					Indsæt navnet på den registrerede juridiske enhed her							
Dokumentnummer: P33S					Dokumenttitel: **Politik for revision og complianceovervågning**							
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 reguleringer

Standard/regulering	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Klausul 9.2, 10	intern revision, løbende forbedring og afhjælpning af afvigelser
ISO/IEC 27002:2022	Kontrol 5.35, 5.37	planlagte interne gennemgange, uafhængige gennemgange af outsourcede processer
NIST SP 800-53 Rev.5	CA-2, CA-7, AU-6	sikkerhedsvurderinger, løbende overvågning, revisionsgennemgang, -analyse og -rapportering
EU GDPR	Artikel 24 og 32	revision af tekniske og organisatoriske foranstaltninger, dokumentation for kontroludførelse
EU NIS2	Artikel 21(2)(f)	proaktiv gennemgang og dokumenterbar efterlevelse
EU DORA	Artikel 10	styring af IKT-risiko, overvågning og rapportering
COBIT 2019	MEA01, MEA03	overvågning og vurdering af overensstemmelse, efterlevelse og beredskab til tredjepartsgennemgang

1. Formål

1.1 Denne politik fastlægger organisationens tilgang til gennemførelse af intern revision, kontrol af sikkerhedskontroller og overvågning af efterlevelse af regulatoriske krav. Den sikrer, at alle kontroller, politikker, systemer og tredjepartsleverandører er omfattet af regelmæssig og struktureret gennemgang.

1.2 Formålet er at identificere kontrolsvigt, forebygge manglende efterlevelse og dokumentere rettidig omhu i overensstemmelse med ISO/IEC 27001, GDPR og relaterede rammeværker.

1.3 Den gør det muligt for SMV'er at opretholde operationel styring og revisionsberedskab til certificering, også uden en særskilt compliancefunktion, ved hjælp af enkle, gentagelige tjeklister og risikoprioriterede revisionskonstateringer.

2. Omfang

2.1 Denne politik gælder for:

2.1.1 Alle interne afdelinger og eksterne tjenesteudbydere med ansvar relateret til it-systemer, personoplysninger og forretningskritiske tjenester

2.1.2 Alle kontroller og systemer inden for omfanget af ledelsessystemet for informationssikkerhed (ISMS)

2.1.3 Al intern revision, gennemgang af sikkerhedskontroller og efterlevelseskontrol, uanset om den udføres internt eller af en ekstern konsulent, kunde eller myndighed

2.2 Denne politik gælder også for indsamling af bevismateriale og rapportering til brug for:

2.2.1 certificerings- og recertificeringsaudits efter ISO/IEC 27001

2.2.2 databeskyttelsesrevisioner efter GDPR eller kontraktlige vilkår

2.2.3 kundedrevne sikkerhedsspørgeskemaer eller due diligence-gennemgange

2.2.4 enhver regulatorisk eller uafhængig gennemgang efter NIS2 eller DORA, hvor relevant

3. Mål

3.1 Sikre, at alle nøglekontroller og politikker regelmæssigt gennemgås med henblik på effektivitet og efterlevelse.

3.2 Opretholde revisionsspor og registreringer af korrigerende handlinger for at dokumentere ansvarlighed og forbedring.

3.3 Understøtte certificering, recertificering og kundekrav til dokumentation (f.eks. ISO 27001, leverandør-onboarding).

3.4 Identificere mangler tidligt, så afhjælpning kan iværksættes hurtigt, før forhold eskalerer eller medfører brud på forpligtelser.

3.5 Sætte direktøren og den eksterne it-leverandør i stand til at koordinere gennemgange med minimal kompleksitet og samtidig sikre juridisk holdbare resultater.

4. Roller og ansvar

4.1 Direktør (GM)

4.1.1 Har det overordnede ansvar for revisionsprogrammet

4.1.2 Godkender interne gennemgangsplaner og revisionskonstateringer

4.1.3 Tildeler og følger op på korrigerende handlinger

4.1.4 Godkender anvendelse af eksterne auditorer eller konsulenter

4.2 It-leverandør / it-administrator

4.2.1 Fremlægger bevismateriale under intern revision og eksterne audits (f.eks. logfiler, konfigurationer, registreringer for adgangsstyring)

4.2.2 Bistår ved tekniske kontroller (f.eks. backupstatus, patch-compliance)

4.2.3 Vedligeholder repository for revisionsbevismateriale

[... 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 af politik og revisionsplan

9.1.1 Direktør (GM) skal gennemgå denne politik og revisionsplanen mindst én gang om året.

9.1.2 Gennemgangen skal evaluere:

9.1.2.1 revisionernes effektivitet i forhold til at identificere mangler

9.1.2.2 gennemførelsesgraden for revisioner og korrigerende handlinger

9.1.2.3 ændringer i gældende juridiske, regulatoriske eller certificeringsmæssige krav

9.2 Udløsende opdateringer

9.2.1 Politikken skal gennemgås og opdateres, når:

9.2.2 en certificerings- eller overvågningsaudit resulterer i en væsentlig afvigelse

9.2.3 juridiske eller regulatoriske rammer ændres (f.eks. ny GDPR-vejledning, national implementering af NIS2)

9.2.4 forretningsændringer påvirker systemer, processer eller leverandører, der er omfattet af revisionsomfanget

9.2.5 en kritisk hændelse eller et brud afdækker tidligere uidentificerede kontrolmangler

9.3 Dokumentation af opdateringer

9.3.1 Alle ændringer i politikken skal spores i en versionslog

9.3.2 Opdateringer skal distribueres til alle teammedlemmer, der er involveret i revisioner

9.3.3 Et sammendrag af ændringer skal vedlægges den opdaterede politik for at sikre forståelse

10. Relaterede politikker og sammenhænge

10.1 Denne politik understøttes af og supplerer flere andre SME-politikker:

10.1.1 P1S – Informationssikkerhedspolitik: Fastlægger grundlaget for alle kontrolforventninger og kræver håndhævelse gennem revisioner.

10.1.2 P2S – Politik for styringsroller og ansvarsområder: Fastlægger ansvarlighed for revisionsplanlægning, gennemførelse og ejerskab af korrigerende handlinger.

10.1.3 P6S – Politik for risikostyring: Identificerer svagheder i kontroller afdækket ved revisioner og sikrer, at revisionskonstateringer dokumenteres i risikoregistret.

10.1.4 P17S – Databeskyttelses- og privatlivspolitik: Definerer de GDPR-kontroller, der skal revideres, herunder datahåndtering, respons ved brud på persondatasikkerheden og privatlivsmeddelelser.

10.1.5 P22S – Lognings- og overvågningspolitik: Leverer de revisionslogfiler og forensiske data, der anvendes under efterlevelses- og kontrolgennemgange.

10.1.6 P30S – Politik for hændelseshåndtering: Kræver periodisk revision af hændelsesregistre og gennemgange efter hændelser for at verificere effektiviteten af responsen.

10.1.7 P31S – Politik for indsamling af bevismateriale og it-forensik: Indeholder procedurer for indsamling af verificerbart bevismateriale med dokumenteret chain of custody under revisioner.

10.2 Samlet skaber disse politikker et lukket kontrolmiljø, der muliggør intern verifikation, ekstern dokumentation og styring i overensstemmelse med relevante standarder.

11. Referencestandarder og rammeværker

11.1 ISO/IEC 27001:

11.1.1 Klausul 9.2 – Kræver intern revision for at evaluere ISMS'ets performance og overensstemmelse med kravene.

11.1.2 Klausul 10.1 – Kræver løbende forbedring baseret på revisionsresultater og afhjælpning af afvigelser.

11.2 ISO/IEC 27002:

11.2.1 Kontrol 5.35 – Kræver planlagte interne gennemgange af kontroller og processer.

11.2.2 Kontrol 5.37 – Fremhæver uafhængige gennemgange, særligt for outsourcede processer.

11.3 NIST SP 800-53 Rev.5:

11.3.1 CA-2 – Sikkerhedsvurderinger: Kræver revision af implementerede kontroller for at verificere effektiviteten.

11.3.2 CA-7 – Løbende overvågning: Fremhæver proaktiv identifikation og gennemgang af svagheder i kontroller.

11.3.3 AU-6 – Revisionsgennemgang, analyse og rapportering: Kræver regelmæssig analyse og håndtering af revisionslogfiler og revisionskonstateringer.

11.4 EU GDPR:

11.4.1 Artikel 24 og 32 – Kræver implementering og revision af tekniske og organisatoriske foranstaltninger, herunder dokumentation for kontroludførelse og forbedring over tid.

11.5 EU NIS2-direktivet (2022/2555):

11.5.1 Artikel 20–21 – Kræver proaktiv kontrolgennemgang, dokumenterbar efterlevelse og revisionssporbarhed for væsentlige og vigtige enheder.

11.6 COBIT 2019:

11.6.1 MEA01 – Overvåg, evaluer og vurder performance og overensstemmelse: Kræver periodisk vurdering af processers og kontrollers performance i forhold til standarder og mål.

11.6.2 MEA03 – Sikr overholdelse af eksterne krav: Fokuserer på intern overvågning og beredskab til tredjepartsrevisioner og regulatoriske gennemgange.