					Indsæt navnet på den registrerede juridiske enhed her							
Dokumentnummer: P01S					Dokumenttitel: **Politik for informationssikkerhed**							
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 5.1, 5.2, 5.3, 6.1, 6.2, 8	Angiver ledelsens engagement, krav til politikker, tildeling af roller, risikovurdering og operationel styring
ISO/IEC 27002:2022	Kontrolforanstaltning 5.1–5	Angiver udarbejdelse af dokumenterede politikker for informationssikkerhed, tildeling af roller, funktionsadskillelse og ledelsesansvar
NIST SP 800-53 Rev.5	PM-1, PL-1, CA-1, AC-1	Krav til sikkerhedsprogramplan, planlægningspolitik, vurdering og autorisation samt adgangskontrol
EU GDPR (2016/679)	Artikel 5(2), artikel 32	Ansvarlighedsprincippet og foranstaltninger til behandlingssikkerhed, særligt vedrørende dokumenterede roller
EU NIS2-direktivet (2022/2555)	Artikel 21(2)(a)	Kræver foranstaltninger til risikostyring samt roller og ansvar for cyberrisici
EU DORA (2022/2554)	Artikel 9, artikel 10	Kræver tildeling af roller for styring af IKT-risici og forretningskontinuitet
COBIT 2019	EDM03, APO13, DSS05	Sikrer risikooptimering, sikkerhedsstyring og styring af sikkerhedstjenester gennem tydelig rollefordeling

1. Formål

1.1 Denne politik dokumenterer organisationens forpligtelse til at beskytte kunde- og forretningsoplysninger ved klart at fastlægge ansvar og praktiske sikkerhedsforanstaltninger, tilpasset organisationer uden dedikerede IT-teams.

1.2 Den sikrer, at alle medarbejdere, kontraktansatte og tjenesteudbydere efterlever ensartede regler, så fuld overholdelse af kravene til ISO/IEC 27001-certificering kan opnås.

1.3 Denne politik gør det muligt for organisationen at opbygge kundernes tillid ved tydeligt at dokumentere, hvordan deres oplysninger beskyttes gennem definerede ansvarsområder, strukturerede processer og tydelig ansvarlighed.

2. Omfang

2.1 Denne politik gælder for alle personer, der tilgår eller administrerer organisationens data og systemer, herunder:

2.1.1 Virksomhedsejere og direktører

2.1.2 Medarbejdere, kontraktansatte og praktikanter

2.1.3 Eksterne IT-tjenesteudbydere eller konsulenter

2.2 Den omfatter alle typer information, systemer og tjenester, herunder:

2.2.1 Forretningsdokumenter, kundedata, adgangskoder og e-mails

2.2.2 IT-udstyr såsom bærbare computere og telefoner

2.2.3 Cloudtjenester til fillagring, kommunikation eller økonomi

2.2.4 Fysiske dokumenter opbevaret på kontorlokationer

2.3 Politikken gælder i alle arbejdsmiljøer – på kontoret, ved fjernarbejde og i cloudmiljøer – og omfatter alle enheder og al software, der anvendes til at behandle eller opbevare forretningsoplysninger.

3. Mål

3.1 Tydelig ansvarsplacering: Det skal sikres, at der altid er en ansvarlig for informationssikkerhed. Dette er typisk direktøren eller den person, som direktøren formelt udpeger.

3.2 Beskyttelse af kunde- og forretningsoplysninger: Der skal etableres pålidelige og ensartede sikkerhedsforanstaltninger for at forhindre misbrug, tab eller tyveri af følsomme data, herunder kunde- og regnskabsoplysninger.

3.3 Understøttelse af ISO/IEC 27001-certificering: Organisationen skal kunne dokumentere fuld overholdelse af kravene i ISO/IEC 27001, så den er klar til revision og egnet til certificering uden behov for kompleks infrastruktur.

3.4 Forankring af sikkerhed i driften: Informationssikkerhed skal integreres i daglige opgaver og beslutninger i hele organisationen.

3.5 Opbygning af sikkerhedsbevidsthed og sikkerhedskultur: Alle medarbejdere skal understøttes i at forstå og efterleve sikker praksis, herunder brug af stærke adgangskoder og rapportering af mistænkelig aktivitet.

4. Roller og ansvar

4.1 Direktør eller virksomhedsejer

4.1.1 Har det overordnede ansvar for informationssikkerhed.

4.1.2 Godkender og vedligeholder denne politik.

4.1.3 Sikrer, at alle væsentlige sikkerhedsopgaver enten udføres direkte eller delegeres skriftligt.

4.1.4 Verificerer, at delegerede sikkerhedsopgaver, såsom adgangsstyring eller hændelseshåndtering, udføres effektivt.

4.1.5 Fungerer som primær kontakt for alle interne og eksterne sikkerhedsforhold, herunder revisioner og kundehenvendelser.

4.1.6 Overvåger fremdriften i forhold til disse mål som led i den årlige gennemgang. Mål skal så vidt muligt være målbare (f.eks. andel af medarbejdere, der er trænet, antal rapporterede hændelser mv.) og revideres på baggrund af sikkerhedsmæssige fund og ændringer i risikobilledet.

4.2 Udpeget medarbejder (hvis relevant)

4.2.1 Kan bistå direktøren med daglige opgaver, såsom oprettelse af brugerkonti, fjernelse af adgang for fratrådte medarbejdere eller koordinering med IT-leverandøren.

4.2.2 Skal være formelt udpeget og have tilstrækkelig bemyndigelse og de nødvendige værktøjer til at udføre opgaverne.

4.2.3 Rapporterer eventuelle forhold til direktøren.

[... 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 Årlig gennemgang

9.1.1 Denne politik skal gennemgås af direktøren mindst én gang om året for at sikre fortsat overholdelse af kravene til ISO/IEC 27001-certificering, ændringer i regulatoriske krav (såsom GDPR, NIS2 og DORA) og udviklingen i forretningsmæssige behov.

9.2 Løbende gennemgange

9.2.1 Yderligere gennemgange skal gennemføres, når der sker væsentlige ændringer, såsom:

9.2.1.1 Større sikkerhedshændelser eller brud.

9.2.1.2 Indførelse af nye forretningsprocesser eller teknologier (f.eks. ny software, platforme til fjernarbejde eller cloudtjenester).

9.2.1.3 Ændringer i lovgivningsmæssige eller regulatoriske krav, der påvirker håndteringen af information.

9.3 Dokumentation af ændringer

9.3.1 Alle gennemgange af politikken og alle ændringer skal dokumenteres formelt med tydelig angivelse af dato, revisionernes karakter og direktørens godkendelse.

9.3.2 En historik over politikversioner skal opretholdes sikkert for at dokumentere politikkens udvikling og efterlevelse under revisioner.

9.4 Kommunikation af opdateringer

9.4.1 Enhver ændring af denne politik skal straks kommunikeres til alle medarbejdere, kontraktansatte og relevante tredjeparter.

9.4.2 Opdaterede versioner af politikken skal være let tilgængelige for alle berørte personer (f.eks. delt elektronisk eller opslået fysisk på arbejdspladsen).

10. Relaterede politikker og sammenhænge

10.1 Denne politik hænger tæt sammen med andre politikker i organisationens SME-politiksæt, herunder specifikt:

10.1.1 P2S – Politik for styringsroller og ansvar: Præciserer tildelingen af sikkerhedsopgaver og ansvarsområder.

10.1.2 P4S – Politik for adgangskontrol: Fastlægger sikker håndtering af adgang til organisationens information.

10.1.3 P8S – Politik for informationssikkerhedsbevidsthed og træning: Indeholder grundlæggende retningslinjer for medarbejdertræning og bevidstgørelse.

10.1.4 P17S – Politik for databeskyttelse og privatliv: Sikrer overholdelse af GDPR og anden databeskyttelseslovgivning.

10.1.5 P30S – Politik for hændelseshåndtering: Beskriver de konkrete handlinger, der kræves som reaktion på sikkerhedshændelser.

10.2 Disse relaterede politikker giver tydelig operationel vejledning og skal implementeres samlet for at opnå fuld overholdelse af kravene til ISO/IEC 27001-certificering.

11. Referencestandarder og rammeværk

11.1 ISO/IEC 27001

11.1.1 Klausul 5.1 – Ledelse og engagement: Kræver topledelsens engagement og ansvar for effektiviteten af informationssikkerheden i organisationen.

11.1.2 Klausul 5.2 – Politik for informationssikkerhed: Kræver klare, dokumenterede politikker i overensstemmelse med organisationens strategi og efterlevelseskrav.

11.1.3 Klausul 5.3 – Organisatoriske roller og ansvar: Fastlægger en klar fordeling af ansvar for informationssikkerhed på tværs af organisationen, hvilket er afgørende for effektiv styring og efterlevelse ved revision.

11.1.4 Klausul 6.1 – Handlinger til håndtering af risici og muligheder: Sikrer, at informationssikkerhedsrisici identificeres, vurderes og behandles systematisk.

11.1.5 Klausul 8.1 – Operationel planlægning og styring: Kræver, at organisationen planlægger og implementerer de processer, der er nødvendige for at opfylde målene for informationssikkerhed og styre tilknyttede risici effektivt.

11.2 ISO/IEC 27002:2022 Kontrolforanstaltning 5.1–5

11.2.1 Bilag A kontrolforanstaltning 5.1 – Politikker for informationssikkerhed: Angiver udarbejdelse og kommunikation af dokumenterede politikker for informationssikkerhed.

11.2.2 Bilag A kontrolforanstaltning 5.2 – Roller for informationssikkerhed: Præciserer og tildeler formelt roller og ansvar for informationssikkerhed til relevante parter.

11.2.3 Bilag A kontrolforanstaltning 5.3 – Funktionsadskillelse: Kræver klar funktionsadskillelse for at reducere interessekonflikter og risiko for svig ved håndtering af følsom information.

11.2.4 Bilag A kontrolforanstaltning 5.4 – Ledelsesansvar: Kræver, at ledelsen demonstrerer engagement i informationssikkerhed gennem aktivt tilsyn og allokering af ressourcer.

11.2.5 Understreger nødvendigheden af klart dokumenterede politikker for informationssikkerhed, roller, ansvar og styringsstrukturer, så ensartet styring og sporbarhed ved revision sikres på tværs af organisationen.

11.3 NIST SP 800-53 Rev.5

11.3.1 PM-1 – Plan for informationssikkerhedsprogram: Kræver dokumenterede strategier og politikker for styring af informationssikkerhed, som giver en ramme for ensartet implementering og styring.

11.3.2 PL-1 – Politik for sikkerhedsplanlægning: Kræver en organisationsdækkende politik for sikkerhedsplanlægning til at understøtte sikker drift og strategisk sammenhæng i informationssikkerhedsaktiviteter.

11.3.3 CA-1 – Politik for sikkerhedsvurdering og autorisation: Kræver klart definerede roller for vurdering og autorisation for at sikre vedvarende effektivitet og efterlevelse af kravene til informationssikkerhed.

11.3.4 AC-1 – Politik for adgangskontrol: Kræver, at organisationer klart definerer, dokumenterer og håndhæver praksis og ansvar for adgangsstyring.

11.4 EU GDPR (2016/679)

11.4.1 Artikel 5(2) – Ansvarlighedsprincippet: Kræver, at organisationer kan dokumentere efterlevelse af databeskyttelsesprincipperne, herunder dokumenterede roller og politikker for databeskyttelsesansvar.

11.4.2 Artikel 32 – Behandlingssikkerhed: Kræver implementering af passende tekniske og organisatoriske foranstaltninger, herunder klare sikkerhedsansvar, for at beskytte personoplysninger mod brud og uautoriseret adgang.

11.5 EU NIS2-direktivet (2022/2555)

11.5.1 Artikel 21(2)(a) – Foranstaltninger til risikostyring: Kræver klare styringsordninger, herunder definerede roller og ansvar for informationssikkerhed, som er nødvendige for effektiv styring af cyberrisici.

11.6 EU DORA (2022/2554)

11.6.1 Artikel 9 – Styring af IKT-risiko: Kræver, at organisationer klart tildeler roller og ansvar i relation til styring af IKT-risici for at styrke robusthed og beredskab for forretningskontinuitet.

11.6.2 Artikel 10 – IKT-forretningskontinuitet: Kræver klar ansvarlighed og strukturerede roller for opretholdelse af IKT-robusthed og kontinuitet, så organisationer kan reagere på driftsforstyrrelser på en pålidelig måde.

11.7 COBIT 2019

11.7.1 EDM03 – Sikre risikooptimering: Fremhæver klart defineret ansvarlighed og roller i styringen af organisatoriske risici og giver stærk styring og effektivt tilsyn med informationssikkerhedsrisici.

11.7.2 APO13 – Styr sikkerhed: Kræver, at organisationer klart fastlægger og kommunikerer ansvar for sikkerhedsstyring, så der sikres sammenhæng med forretningsmål og regulatoriske krav.

11.7.3 DSS05 – Styr sikkerhedstjenester: Kræver strukturerede roller og tydelige ansvarsområder ved styring af sikkerhedstjenester, så ensartet implementering og verifikation af efterlevelse muliggøres.