					Indsæt navnet på den registrerede juridiske enhed her						
Dokumentnummer: P13					Dokumenttitel: **Politik for dataklassificering og mærkning**						
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**

1. Formål

1.1 Denne politik fastlægger den formelle ramme for klassificering og mærkning af organisationens informationsaktiver baseret på følsomhed, risikoeksponering og regulatoriske forpligtelser.

1.2 Den sikrer, at alle oplysninger – uanset om de lagres, overføres eller behandles – klassificeres og mærkes entydigt på en måde, der tydeliggør det nødvendige beskyttelses- og håndteringsniveau.

1.3 Politikken fastsætter en struktureret klassificering, der er tilpasset organisationens praksis for risikostyring og understøtter målene for fortrolighed, integritet og tilgængelighed (CIA) på tværs af både digitale og fysiske datatyper.

1.4 Denne kontrol er væsentlig for at understøtte rollebaseret adgang, revisionsberedskab, passende datadeling og effektiv anvendelse af tekniske sikkerhedsforanstaltninger såsom kryptering, sikkerhedskopiering og overvågning.

2. Omfang

2.1 Denne politik gælder for:

2.1.1 Alle organisationens informationsaktiver, herunder dokumenter, databaser, registre og kommunikation

2.1.2 Alle dataformater, herunder digitale, trykte, skriftlige og mundtlige

2.1.3 Alle miljøer: lokale miljøer, fjernarbejdspladser, mobile miljøer og cloudmiljøer

2.1.4 Alle medarbejdere, kontrahenter, tjenesteudbydere og tredjepartsdatabehandlere, som opretter, håndterer eller lagrer organisationens oplysninger

2.2 Omfanget omfatter internt udviklet indhold, eksternt indhentede data, personoplysninger omfattet af databeskyttelsesretlige forpligtelser (f.eks. GDPR) samt oplysninger, der udveksles med kunder, partnere og myndigheder.

2.3 Politikken gælder for alle systemer, der anvendes til at lagre eller overføre data, herunder forretningsapplikationer, filservere, e-mailsystemer, cloudplatforme og backuprepositorier.

3. Mål

3.1 At etablere en standardiseret, organisationsdækkende klassificeringsordning baseret på konsekvenserne af dataeksponering eller kompromittering.

3.2 At sikre, at alle oplysninger mærkes synligt og vedvarende, så deres klassifikationsniveau og håndteringskrav fremgår klart.

3.3 At håndhæve datahåndtering og adgangsstyring i overensstemmelse med klassificeringen, herunder kryptering, logning, beskyttelse under overførsel og planlægning af opbevaringsperioder.

3.4 At understøtte overholdelse af internationale standarder (ISO/IEC 27001, 27002), regulatoriske rammer (GDPR, NIS2, DORA) og interne politikker for risikostyring.

3.5 At sikre, at alle brugere forstår deres ansvar for at beskytte data, anvende mærkninger og håndtere klassificerede oplysninger korrekt.

3.6 At opretholde sporbarhed mellem klassificeringsstatus, tilknyttede kontroller og organisationens aktivfortegnelse til brug for revision og compliance.

4. Roller og ansvar

4.1 Informationssikkerhedschefen (CISO)

4.1.1 Er ansvarlig for politikken for informationsklassificering og mærkning og sikrer, at den er afstemt med regulatoriske, kontraktlige og operationelle krav.

4.1.2 Godkender klassificeringsniveauer, mærkningsstandarder og revisioner af politikken.

4.1.3 Fører tilsyn med efterlevelse af politikken gennem audits, målepunkter og gennemgang af undtagelser.

4.1.4 Koordinerer tværgående styring med juridisk funktion, databeskyttelsesfunktion og risikofunktioner.

4.2 Informationsejere

4.2.1 Er ansvarlige for at klassificere informationsaktiver under deres kontrol ved anvendelse af organisationens klassificeringsordning.

4.2.2 Anvender klassificeringsmærkninger ved oprettelse, opdatering eller modtagelse.

4.2.3 Gennemgår periodisk klassificeringen af aktiver, særligt ved ændringer i følsomhed, regulatorisk omfang eller forretningsværdi.

4.2.4 Sikrer, at følsomme data håndteres og mærkes korrekt gennem hele deres livscyklus.

[... 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 Denne politik skal gennemgås mindst årligt for at sikre overensstemmelse med:

9.1.1 Udvikling i regulatoriske krav (f.eks. GDPR, NIS2, DORA)

9.1.2 Opdateringer til vejledning om klassificering i ISO/IEC 27001 eller 27002

9.1.3 Organisatoriske ændringer, der påvirker datafølsomhed eller ejerskab

9.1.4 Teknologiske ændringer, herunder nye platforme til dokument- eller datahåndtering

9.2 Informationssikkerhedschefen (CISO) skal iværksætte gennemgangen i samarbejde med Informationssikkerhedsudvalget, juridisk funktion og berørte forretningsenheder.

9.3 Gennemgange skal omfatte:

9.3.1 Effektiviteten af håndhævelse af klassificering og brugernes efterlevelse

9.3.2 Analyse af hændelser eller undtagelser knyttet til fejlklassificering

9.3.3 Brugerfeedback om mærkningsværktøjer eller vejledningsmateriale

9.3.4 Benchmarking mod branchestandarder for klassificering

9.4 Opdateringer af politikken skal være underlagt versionsstyring, dokumenteres i ISMS-repositoriet og kommunikeres til alt relevant personale med vægt på nye ansvarsområder eller ændringer i værktøjer.

9.5 Nyansatte skal introduceres til den gældende version af politikken under onboarding. Alle medarbejdere skal gennemføre genopfriskningsuddannelse efter væsentlige ændringer i politikken.

10. Relaterede politikker og sammenhænge

10.1 Denne politik understøttes direkte af og håndhæver kontroller beskrevet i følgende relaterede politikker:

10.1.1 P4 - Politik for adgangskontrol: Adgang til oplysninger styres af klassificeringsniveauer; mere følsomme data kræver strengere adgangsstyring og godkendelsesmekanismer.

10.1.2 P11 - Politik for brugeradministration og privilegeret adgangsstyring: Understøtter tildeling af privilegier baseret på need-to-know-princippet, som informeres af klassificeringsniveauer.

10.1.3 P12 - Politik for aktivstyring: Sikrer, at hvert aktiv i fortegnelsen omfatter dets klassificering og mærkning, hvilket understøtter sporbarhed og ansvarlighed.

10.1.4 P14 - Politik for dataopbevaring og bortskaffelse: Regler for bortskaffelse og opbevaring fastsættes ud fra dataenes klassificeringsniveau og regulatoriske krav til opbevaring.

10.1.5 P18 - Politik for kryptografiske kontroller: Anvender passende krypteringsstandarder på baggrund af klassificeringen af informationsaktivet.

10.1.6 P22 - Politik for logning og overvågning: Muliggør overvågning af adgang til og bevægelse af klassificerede oplysninger og sikrer revisionssporbarhed samt detektion af fejlmærkning eller misbrug.

10.2 Hver sammenhæng sikrer ensartet beskyttelse af oplysninger gennem hele deres livscyklus, fra oprettelse og klassificering til sikker håndtering, lagring, overførsel og endelig destruktion.

11. Referencestandarder og rammeværker

11.1 Denne politik er tilpasset internationalt anerkendte standarder og regulatoriske rammer for klassificering og mærkning af følsomme oplysninger.

11.2 ISO/IEC 27001

11.2.1 Klausul 4.2 - Forståelse af interesserede parters behov og forventninger. Klassificeringskrav udspringer ofte af juridiske, regulatoriske eller kontraktlige forpligtelser pålagt af interessenter (f.eks. GDPR og kunders fortrolighedserklæringer), som skal afspejles i politikken.

11.2.2 Klausul 6.1.3 - Informationssikkerhedsrisikostyring. Klassificering har direkte betydning for udvælgelsen af kontroller til risikobehandling, herunder adgangsstyring, kryptering og opbevaring, baseret på datafølsomhed.

11.2.3 Klausul 7.2 - Kompetence. Politikken kræver, at personale med ansvar for klassificering og mærkning er uddannet, hvilket falder ind under krav til kompetence.

11.2.4 Klausul 7.3 - Bevidsthed. Politikken kræver, at alle brugere er bekendt med klassificeringsniveauer og deres ansvar ved håndtering af oplysninger, i overensstemmelse med krav om bevidstgørelse.

11.2.5 Klausul 7.5 - Dokumenteret information. Selve klassificeringspolitikken er et styret dokument, og procedurer, uddannelsesregistreringer og klassificeringsmærkninger indgår i den dokumenterede information.

11.2.6 Klausul 8.1 - Operationel planlægning og styring. Klassificering og mærkning er operationelle processer indlejret i styring af datalivscyklussen, og denne klausul sikrer, at sådanne aktiviteter planlægges, implementeres og styres.

11.2.7 Klausul 9.1 - Overvågning, måling, analyse og evaluering. Politikken indeholder bestemmelser om overvågning af efterlevelse af klassificering, hændelsestendenser og effektiviteten af mærkningsordningen.

11.2.8 Klausul 10.1 - Afvigelse og korrigerende handling. Politikken definerer reaktioner på fejlklassificering, herunder korrigerende handlinger såsom genoptræning, opdateringer og undtagelseshåndtering.

11.3 ISO/IEC 27002:2022

11.3.1 Kontrol 5.12 - Klassificering af information. Denne kontrol sikrer, at oplysninger klassificeres efter deres følsomhed, værdi og kritikalitet – præcis det, denne politik formaliserer.

11.3.2 Kontrol 5.13 - Mærkning af information. Denne kontrol kræver passende mærkning af oplysninger i overensstemmelse med deres klassificeringsniveau, hvilket fuldt ud er adresseret i denne politik.

11.3.3 Kontrol 5.10 - Acceptabel brug af information og andre tilknyttede aktiver. Politikken håndhæver, hvordan brugere skal håndtere klassificerede data, understøtter direkte acceptabel brug og forebygger misbrug.

11.3.4 Kontrol 5.11 - Returnering af aktiver. Klassificering bidrager til at sikre, at følsomme data identificeres og returneres sikkert eller slettes forsvarligt, når en medarbejder eller leverandør fratræder.

11.3.5 Kontrol 5.9 - Fortegnelse over information og andre tilknyttede aktiver. Klassificering er ofte knyttet til aktivfortegnelsen, som skal afspejle klassificeringsniveauet for hvert element for at understøtte korrekt tildeling af kontroller.

11.3.6 Kontrol 5.14 - Informationsoverførsel. Klassificeringsniveauer påvirker kontroller for intern og ekstern dataoverførsel (f.eks. kryptering, godkendelse og adgangsbegrænsninger).

11.3.7 Kontrol 8.12 - Forebyggelse af datalækage. Håndhævelse af klassificering og mærkning understøtter forebyggelse af uautoriseret videregivelse og datatab.

11.3.8 Kontrol 8.11 - Datamaskering. Visse klassificeringsniveauer (f.eks. Fortrolig, Begrænset) kan kræve maskering, når data anvendes i test- eller udviklingsmiljøer eller analyser.

11.4 NIST SP 800-53 Rev.5

11.4.1 PL-2 - Politik og procedurer for beskyttelse af systemer og kommunikation: Understøtter klassificeringspolitikker som en del af den overordnede databeskyttelse.

11.4.2 AC-16 - Sikkerhedsattributter: Implementerer håndhævelse af adgang baseret på klassificeringsmetadata og brugertilladelser.

11.4.3 MP-3 / MP-5 - Mærkning af medier og transportbeskyttelse: Håndhæver mærkning og beskyttelse af data i hvile og data under overførsel baseret på klassificering.

11.5 EU GDPR (2016/679)

11.5.1 Artikel 5 - Principper for databeskyttelse: Kræver, at personoplysninger behandles sikkert og proportionalt med deres følsomhed.

11.5.2 Artikel 32 - Behandlingssikkerhed: Understreger klassificering som en mekanisme til risikobaseret databeskyttelse og passende tekniske foranstaltninger.

11.6 EU NIS2-direktivet (2022/2555)

11.6.1 Artikel 21(2)(a): Kræver politikker for informationssikkerhedsrisikostyring, herunder kontroller for aktiv- og dataklassificering.

11.6.2 Artikel 21(3): Tilskynder til indførelse af foranstaltninger, der håndhæver passende datahåndtering – understøttet gennem klassificeringsbaseret mærkning.

11.7 EU DORA (2022/2554)

11.7.1 Artikel 5 - Styring og kontrol: Kræver styringsrammer, der klassificerer dataaktiver med henblik på styring af IKT-risiko.

11.7.2 Artikel 9 - Styring af IKT-risiko: Fastlægger tekniske og organisatoriske foranstaltninger for kritiske IKT-aktiver, herunder klassificering og mærkning.

11.8 COBIT 2019

11.8.1 DSS05.02 - Styring af sikkerhedstjenester: Håndhæver informationssikkerhedsklassificeringer for at sikre beskyttelse af virksomhedens data.

11.8.2 MEA03 - Overvåg, evaluer og vurder overholdelse: Understøtter regelmæssig revision og gennemgang af klassificeringspraksis for at sikre overholdelse af politikken og modenhed.