					Indsæt navnet på den registrerede juridiske enhed her							
Dokumentnummer: P33					Dokumenttitel: **Politik for revision og overvågning af efterlevelse**							
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 9.2, 9.3, 10	
ISO/IEC 27002:2022	Kontrol 5.35–5.37	
NIST SP 800-53 Rev.5	CA-2, CA-5, CA-7	
EU GDPR	Artikel 24, 32, 33	
EU NIS2	Artikel 21(2)(g), 27	
EU DORA	Artikel 10(2)(e), 25	
COBIT 2019	MEA01, MEA03	

1. Formål

1.1 Formålet med denne politik er at etablere og styre organisationens program for revision, compliance og overvågning af efterlevelse med henblik på at:

1.1.1 Validere effektiviteten af sikkerheds- og databeskyttelseskontroller

1.1.2 Sikre overensstemmelse med gældende standarder, lovgivningsmæssige rammer og kontraktlige forpligtelser

1.1.3 Identificere afvigelser, ineffektivitet og efterlevelsesrisici rettidigt

1.1.4 Understøtte løbende forbedring og beredskab til certificeringer, vurderinger og myndighedsmæssige gennemgange

1.2 Denne politik understøtter integriteten og modenheden i ledelsessystemet for informationssikkerhed (ISMS) ved at indarbejde strukturerede, risikobaserede og evidensbaserede praksisser for revision og overvågning.

2. Omfang

2.1 Denne politik gælder for alle:

2.1.1 Interne forretningsenheder, funktioner og afdelinger

2.1.2 Fysiske faciliteter, cloudmiljøer, SaaS-platforme og outsourcede tjenester

2.1.3 Informationssystemer, applikationer, infrastruktur og dataaktiver, der er omfattet af ISMS

2.1.4 Medarbejdere, kontraktansatte og tredjepartsleverandører med revisions- eller efterlevelsesforpligtelser

2.2 Politikken omfatter:

2.2.1 Intern revision

2.2.2 Eksterne revisioner/certificeringsrevisioner

2.2.3 Teknisk overvågning af efterlevelse

2.2.4 Leverandør- og tredjepartsrevisioner

2.2.5 Korrigerende og forebyggende handlinger (CAPA)

2.2.6 Målepunkter, dashboards og rapporteringsprocesser

2.3 Den gælder for alle relevante rammeværker, som organisationen er underlagt, herunder ISO/IEC 27001, GDPR, NIS2, DORA og SOC 2.

3. Mål

3.1 Verificere tilstrækkeligheden og effektiviteten af implementerede kontroller, politikker og procedurer på tværs af ISMS og relaterede miljøer.

3.2 Identificere og afhjælpe eventuelle mangler, afvigelser eller efterlevelsesgab, før de udvikler sig til hændelser eller overtrædelser.

3.3 Sikre vedvarende beredskab til interne ledelsesgennemgange, eksterne revisioner og uafhængige certificeringer.

3.4 Generere juridisk forsvarlig dokumentation og revisionsspor til brug ved myndighedsmæssige forespørgsler, retlige processer eller anmodninger fra kunder eller partnere om dokumentation.

3.5 Integrere revisionsresultater i organisationens overordnede risikostyring, sikkerhedsmålinger og aktiviteter for løbende forbedring.

4. Roller og ansvar

4.1 Intern revisionsansvarlig / compliance-ansvarlig

4.1.1 Planlægger, skemalægger og gennemfører intern revision baseret på risikoprioritering.

4.1.2 Vedligeholder revisionsregisteret, koordinerer revisionsaktiviteter og følger op på korrigerende handlinger.

4.2 Chief Information Security Officer (CISO)

4.2.1 Sikrer, at revisionsomfanget dækker alle relevante ISMS-elementer og kontroller i bilag A.

4.2.2 Fører tilsyn med verifikation af CAPA og integrerer revisionsresultater i sikkerhedsprogrammet.

[... 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 af den compliance-ansvarlige og CISO, eller tidligere som reaktion på:

9.1.1 Ændringer i regulatoriske, kontraktlige eller certificeringsmæssige rammer

9.1.2 Væsentlige revisionskonstateringer eller gentagne kontrolsvigt

9.1.3 Organisatorisk omstrukturering eller ændringer i GRC-systemet

9.1.4 Anbefalinger fra eksterne revisorer eller tilbagemeldinger fra tilsynsmyndigheder

9.2 Gennemgangsprocessen skal vurdere:

9.2.1 Metodik og frekvens for revisionsplanlægning

9.2.2 Ændringer i ISMS-omfang eller infrastruktur

9.2.3 Opdateringer af kontrolkataloget eller det juridiske register

9.2.4 Konsistens og kvalitet i revisionsbevismateriale og CAPA-processer

9.3 Alle ændringer i politikken skal:

9.3.1 Dokumenteres i et versionsstyret repository

9.3.2 Godkendes af direktionen

9.3.3 Kommunikeres til alle berørte medarbejdere og integreres i opdaterede procedurer og programmer for sikkerhedsbevidsthed

9.4 Validering efter gennemgang skal bekræfte, at opdaterede krav er afspejlet i revisionsregisteret, efterlevelsesværktøjer og interne overvågningsdashboards.

10. Relaterede politikker og sammenhænge

10.1 Denne politik er afstemt med følgende relaterede organisatoriske politikker:

10.1.1 P1 – Informationssikkerhedspolitik: Definerer ISMS og fastlægger ansvarlighed for efterlevelse og løbende forbedring

10.1.2 P5 – Politik for ændringsstyring: Sikrer revisionsmæssig sporbarhed i ændringer i infrastruktur og konfiguration, der påvirker kontrolmiljøer

10.1.3 P6 – Politik for risikostyring: Integrerer revisionsresultater i organisationens risikovurdering og aktiviteter for risikobehandling

10.1.4 P14 – Dataopbevarings- og bortskaffelsespolitik: Regulerer opbevaring af revisionsbevismateriale, logfiler og efterlevelsesregistreringer

10.1.5 P18 – Politik for kryptografiske kontroller: Understøtter sikker opbevaring og overførsel af følsomme revisionsdata

10.1.6 P26 – Politik for tredjeparts- og leverandørsikkerhed: Omfatter revisionsrettigheder, sikkerhedsdokumentation og tilsyn med leverandørers efterlevelse

10.1.7 P30 – Politik for hændelseshåndtering: Afstemmer revision af hændelseshåndteringsprocesser med ISMS-mål for sikkerhed og dokumentation

10.1.8 P32 – Politik for forretningskontinuitet og katastrofeberedskab: Kræver verifikation af test af forretningskontinuitet og efterlevelse af DRP under revisionscyklusser

11. Referencestandarder og rammeværker

11.1 Denne politik er tilpasset globale standarder og lovkrav vedrørende revision og løbende validering af efterlevelse.

11.2 ISO/IEC 27001:

11.2.1 Klausul 9.2 – intern revision: Kræver regelmæssige, risikobaserede revisioner af ISMS for at evaluere effektivitet og overensstemmelse.

11.2.2 Klausul 9.3 – ledelsens gennemgang: Revisionsresultater skal indgå i strategisk gennemgang og forbedring.

11.2.3 Klausul 10.1 – afvigelse og korrigerende handling: Revisionskonstateringer skal håndteres gennem dokumenterede CAPA-procedurer.

11.3 ISO/IEC 27002:2022 – Kontrol 5.35–5.37:

11.3.1 Kontroller i bilag A 5.35–5.37: Omfatter uafhængig gennemgang, efterlevelse af juridiske og kontraktlige krav samt revisionslogning.

11.3.2 Giver implementeringsvejledning til planlægning, gennemførelse og forbedring af revisions- og efterlevelsesprogrammer.

11.4 NIST SP 800-53 Rev.5:

11.4.1 CA-2 – Kontrolvurderinger: Kræver rutinemæssig gennemgang af implementerede sikkerhedskontroller.

11.4.2 CA-5 – Plan of Action and Milestones (POA&M): Er afstemt med sporing og afhjælpning af revisionskonstateringer.

11.4.3 CA-7 – Løbende overvågning: Understøtter proaktive, automatiserede vurderinger af efterlevelse.

11.5 EU GDPR (2016/679):

11.5.1 Artikel 24 og 32: Kræver dokumentation for implementering og effektivitet af sikkerhedskontroller gennem passende styringsstrukturer.

11.5.2 Artikel 33: Understøtter behovet for verificerede revisionsspor ved håndtering af brud på persondatasikkerheden og underretning.

11.6 EU NIS2-direktivet (2022/2555):

11.6.1 Artikel 21(2)(g): Kræver revision af politikker og procedurer som en del af de minimumsforanstaltninger, der gælder for styring af cybersikkerhedsrisici.

11.6.2 Artikel 27: Nationale myndigheder kan gennemføre eller kræve revisioner for væsentlige og vigtige enheder.

11.7 EU DORA (2022/2554):

11.7.1 Artikel 10(2)(e): Enheder skal gennemføre interne og eksterne revisioner af praksisser for styring af IKT-risici.

11.7.2 Artikel 25 – Revisionskrav: Kræver periodiske revisioner udført af interne eller uafhængige eksterne revisorer med regulatorisk indsigt.

11.8 COBIT 2019:

11.8.1 MEA01 – Overvågning, evaluering og vurdering af performance og overensstemmelse: Sikrer, at kontrollers effektivitet verificeres og rapporteres til styrende organer.

11.8.2 MEA03 – Overvågning, evaluering og vurdering af efterlevelse: Kræver, at organisatoriske praksisser er afstemt med juridiske, kontraktlige og standardbaserede krav.