					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: P33					Dokumenttitel: **Policy för revision och övervakning av regelefterlevnad**							
Version: 1.0		Ikraftträdandedatum: 01.01.2025			Dokumentägare:							
X	Policy		Standard		Rutin		Formulär		Register		Övrigt	

Revisionshistorik				
Revisionsnummer	**Revisionsdatum**	**Ändringar**	**Granskad av**	**Processägare**

Godkännanden			
Namn	**Titel**	**Datum**	**Underskrift**

Anpassad till standarder och regelverk

Standard/regelverk	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Klausuler 9.2, 9.3, 10	
ISO/IEC 27002:2022	Kontroller 5.35–5.37	
NIST SP 800-53 Rev.5	CA-2, CA-5, CA-7	
EU:s GDPR	Artiklar 24, 32, 33	
EU:s NIS2-direktiv	Artikel 21(2)(g), 27	
EU:s DORA-förordning	Artiklar 10(2)(e), 25	
COBIT 2019	MEA01, MEA03	

1. Syfte

1.1 Syftet med denna policy är att fastställa och styra organisationens program för revision och övervakning av regelefterlevnad för att:

1.1.1 Verifiera effektiviteten i säkerhets- och dataskyddskontroller

1.1.2 Säkerställa överensstämmelse med tillämpliga standarder, rättsliga ramverk och avtalskrav

1.1.3 I rätt tid identifiera avvikelser, brister och risker kopplade till regelefterlevnad

1.1.4 Stödja ständiga förbättringar och beredskap för certifieringar, granskningar och tillsyn

1.2 Denna policy stärker informationssäkerhetsledningssystemets (ISMS) riktighet och mognad genom att införa strukturerade, riskbaserade och evidensbaserade metoder för revision och övervakning.

2. Omfattning

2.1 Denna policy gäller för alla:

2.1.1 Interna verksamhetsenheter, funktioner och avdelningar

2.1.2 Fysiska anläggningar, molnmiljöer, SaaS-plattformar och outsourcade tjänster

2.1.3 Informationssystem, applikationer, infrastruktur och datatillgångar som omfattas av ISMS

2.1.4 Anställda, konsulter och tredjepartsleverantörer med revisionsrelaterade eller regelefterlevnadsrelaterade skyldigheter

2.2 Policyn omfattar:

2.2.1 Internrevisioner

2.2.2 Externa revisioner/certifieringsrevisioner

2.2.3 Teknisk övervakning av regelefterlevnad

2.2.4 Leverantörs- och tredjepartsrevisioner

2.2.5 Korrigerande och förebyggande åtgärder (CAPA)

2.2.6 Nyckeltal, instrumentpaneler och rapporteringsprocesser

2.3 Den gäller för alla relevanta ramverk som organisationen omfattas av, inklusive ISO/IEC 27001, GDPR, NIS2, DORA och SOC 2.

3. Mål

3.1 Att verifiera ändamålsenligheten och effektiviteten i införda kontroller, policyer och rutiner inom hela ISMS och relaterade miljöer.

3.2 Att identifiera och åtgärda kontrollbrister, avvikelser eller efterlevnadsgap innan de eskalerar till incidenter eller överträdelser.

3.3 Att säkerställa varaktig beredskap för interna styrningsgranskningar, externa revisioner och oberoende certifieringar.

3.4 Att ta fram försvarbart bevismaterial och revisionsspår till stöd för regulatoriska förfrågningar, rättsprocesser eller förfrågningar om säkerhetsförsäkran från kunder eller partner.

3.5 Att integrera revisionsresultat i organisationens övergripande riskhantering, säkerhetsmätetal och arbete med ständiga förbättringar.

4. Roller och ansvar

4.1 Internrevisionsansvarig / regelefterlevnadschef

4.1.1 Planerar, schemalägger och genomför internrevisioner utifrån riskprioritering.

4.1.2 Underhåller revisionsregistret, samordnar revisionsaktiviteter och följer upp korrigerande åtgärder.

4.2 Informationssäkerhetschef (CISO)

4.2.1 Säkerställer att revisionsomfattningen täcker alla relevanta delar av ISMS och kontroller i bilaga A.

4.2.2 Utövar tillsyn över verifiering av CAPA och integrerar revisionsresultat i informationssäkerhetsprogrammet.

[... Avsnitt 4.3–8 ingår inte i denna förhandsvisning. Köp det fullständiga dokumentet för att få tillgång till hela innehållet. ...]

9. Krav för granskning och uppdatering

9.1 Denna policy ska granskas minst årligen av regelefterlevnadschefen och informationssäkerhetschefen (CISO), eller tidigare som svar på:

9.1.1 Förändringar i regulatoriska ramverk, avtalsramverk eller certifieringsramverk

9.1.2 Betydande revisionsiakttagelser eller upprepade kontrollbrister

9.1.3 Omstrukturering i organisationen eller ändringar i GRC-systemet

9.1.4 Rekommendationer från externa revisorer eller återkoppling från tillsynsmyndighet

9.2 Granskningsprocessen ska bedöma:

9.2.1 Metodik och frekvens för revisionsplanering

9.2.2 Förändringar i ISMS-omfattning eller infrastruktur

9.2.3 Uppdateringar av kontrollkatalogen eller det rättsliga registret

9.2.4 Konsekvens och kvalitet i revisionsbevis samt CAPA-processer

9.3 Alla policyändringar ska:

9.3.1 Dokumenteras i ett versionshanterat register

9.3.2 Godkännas av verkställande ledning

9.3.3 Kommuniceras till all berörd personal och integreras i uppdaterade rutiner och medvetandeprogram

9.4 Validering efter granskning ska bekräfta att uppdaterade krav återspeglas i revisionsregistret, verktyg för regelefterlevnad och interna övervakningspaneler.

10. Relaterade policyer och kopplingar

10.1 Denna policy är anpassad till följande relaterade organisationspolicyer:

10.1.1 P1 – Informationssäkerhetspolicy: Definierar ISMS och fastställer ansvarsskyldighet för regelefterlevnad och ständiga förbättringar

10.1.2 P5 – Policy för ändringshantering: Säkerställer revisionsinsyn i ändringar av infrastruktur och konfiguration som påverkar kontrollmiljöer

10.1.3 P6 – Riskhanteringspolicy: Integrerar revisionsutfall i organisationens riskutvärdering och aktiviteter för riskbehandling

10.1.4 P14 – Policy för databevarande och bortskaffande: Styr bevarande av revisionsbevis, loggar och uppgifter om regelefterlevnad

10.1.5 P18 – Policy för kryptografiska kontroller: Stödjer säker lagring och överföring av känsliga revisionsdata

10.1.6 P26 – Policy för leverantörssäkerhet och tredjepartssäkerhet: Omfattar revisionsrätt, dokumentation för säkerhetsförsäkran och tillsyn över leverantörers efterlevnad

10.1.7 P30 – Policy för incidenthantering: Anpassar revisioner av incidenthanteringsprocesser till ISMS-mål för säkerhetsförsäkran

10.1.8 P32 – Policy för verksamhetskontinuitet och katastrofåterställning: Kräver verifiering av kontinuitetstester och efterlevnad av DRP under revisionscykler

11. Referensstandarder och ramverk

11.1 Denna policy är anpassad till globala standarder och rättsliga krav för revision och kontinuerlig validering av regelefterlevnad.

11.2 ISO/IEC 27001:

11.2.1 Klausul 9.2 – Internrevision: Kräver regelbundna, riskbaserade revisioner av ISMS för att utvärdera effektivitet och överensstämmelse.

11.2.2 Klausul 9.3 – Ledningens genomgång: Revisionsutfall ska ligga till grund för strategisk granskning och förbättring.

11.2.3 Klausul 10.1 – Avvikelse och korrigerande åtgärd: Revisionsiakttagelser ska hanteras genom dokumenterade CAPA-rutiner.

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

11.3.1 Kontroller i bilaga A 5.35–5.37: Omfattar oberoende granskning, efterlevnad av rättsliga krav och avtalskrav samt revisionsloggning.

11.3.2 Ger vägledning för genomförande vid planering, utförande och förbättring av program för revision och övervakning av regelefterlevnad.

11.4 NIST SP 800-53 Rev.5:

11.4.1 CA-2 – Kontrollbedömningar: Kräver rutinmässig granskning av införda säkerhetskontroller.

11.4.2 CA-5 – Åtgärdsplan och milstolpar (POA&M): Harmoniserar med uppföljning och åtgärdande av revisionsiakttagelser.

11.4.3 CA-7 – Kontinuerlig övervakning: Stödjer proaktiva, automatiserade bedömningar av regelefterlevnad.

11.5 EU:s GDPR (2016/679):

11.5.1 Artiklarna 24 och 32: Kräver bevis på att säkerhetskontroller har införts och är effektiva genom lämpliga styrningsstrukturer.

11.5.2 Artikel 33: Stödjer behovet av verifierade revisionsspår vid hantering och anmälan av personuppgiftsincidenter.

11.6 EU:s NIS2-direktiv (2022/2555):

11.6.1 Artikel 21(2)(g): Kräver revision av policyer och rutiner som en del av minimiåtgärder för cybersäkerhetsriskhantering.

11.6.2 Artikel 27: Nationella myndigheter kan utföra eller kräva revisioner för väsentliga och viktiga entiteter.

11.7 EU:s DORA-förordning (2022/2554):

11.7.1 Artikel 10(2)(e): Entiteter ska utföra interna och externa revisioner av praxis för IKT-riskhantering.

11.7.2 Artikel 25 – Revisionskrav: Kräver periodiska revisioner av interna eller oberoende externa revisorer med regulatorisk insyn.

11.8 COBIT 2019:

11.8.1 MEA01 – Mätning, utvärdering och analys av prestanda och överensstämmelse: Säkerställer att kontrolleffektivitet verifieras och rapporteras till styrande organ.

11.8.2 MEA03 – Mätning, utvärdering och analys av regelefterlevnad: Kräver att organisationens praxis är anpassad till rättsliga, avtalsmässiga och standardbaserade krav.