					Indsæt navnet på den registrerede juridiske enhed her						
Dokumentnummer: P01					Dokumenttitel: **Informationssikkerhedspolitik**						
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 organisationens overordnede forpligtelse til informationssikkerhed gennem etablering af et formelt ledelsessystem for informationssikkerhed (ISMS).

1.2 Den angiver den strategiske retning og de grundlæggende krav til beskyttelse af fortrolighed, integritet, tilgængelighed og robusthed for alle informationsaktiver på tværs af fysiske, digitale og cloudmiljøer.

1.3 Politikken opfylder ISO/IEC 27001:2022, klausul 5.1 og 5.2, ved at udtrykke ledelsens hensigt, den øverste ledelses forpligtelse og tilpasning af sikkerhedsaktiviteter til organisationens mål.

1.4 Den udgør den autoritative reference for alle underliggende politikker, standarder og procedurer inden for ISMS og er afgørende for at understøtte et risikobaseret, efterlevelsesdrevet og løbende forbedret sikkerhedsmiljø.

2. Omfang

2.1 Denne politik gælder for alle personer, aktiver og processer, der er omfattet af ISMS'ets omfang, herunder:

2.1.1 Alle forretningsenheder, afdelinger, datterselskaber og filialer

2.1.2 Medarbejdere, kontraktansatte, midlertidigt ansatte, konsulenter og tredjepartsleverandører

2.1.3 Alle data, informationssystemer, applikationer, infrastrukturer og kommunikationskanaler

2.1.4 Alle fysiske, cloudbaserede, eksterne og hybride miljøer, hvor organisationens data behandles eller tilgås

2.2 Politikken er bindende for alle enheder, der håndterer organisationens information, og gælder for alle faser af informationens livscyklus – fra oprettelse og overførsel til lagring og bortskaffelse.

2.3 Enhver undtagelse fra eller begrænsning af dette omfang skal dokumenteres i ISMS'ets omfangsbeskrivelse og begrundes med formel godkendelse fra den øverste ledelse.

3. Mål

3.1 At etablere et ISMS, der er i overensstemmelse med ISO/IEC 27001:2022 og kan understøtte risikobaseret beslutningstagning på tværs af organisationen.

3.2 At sikre, at principperne om fortrolighed, integritet og tilgængelighed er integreret i alle organisatoriske aktiviteter, systemer og samarbejdsrelationer.

3.3 At understøtte regulatorisk og kontraktuel efterlevelse ved at fastlægge målbare, politikdrevne sikkerhedsmål og integrere dem i forretningsdriften.

3.4 At minimere sandsynligheden for og konsekvenserne af informationssikkerhedshændelser gennem effektive forebyggende, detekterende og korrigerende kontroller.

3.5 At fremme løbende forbedring af informationssikkerhedens modenhed gennem fastlagte præstationsindikatorer, revisionsresultater og ledelsens gennemgang.

3.6 At fremme en kultur præget af ansvarlighed, bevidsthed og robusthed, hvor sikkerhedsansvar er forstået og efterlevet af alt personale.

4. Roller og ansvar

4.1 Den øverste ledelse

4.1.1 Godkender informationssikkerhedspolitikken og ISMS-rammen og tilslutter sig disse.

4.1.2 Sikrer sammenhæng mellem sikkerhedsmål og forretningsstrategi.

4.1.3 Går forrest og fremmer en stærk kultur for informationssikkerhed.

4.1.4 Gennemgår og godkender væsentlige ændringer i ISMS'ets omfang, risikohåndtering og styringsstruktur.

4.2 Chief Information Security Officer (CISO) / ISMS-ansvarlig

4.2.1 Har det overordnede ansvar for ISMS'et og vedligeholder denne politik i overensstemmelse med ISO/IEC 27001.

4.2.2 Leder risikovurderinger, implementering af kontroller og processer for løbende forbedring.

4.2.3 Sikrer tværgående koordinering af sikkerhedsindsatsen og fører tilsyn med underliggende politikker.

4.2.4 Rapporterer status for ISMS, hændelser, revisionsresultater og målinger til den øverste ledelse.

4.2.5 Sikrer, at politikken gennemgås og opdateres i overensstemmelse med afsnit 9 i dette dokument.

[... 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 Hyppighed for gennemgang

9.1.1 Denne politik skal gennemgås mindst én gang årligt eller ved en af følgende udløsende hændelser:

9.1.1.1 Væsentlige ændringer i retlige, regulatoriske eller kontraktuelle forpligtelser

9.1.1.2 Væsentlige ændringer i organisationens risikoprofil

9.1.1.3 Resultater fra interne eller eksterne revisioner

9.1.1.4 Større hændelser eller kontrolsvigt

9.2 Ansvar og proces for gennemgang

9.2.1 CISO eller den udpegede ISMS-ansvarlige skal lede gennemgangsprocessen.

9.2.2 Input til gennemgangen skal omfatte:

9.2.2.1 Resultater fra intern revision

9.2.2.2 Tendenser i risikovurderinger

9.2.2.3 Ændringer i forretningsprocesser og teknologi

9.2.2.4 Performance i forhold til KPI'er og risikotærskler

9.2.3 Alle opdateringer skal:

9.2.3.1 Være versionsstyrede og dokumenterede

9.2.3.2 Være godkendt af den øverste ledelse

9.2.3.3 Distribueres til alle berørte parter gennem officielle kommunikationskanaler

9.2.3.4 Udløse nødvendige opdateringer af underliggende dokumentation og uddannelse

10. Relaterede politikker og sammenhænge

10.1 Denne overordnede politik er direkte knyttet til følgende organisatoriske sikkerhedspolitikker og rammer:

10.1.1 P2 – Politik for styringsroller og ansvar: Definerer den styringsstruktur og det autoritetshierarki, der henvises til i dette dokument.

10.1.2 P3 – Politik for acceptabel brug: Fastlægger adfærdsmæssig efterlevelse og korrekt håndtering af informationsaktiver.

10.1.3 P4 – Politik for adgangsstyring: Operationaliserer adgangsrelaterede kontroller afledt af denne overordnede politik.

10.1.4 P6 – Politik for risikostyring: Giver den risikobaserede kontekst for valg af kontroller og accept af restrisici.

10.1.5 P33 – Politik for revision og overvågning af efterlevelse: Beskriver, hvordan interne sikringsmekanismer validerer håndhævelse af politikken.

10.2 Disse indbyrdes afhængigheder sikrer samlet sammenhæng og sporbarhed på tværs af ISMS'et og understøtter ensartet styring af risiko og efterlevelse.

11. Referencestandarder og rammer

11.1 Denne informationssikkerhedspolitik er formelt tilpasset følgende standarder og rammer for at sikre fuld efterlevelse, revisionsberedskab og juridisk forsvarlighed:

11.2 ISO/IEC 27001

11.2.1 Klausul 5.1 – Lederskab og forpligtelse: Denne politik dokumenterer den øverste ledelses forpligtelse til informationssikkerhed og fastlægger ansvar og ressourceallokering for ISMS'et.

11.2.2 Klausul 5.2 – Informationssikkerhedspolitik: Dette dokument udgør organisationens formelle informationssikkerhedspolitik og er tilpasset fastlagte sikkerhedsmål, forretningsstrategi og efterlevelse af ISO/IEC 27001.

11.2.3 Klausul 6.1 – Tiltag til håndtering af risici og muligheder: Den risikobaserede tilgang, der afspejles i denne politik, sikrer, at sikkerhedsressourcer anvendes proportionalt i forhold til trusselsbilledet.

11.2.4 Klausul 9.2 – Intern revision og klausul 10 – Forbedring: Denne politik er integreret i organisationens livscyklus for løbende forbedring og er underlagt validering gennem intern revision.

11.2.5 ISO/IEC 27002:2022 – Kontrol 5.1: Angiver vejledning til etablering og vedligeholdelse af sikkerhedspolitikker. Denne politik afspejler anbefalingerne i ISO/IEC 27002 om hierarkisk dokumentation, gennemgangscyklusser og håndhævelse.

11.3 NIST SP 800-53 Rev.5

11.3.1 PL-1 (Politik og procedurer for sikkerhedsplanlægning): Denne politik opfylder kravet om at udvikle, formidle og gennemgå en formel informationssikkerhedspolitik for hele organisationen.

11.3.2 PM-1 til PM-5: Omfatter styring på programniveau, herunder roller inden for informationssikkerhed, ressourceallokering, risikostrategi og integration af sikkerhedsplanlægning i organisationens drift.

11.4 EU GDPR (2016/679)

11.4.1 Artikel 5(2): Håndhæver princippet om ansvarlighed. Denne politik fastlægger ansvarlige parter og sporbare håndhævelseshandlinger.

11.4.2 Artikel 24: Kræver implementering af tekniske og organisatoriske foranstaltninger, herunder politikker tilpasset risiko.

11.4.3 Artikel 32: Understøtter implementering af passende foranstaltninger til at sikre persondatas sikkerhed gennem hele livscyklussen.

11.5 EU NIS2-direktivet (2022/2555)

11.5.1 Artikel 21(2)(a): Forpligter enheder til at implementere en dokumenteret sikkerhedspolitik, der adresserer risikostyring og styring. Denne politik opfylder dette krav og understøtter et bredere cyberberedskab og beskyttelse af kritisk infrastruktur.

11.6 EU DORA (2022/2554)

11.6.1 Artikel 5(2): Kræver en dokumenteret intern styringsramme for håndtering af IKT-risici. Denne politik understøtter efterlevelse i den finansielle sektor ved at tildele roller, kontroller og tilsynsfunktioner i overensstemmelse med DORA's forventninger til styring.

11.7 COBIT 2019

11.7.1 EDM01 – Etablering af styringsramme: Denne politik understøtter virksomhedsstyring ved at fastlægge ISMS-roller, ledelsesforpligtelser og strategiske mål.

11.7.2 APO01 – Ledelsesramme: Understøtter etablering og drift af et struktureret ISMS.

11.7.3 APO12 – Risikostyring: Danner grundlag for styring af informationssikkerhedsrisici.

11.7.4 MEA01/MEA03 – Overvåg, evaluer og vurder: Understøtter løbende performanceevaluering og overvågning af interne kontroller gennem håndhævelse af politikefterlevelse.