					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: P03					Dokumenttitel: **Policy för godtagbar användning**							
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 där så är tillämpligt

Standard/regelverk	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Klausul 5	Fastställer beteendenormer och krav för policy för godtagbar användning
ISO/IEC 27002:2022	Kontroller 6.1, 6.2, 8.1, 8.12	Ger vägledning om ansvar för informationssäkerhet, medvetenhet samt styrning av enheter och data
NIST SP 800-53 Rev. 5	AC-19, AC-20, AT-2	Åtkomstkontroll samt kontroller för medvetenhet och beteende som är relevanta för användning av IT-tillgångar
EU:s dataskyddsförordning (GDPR)	Artiklarna 5.1 f, 32; skäl 39	Säkerställer konfidentialitet och riktighet, kräver tekniska och organisatoriska kontroller samt rättslig grund för korrekt användning
EU:s NIS2-direktiv	Artikel 21.2 a–d	Kräver operativa policyer och utbildning i säker användning
EU:s DORA-förordning	Artikel 5	Stödjer IKT-riskhantering genom att reglera användarbeteende
COBIT 2019	APO07, BAI05, DSS05, MEA01	Personalresurser, ändringshantering, hanterade säkerhetstjänster samt övervakning av efterlevnad och prestanda

1. Syfte

1.1 Denna policy definierar godtagbar och otillåten användning av organisationens informationssystem, datorresurser, kommunikationsverktyg och praxis för datahantering.

1.2 Den säkerställer att alla användare förstår sitt ansvar vid användning av organisationens IT-tillgångar och att deras agerande stödjer konfidentialitet, riktighet, tillgänglighet samt laglig behandling av information.

1.3 Policyn uppfyller ISO/IEC 27001:2022, klausul 5.10, genom att fastställa beteendenormer för systemanvändning och genom att tillämpa tekniska och administrativa skyddsåtgärder för att minimera risken för felaktig användning, oaktsamhet eller missbruk.

1.4 Den stödjer även utredning och åtgärder vid tillämpning, inklusive incidenthantering och disciplinära åtgärder vid överträdelser.

2. Omfattning

2.1 Denna policy gäller för alla individer och enheter som har beviljats åtkomst till organisationens informationssystem och tillgångar, inklusive men inte begränsat till:

2.1.1 Anställda, entreprenörer, konsulter, praktikanter och inhyrd personal

2.1.2 Tredjepartsleverantörer med systemåtkomst eller delegerade administrativa roller

2.1.3 Gäster eller partner som använder organisationens egen eller godkänd IT-infrastruktur

2.2 Omfattningen inkluderar all organisatorisk teknik och alla datatillgångar, inklusive:

2.2.1 Arbetsstationer, bärbara datorer, mobila enheter och servrar

2.2.2 Nätverksinfrastruktur och molntjänster

2.2.3 E-post, meddelandetjänster, fillagring, samarbetsplattformar och VPN

2.2.4 Data i vila, under överföring eller under behandling, oavsett format eller plats

2.2.5 Alla personliga enheter som används inom ramen för Bring Your Own Device (BYOD) och som ansluter till organisationens system

2.3 Denna policy gäller i alla arbetsmiljöer, inklusive:

2.3.1 Organisationens kontor och produktionsanläggningar

2.3.2 Platser för distansarbete eller hybrida arbetsformer

2.3.3 Fältbaserad verksamhet eller lokaler som hanteras av tredje part

2.4 Alla användare ska bekräfta och följa denna policy som ett villkor för att få åtkomst till företagets system eller hantera företagets data.

3. Mål

3.1 Att definiera och tillämpa regler för godtagbar användning av organisationens IT-tillgångar.

3.2 Att förhindra obehörig åtkomst, dataläckage eller skada till följd av oaktsam eller skadlig användning.

3.3 Att skydda företagets nätverk, tillgångar och data mot hot som uppstår genom användarbeteende.

3.4 Att stödja rättsliga skyldigheter och avtalskrav genom att visa tillbörlig aktsamhet i styrningen av IT-resurser.

3.5 Att säkerställa konsekvens och tydlighet vid tillämpning av disciplinära åtgärder och processer för undantagshantering.

3.6 Att främja en kultur av etisk, säker och ansvarsfull användning av digitala och fysiska datorresurser.

4. Roller och ansvar

4.1 Verkställande ledning

4.1.1 Godkänner policy för godtagbar användning och säkerställer att den är i linje med verksamhetsmål, regulatoriska krav och organisationens värderingar.

4.1.2 Tilldelar resurser för tillämpning, utbildning, övervakning och policygranskning.

4.1.3 Granskar status för regelefterlevnad och disciplinära åtgärder kopplade till policyöverträdelser som en del av styrningen av ledningssystemet för informationssäkerhet.

4.2 IT- och informationssäkerhetsfunktionen

4.2.1 Inför tekniska skyddsåtgärder för att upprätthålla denna policy, inklusive:

4.2.2 Innehållsfiltrering, skydd mot skadlig kod, endpointskydd och nätverksövervakningsverktyg

4.2.3 E-postsäkerhetskonfigurationer och lösningar för dataförlustprevention (DLP)

4.2.4 Blocklistor och tillåtelselistor för programvara, hårdvara och webbplatser

4.2.5 Upprätthåller en inventering över godkänd och förbjuden programvara, utrustning och tjänster.

4.2.6 Utreder misstänkta överträdelser av policyn för godtagbar användning, säkrar forensisk bevisning och stödjer disciplinära eller rättsliga åtgärder där så är lämpligt.

4.2.7 Samarbetar med HR och juridikfunktionen kring incidenthantering, eskalering och rapporteringsskyldigheter.