					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: P33S					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**

Ansluten till standarder och regelverk

Standard/regelverk	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Klausul 9.2, 10	Internrevision, kontinuerlig förbättring och hantering av avvikelser
ISO/IEC 27002:2022	Kontroller 5.35, 5.37	Planerade interna granskningar, oberoende granskningar av outsourcade processer
NIST SP 800-53 Rev.5	CA-2, CA-7, AU-6	Säkerhetsbedömningar, kontinuerlig övervakning, granskning, analys och rapportering av revisionsdata
EU:s GDPR	Artiklarna 24 och 32	Granskning av tekniska och organisatoriska åtgärder samt bevis för kontrollernas effektivitet
EU:s NIS2-direktiv	Artikel 21(2)(f)	Proaktiv granskning och evidensbaserad regelefterlevnad
EU:s DORA-förordning	Artikel 10	IKT-riskhantering, övervakning och rapportering
COBIT 2019	MEA01, MEA03	Övervakning och bedömning av efterlevnad, regelefterlevnad och beredskap för tredjepartsgranskningar

1. Syfte

1.1 Denna policy fastställer organisationens arbetssätt för att genomföra internrevisioner, granskning av säkerhetsåtgärder och övervakning av regelefterlevnad. Den säkerställer att samtliga kontroller, policyer, system och tjänsteleverantörer omfattas av regelbunden och strukturerad granskning.

1.2 Syftet är att identifiera kontrollbrister, förebygga bristande efterlevnad och påvisa tillbörlig aktsamhet enligt ISO/IEC 27001, GDPR och relaterade ramverk.

1.3 Policyn möjliggör för små och medelstora företag att upprätthålla operativ styrning och certifieringsberedskap även utan en särskild regelefterlevnadsfunktion, genom användning av enkla, repeterbara checklistor och riskbaserade iakttagelser.

2. Omfattning

2.1 Denna policy gäller för:

2.1.1 Samtliga interna avdelningar och externa IT-tjänsteleverantörer med ansvar kopplat till IT-system, personuppgifter och verksamhetskritiska tjänster

2.1.2 Samtliga kontroller och system inom ISMS omfattning

2.1.3 Samtliga internrevisioner, granskningar av säkerhetskontroller och regelefterlevnadskontroller, oavsett om de utförs internt eller av extern konsult, kund eller tillsynsmyndighet

2.2 Denna policy gäller även för insamling av bevismaterial och rapportering för:

2.2.1 ISO/IEC 27001-certifieringsrevisioner och omcertifieringsrevisioner

2.2.2 Dataskyddsrevisioner enligt GDPR eller avtalsvillkor

2.2.3 Kunddrivna säkerhetsfrågeformulär eller leverantörsgranskningar

2.2.4 Regulatoriska eller oberoende granskningar enligt NIS2 eller DORA, där så är tillämpligt

3. Mål

3.1 Säkerställa att alla nyckelkontroller och policyer granskas regelbundet avseende effektivitet och efterlevnad.

3.2 Upprätthålla revisionsspår och register över korrigerande åtgärder för att visa ansvarsskyldighet och förbättring.

3.3 Förbereda för certifiering, omcertifiering och kundförsäkransprogram, till exempel ISO 27001 och onboarding av leverantörer.

3.4 Identifiera brister i ett tidigt skede så att åtgärder kan vidtas skyndsamt innan frågor eskalerar eller leder till bristande kravuppfyllelse.

3.5 Ge verkställande chef och IT-supportleverantör förutsättningar att samordna granskningar med låg komplexitet och samtidigt säkerställa försvarbara resultat.

4. Roller och ansvar

4.1 Verkställande chef (GM)

4.1.1 Har övergripande ansvar för revisionsprogrammet

4.1.2 Godkänner planer för interna granskningar och revisionsiakttagelser

4.1.3 Tilldelar och följer upp korrigerande åtgärder

4.1.4 Godkänner anlitande av externa revisorer eller konsulter

4.2 IT-supportleverantör/administratör

4.2.1 Tillhandahåller bevismaterial vid interna och externa revisioner, till exempel loggar, konfigurationer och register för åtkomstkontroll

4.2.2 Biträder vid tekniska kontroller, till exempel kontroll av säkerhetskopieringsstatus och efterlevnad av patchning

4.2.3 Underhåller revisionsarkivet för bevismaterial

[... 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 Årlig granskning av policy och revisionsplan

9.1.1 Verkställande chef (GM) ska granska denna policy och revisionsschemat minst en gång per år.

9.1.2 Granskningen ska utvärdera:

9.1.2.1 Revisionernas effektivitet i att identifiera brister

9.1.2.2 Genomförandegrad för revisioner och korrigerande åtgärder

9.1.2.3 Förändringar i tillämpliga rättsliga, regulatoriska eller certifieringsrelaterade krav

9.2 Händelsestyrda uppdateringar

9.2.1 Policyn ska granskas och uppdateras när:

9.2.2 En certifieringsrevision eller uppföljande revision resulterar i en större avvikelse

9.2.3 Rättsliga eller regulatoriska ramverk förändras, till exempel ny vägledning om GDPR eller nationellt genomförande av NIS2

9.2.4 Verksamhetsförändringar påverkar system, processer eller leverantörer som ingår i revisionsomfattningen

9.2.5 En kritisk incident eller överträdelse påvisar tidigare oupptäckta kontrollbrister

9.3 Dokumentation av uppdateringar

9.3.1 Samtliga revideringar ska följas upp i en versionslogg för policyn

9.3.2 Uppdateringar ska distribueras till alla teammedlemmar som medverkar i revisioner

9.3.3 En ändringssammanfattning ska bifogas den uppdaterade policyn för att säkerställa förståelse

10. Relaterade policyer och kopplingar

10.1 Denna policy stöds av och förstärker flera andra SME-policyer:

10.1.1 P1S – Informationssäkerhetspolicy: Fastställer baslinjen för samtliga kontrollkrav och kräver uppföljning genom revisioner.

10.1.2 P2S – Policy för styrningsroller och ansvar: Fastställer ansvarsskyldighet för revisionsplanering, genomförande och ägarskap för korrigerande åtgärder.

10.1.3 P6S – Riskhanteringspolicy: Identifierar kontrollsvagheter som upptäcks vid revisioner och säkerställer att revisionsiakttagelser dokumenteras i riskregistret.

10.1.4 P17S – Policy för dataskydd och integritet: Definierar GDPR-kontroller som ska revideras, inklusive datahantering, incidenthantering och integritetsmeddelanden.

10.1.5 P22S – Loggnings- och övervakningspolicy: Tillhandahåller revisionsloggar och forensiska data som används vid granskning av regelefterlevnad och kontroller.

10.1.6 P30S – Policy för incidenthantering: Kräver periodisk revision av incidentunderlag och granskningar efter incidenter för att verifiera incidenthanteringens effektivitet.

10.1.7 P31S – Policy för bevisinsamling och forensik: Anger rutiner för att samla in verifierbart bevismaterial med dokumentation av beviskedjan under revisioner.

10.2 Tillsammans skapar dessa policyer en sammanhållen kontrollmiljö som möjliggör intern verifiering, extern säkerhetsförsäkran och styrning i linje med standarder.

11. Referensstandarder och ramverk

11.1 ISO/IEC 27001:

11.1.1 Klausul 9.2 – Kräver internrevisioner för att utvärdera ISMS prestanda och överensstämmelse med krav.

11.1.2 Klausul 10.1 – Kräver kontinuerlig förbättring baserad på revisionsresultat och hantering av avvikelser.

11.2 ISO/IEC 27002:

11.2.1 Kontroll 5.35 – Kräver planerade interna granskningar av kontroller och processer.

11.2.2 Kontroll 5.37 – Betonar oberoende granskningar, särskilt av outsourcade processer.

11.3 NIST SP 800-53 Rev.5:

11.3.1 CA-2 – Säkerhetsbedömningar: Kräver revision av införda kontroller för att verifiera effektivitet.

11.3.2 CA-7 – Kontinuerlig övervakning: Betonar proaktiv identifiering och granskning av kontrollsvagheter.

11.3.3 AU-6 – Granskning, analys och rapportering av revision: Kräver regelbunden analys och hantering av revisionsloggar och revisionsiakttagelser.

11.4 EU:s GDPR:

11.4.1 Artiklarna 24 och 32 – Kräver genomförande och granskning av tekniska och organisatoriska åtgärder, inklusive bevis för kontrollernas effektivitet och förbättring över tid.

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

11.5.1 Artiklarna 20–21 – Kräver proaktiv kontrollgranskning, evidensbaserad regelefterlevnad och revisionsbarhet för väsentliga och viktiga aktörer.

11.6 COBIT 2019:

11.6.1 MEA01 – Övervaka, utvärdera och bedöma prestanda och överensstämmelse: Kräver periodisk bedömning av process- och kontrollprestanda mot standarder och mål.

11.6.2 MEA03 – Säkerställa efterlevnad av externa krav: Fokuserar på intern övervakning och beredskap för tredjepartsrevisioner och regulatoriska granskningar.