					Indsæt navnet på den registrerede juridiske enhed her							
Dokumentnummer: P13S					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**

Tilpasset relevante standarder og regler

Standard/regulering	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Klausul 5.3, 8	
ISO/IEC 27002:2022	Kontrol 5.12, 5	
NIST SP 800-53 Rev. 5	AC-16, MP-3, MP-5	
EU NIS2	Artikel 21(2)(a)	
EU DORA	Artikel 5(8)	
COBIT 2019	BAI03.05, DSS05	
GDPR	Artikel 5, 32	

1. Formål

1.1 Denne politik fastlægger, hvordan alle oplysninger, der behandles af organisationen, skal klassificeres og mærkes for at sikre, at deres fortrolighed, integritet og tilgængelighed opretholdes gennem hele livscyklussen.

1.2 Politikken understøtter ensartet datahåndtering ved at tildele passende beskyttelsesniveauer til oplysninger ud fra følsomhed, forretningsmæssig påvirkning eller retlige forpligtelser.

1.3 Klassificering og mærkning bidrager til at reducere risikoen for utilsigtet videregivelse, uautoriseret adgang eller fejlhåndtering af følsomme data, særligt i små og mellemstore virksomheder, som kan være afhængige af enklere systemer og færre formaliserede kontroller.

1.4 Denne politik er central for certificering efter ISO/IEC 27001 og for regulatorisk efterlevelse, særligt i forhold til databeskyttelseslovgivning som GDPR og cybersikkerhedsrammer som NIS2 og DORA.

2. Omfang

2.1 Denne politik gælder for alle organisationens data, uanset format eller placering, herunder:

2.1.1 Elektroniske dokumenter, regneark, e-mails, formularer, billeder og scannede filer

2.1.2 Fysiske dokumenter såsom udskrevne registreringer, rapporter, fakturaer og notater

2.1.3 Data, der lagres eller behandles i cloudtjenester, på lokale servere, flytbare medier eller private enheder, der anvendes til forretningsformål

2.1.4 Midlertidige eller forbigående data, der genereres under driften (f.eks. logfiler, cachefiler, e-mails)

2.2 Alle medarbejdere, konsulenter, vikarer og eksterne leverandører med adgang til organisationens data skal efterleve denne politik.

2.3 Politikken gælder gennem hele dataenes livscyklus — fra oprettelse og lagring, over adgang og overførsel, til arkivering eller sletning.

3. Mål

3.1 Etablere en enkel og håndhævelig klassificeringsordning, som let kan forstås og anvendes i hele organisationen.

3.2 Kræve, at hvert dataaktiv klassificeres efter dets følsomhed og mærkes i overensstemmelse hermed for at sikre korrekt håndtering, lagring og adgang.

3.3 Sikre, at praksis for mærkning af data integreres i forretningsprocesser såsom onboarding, projektopstart og systemopsætning.

3.4 Reducere risikoen for brud på persondatasikkerheden ved at anvende passende beskyttelsesforanstaltninger (f.eks. kryptering, adgangsbegrænsning) i henhold til klassificeringsniveauet.

3.5 Sikre efterlevelse af lovgivning om databeskyttelse og informationssikkerhed ved at dokumentere, at følsomme data (f.eks. personoplysninger, finansielle oplysninger eller forretningshemmeligheder) mærkes og forvaltes korrekt.

3.6 Etablere tydeligt ansvar for klassificeringsbeslutninger og sikre periodiske gennemgange og opdateringer baseret på ændrede forretningsmæssige og retlige behov.

4. Roller og ansvar

4.1 Direktør (GM)

4.1.1 Er ejer af denne politik og godkender klassificeringsordningen.

4.1.2 Fører tilsyn med, at ansvar for klassificering delegeres og håndhæves.

4.1.3 Skal gennemgå og godkende eventuelle undtagelser fra krav til klassificering eller mærkning.

4.1.4 Sikrer, at praksis for datahåndtering opfylder gældende krav til efterlevelse efter lovgivning som GDPR og DORA.

4.2 Informationsejer / dataansvarlig

4.2.1 Tildeler en indledende klassificering til hvert nyt datasæt eller informationsaktiv ved oprettelse eller anskaffelse.

4.2.2 Sikrer, at synlige mærkninger (f.eks. filoverskrifter, sidefødder, vandmærker, mappenavne) anvendes, hvor det er relevant.

4.2.3 Gennemgår klassificeringer periodisk for at verificere relevans, nøjagtighed og behov for ændringer (f.eks. ved nedklassificering eller offentliggørelse).

4.2.4 Samarbejder med den it-ansvarlige om at håndhæve tekniske beskyttelsesforanstaltninger baseret på klassificering (f.eks. adgangsrettigheder, kryptering).

[... 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 årligt af direktøren og den dataansvarlige for at sikre, at den afspejler:

9.1.1 Ændringer i forretningsdriften eller datatyper

9.1.2 Nye regulatoriske krav (f.eks. vedrørende databeskyttelse eller finansielt tilsyn)

9.1.3 Teknologiske ændringer, der påvirker mulighederne for mærkning eller klassificering

9.2 Gennemgangen skal omfatte opdateringer af klassificeringskategorier, mærkningsværktøjer eller praksis samt indhold til awareness og træning.

9.3 Revisioner af politikken skal godkendes af direktøren og kommunikeres til alle medarbejdere. En registrering af versionsændringer skal opbevares til revisionsformål.

10. Relaterede politikker og sammenhænge

10.1 P2S – Politik for styringsroller og ansvarsområder: Fastlægger ansvarlighed for ejerskab og håndhævelse af politikker.

10.2 P4S – Politik for adgangskontrol: Afstemmer systemadgang med niveauer for dataklassificering.

10.3 P12S – Politik for aktivstyring: Registrerer de fysiske og digitale aktiver, der lagrer klassificerede data.

10.4 P17S – Databeskyttelses- og privatlivspolitik: Regulerer beskyttelsen af personoplysninger, hvoraf en stor del klassificeres som Fortrolig.

10.5 P30S – Politik for hændelseshåndtering: Fastlægger eskalationsveje og responsprocedurer ved overtrædelser af klassificering eller dataeksponering.

11. Referencestandarder og rammeværker

11.1 ISO/IEC 27001

11.1.1 Klausul 5.3: Kræver klart definerede ansvarsområder for datahåndtering og beskyttelse.

11.1.2 Klausul 8.1: Kræver operationel planlægning og styring, herunder kontroller knyttet til dataklassificering.

11.2 ISO/IEC 27002

11.2.1 Kontrol 5.12: Giver vejledning om informationsklassificering baseret på risiko og regulatoriske krav.

11.2.2 Kontrol 5.13: Beskriver praktiske mekanismer til mærkning og tilhørende håndteringsregler.

11.3 NIST SP 800-53 Rev. 5

11.3.1 AC-16: Kræver mærkning af oplysninger for at sikre, at beskyttelsesforanstaltninger stemmer overens med klassificeringen.

11.3.2 MP-3 / MP-5: Giver vejledning om mærkning og styring af medier og output.

11.4 GDPR

11.4.1 Artikel 5 og 32: Understøtter dataminimering og integritet gennem passende klassificering og sikkerhedsforanstaltninger for håndtering.

11.5 EU NIS2

11.5.1 Artikel 21(2)(a): Kræver tekniske og organisatoriske kontroller for risikobaseret databeskyttelse.

11.6 EU DORA

11.6.1 Artikel 5(8): Kræver, at virksomheder klassificerer dataaktiver som led i deres styring af IKT-risici.

11.7 COBIT 2019

11.7.1 BAI03.05: Kræver informationsklassificering og risikotilpasset beskyttelse.

11.7.2 DSS05.02: Omhandler håndhævelse af klassificeringsbaserede kontroller og overvågning.