmärkning eller otillbörlig användning.

10.2 Varje koppling säkerställer ett konsekvent skydd av information genom hela dess livscykel, från skapande och klassificering till säker hantering, lagring, överföring och slutlig förstöring.

11. Referensstandarder och ramverk

11.1 Denna policy är anpassad till internationellt erkända standarder och regulatoriska ramverk för klassificering och märkning av känslig information.

11.2 ISO/IEC 27001

11.2.1 Klausul 4.2 - Förståelse av intressenters behov och förväntningar. Krav på klassificering följer ofta av rättsliga, regulatoriska eller avtalsmässiga skyldigheter som ställs av intressenter (t.ex. GDPR, kunders sekretessavtal (NDA)) och som ska återspeglas i policyn.

11.2.2 Klausul 6.1.3 - Behandling av informationssäkerhetsrisker. Klassificering påverkar direkt valet av riskbehandlingskontroller, inklusive åtkomstkontroll, kryptering och bevarande, utifrån datats känslighet.

11.2.3 Klausul 7.2 - Kompetens. Policyn kräver att personal med ansvar för klassificering och märkning har relevant utbildning, vilket omfattas av kompetenskraven.

11.2.4 Klausul 7.3 - Medvetenhet. Policyn kräver att alla användare känner till klassificeringsnivåerna och sitt ansvar för informationshantering, i linje med kraven på medvetenhet.

11.2.5 Klausul 7.5 - Dokumenterad information. Själva klassificeringspolicyn är ett styrt dokument, och rutiner, utbildningsregister samt klassificeringsmärkning utgör dokumenterad information.

11.2.6 Klausul 8.1 - Operativ planering och styrning. Klassificering och märkning är operativa processer som byggs in i hanteringen av informationens livscykel, och denna klausul säkerställer att sådana aktiviteter planeras, genomförs och styrs.

11.2.7 Klausul 9.1 - Övervakning, mätning, analys och utvärdering. Policyn innehåller bestämmelser om övervakning av efterlevnad, incidenttrender och effektiviteten i märkningsmodellen.

11.2.8 Klausul 10.1 - Avvikelse och korrigerande åtgärd. Policyn definierar åtgärder vid felklassificering, inklusive korrigerande åtgärder såsom omutbildning, uppdateringar och undantagshantering.

11.3 ISO/IEC 27002:2022

11.3.1 Kontroll 5.12 - Klassificering av information. Denna kontroll säkerställer att information klassificeras utifrån känslighet, värde och kritikalitet, vilket är precis vad denna policy formaliserar.

11.3.2 Kontroll 5.13 - Märkning av information. Denna kontroll kräver lämplig märkning av information i enlighet med dess klassificeringsnivå, vilket fullt ut hanteras i denna policy.

11.3.3 Kontroll 5.10 - Godtagbar användning av organisationens tillgångar. Policyn anger hur användare ska hantera klassificerade data, vilket direkt stödjer godtagbar användning och förebygger felaktig användning.

11.3.4 Kontroll 5.11 - Återlämning av tillgångar. Klassificering bidrar till att känsliga data identifieras och återlämnas eller saneras på ett säkert sätt när en anställd eller leverantör lämnar organisationen.

11.3.5 Kontroll 5.9 - Inventering av information och andra tillhörande tillgångar. Klassificering är ofta kopplad till tillgångsförteckningen, som ska återspegla klassificeringsnivån för varje objekt för att stödja korrekt tilldelning av kontroller.

11.3.6 Kontroll 5.14 - Informationsöverföring. Klassificeringsnivåer påverkar kontroller för interna och externa dataöverföringar (t.ex. kryptering, godkännande, åtkomstbegränsningar).

11.3.7 Kontroll 8.12 - Förebyggande av dataläckage. Upprätthållande av klassificering och märkning stödjer förebyggandet av obehörigt röjande och dataförlust.

11.3.8 Kontroll 8.11 - Datamaskering. Vissa klassificeringsnivåer (t.ex. Konfidentiell, Begränsad) kan kräva maskering när data används i test-, utvecklings- eller analysmiljöer.

11.4 NIST SP 800-53 Rev.5

11.4.1 PL-2 - Policy och rutiner för skydd av system och kommunikation: Stödjer klassificeringspolicyer som en del av det övergripande dataskyddet.

11.4.2 AC-16 - Säkerhetsattribut: Implementerar åtkomststyrning baserat på klassificeringsmetadata och användarbehörigheter.

11.4.3 MP-3 / MP-5 - Märkning av medier och skydd vid transport: Säkerställer märkning och skydd av data vid lagring och överföring utifrån klassificering.

11.5 EU:s dataskyddsförordning (GDPR)

11.5.1 Artikel 5 - Principer för behandling av personuppgifter: Kräver att personuppgifter behandlas säkert och proportionerligt i förhållande till deras känslighet.

11.5.2 Artikel 32 - Säkerhet i samband med behandling: Stärker klassificering som en mekanism för riskbaserat dataskydd och lämpliga tekniska åtgärder.

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

11.6.1 Artikel 21(2)(a): Kräver policyer för informationssäkerhetsriskhantering, inklusive kontroller för klassificering av tillgångar och data.

11.6.2 Artikel 21(3): Främjar införande av åtgärder för att säkerställa lämplig datahantering, vilket stöds genom klassificeringsbaserad märkning.

11.7 EU:s DORA-förordning (2022/2554)

11.7.1 Artikel 5 - Styrning och kontroll: Kräver styrningsramverk som klassificerar datatillgångar för kontroll av IKT-risker.

11.7.2 Artikel 9 - IKT-riskhantering: Ställer krav på tekniska och organisatoriska åtgärder för kritiska IKT-tillgångar, inklusive klassificering och märkning.

11.8 COBIT 2019

11.8.1 DSS05.02 - Hantera säkerhetstjänster: Säkerställer klassificering av information för att skydda verksamhetsdata.

11.8.2 MEA03 - Övervaka, utvärdera och bedöma efterlevnad: Stödjer regelbunden revision och granskning av klassificeringspraxis för att säkerställa policyefterlevnad och mognad.