					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: P03S					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

Standard/regelverk	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Klausul 5	Relevant för policyens övergripande omfattning och tillämpning
ISO/IEC 27002:2022	5.10, 5.11, 5	Vägledning om krav och säkerhetsåtgärder för godtagbar användning
NIST SP 800-53 Rev.5	AC-19, AC-20, AT-2	Omfattar användning av system och enheter, övervakning samt användarutbildning
EU:s GDPR	Artiklarna 5(1)(f), 32	Integritet och konfidentialitet för data samt säkerhetsåtgärder
EU:s NIS2-direktiv	Artikel 21(2)(b)	Kräver lämpliga säkerhetspolicyer och regler för godtagbar användning
DORA-förordningen	Artikel 9	Policy för IKT-riskhantering, säkerhetsåtgärder och tillämpning
COBIT 2019	DSS05, BAI	Säkerhetstjänster och kunskapshantering

1. Syfte

1.1. Denna policy fastställer krav för godtagbar, ansvarsfull och säker användning av system, enheter, internetåtkomst, e-post, molntjänster och personligt ägda enheter som tillhandahålls av eller används för verksamhetens behov.

1.2. Policyn säkerställer att användare förstår sina skyldigheter vid användning av organisationens IT-resurser samt skyddar dataintegritet, dataskydd och verksamhetens kontinuitet.

1.3. Denna policy stödjer efterlevnad av ISO/IEC 27001:2022 genom att fastställa tydliga krav på användarbeteende i enlighet med rättsliga skyldigheter, avtalskrav och regulatoriska krav.

2. Omfattning

2.1. Denna policy gäller för alla personer som har åtkomst till, administrerar eller på annat sätt interagerar med organisationens system eller data, inklusive:

2.1.1. anställda, uppdragstagare och tredjepartsleverantörer

2.1.2. visstidsanställda eller praktikanter

2.1.3. externa IT-tjänsteleverantörer

2.2. Policyn omfattar:

2.2.1. datorer, telefoner och surfplattor som ägs av organisationen

2.2.2. personligt ägda enheter som godkänts för verksamhetsbruk (BYOD)

2.2.3. organisationens nätverk, molnplattformar och programvarutjänster

2.2.4. internetåtkomst, e-postsystem, delad lagring och verksamhetsapplikationer

2.3. Denna policy gäller i alla arbetsmiljöer – på arbetsplatsen, på distans och vid hybridarbete – samt under all arbetstid.

3. Mål

3.1. Fastställa vad som utgör godtagbar respektive otillåten användning av IT-system.

3.1.1. Minska säkerhetsrisker som uppstår genom missbruk, obehörig åtkomst eller införande av skadlig kod.

3.1.2. Skydda verksamhetsdata, kundinformation och organisationens anseende.

3.1.3. Fastställa bindande regler och säkerställa ansvarsskyldighet för samtliga användare.

3.1.4. Stödja övervakning och uppföljning av efterlevnad för att tidigt upptäcka överträdelser och vidta korrigerande åtgärder.

4. Roller och ansvar

4.1. Verkställande direktör

4.1.1. Godkänner denna policy och ansvarar för att resurser och befogenheter finns för dess tillämpning.

4.1.2. Granskar och godkänner eventuella undantag från denna policy.

4.2. IT-chef eller extern IT-tjänsteleverantör

4.2.1. Upprätthåller inventarieförteckningar över godkänd programvara och hårdvara.

4.2.2. Konfigurerar enheter för att genomdriva reglerna för godtagbar användning, till exempel innehållsfiltrering och revisionsloggning.

4.2.3. Övervakar användning för att identifiera möjliga överträdelser och utreder incidenter.

4.2.4. Säkerställer att personligt ägda enheter (BYOD) är godkända och säkra om de används i verksamheten.

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

9. Krav på granskning och uppdatering

9.1. Årlig granskning

9.1.1. Denna policy ska granskas årligen av IT-chefen, med slutligt godkännande av verkställande direktören, för att säkerställa att den fortsatt är anpassad till teknikens användningsmönster, nya risker och krav på regelefterlevnad.

9.2. Utlösande faktorer för extra granskning

9.2.1. Granskningar ska även genomföras vid:

9.2.2. nya system eller tekniker, till exempel en ny molntjänst eller en ny plattform för endpointskydd

9.2.3. betydande policyöverträdelser

9.2.4. uppdaterade lagkrav eller avtalsvillkor som påverkar användningen av IT

9.3. Dokumentation av ändringar

9.3.1. Samtliga uppdateringar ska registreras i en versionslogg som omfattar:

9.3.1.1. versionsnummer

9.3.1.2. granskningsdatum

9.3.1.3. sammanfattning av ändringar

9.3.1.4. godkännandeinstans

9.4. Kommunikation av policy

9.4.1. Reviderade versioner av denna policy ska kommuniceras till samtliga berörda användare. Anställda ska bekräfta mottagande och förståelse som en del av sina skyldigheter avseende säkerhetsmedvetenhet.

10. Relaterade policyer och kopplingar

10.1. Denna policy ska tillämpas tillsammans med flera andra SME-policyer för att säkerställa en heltäckande reglering av säkerhetsansvar:

10.1.1. P4S – Policy för åtkomstkontroll: Fastställer tekniskt och processmässigt genomförande av tillåten användning och kontobegränsningar.

10.1.2. P8S – Policy för informationssäkerhetsmedvetenhet och utbildning: Tillhandahåller användarutbildning om gränser för godtagbar användning och rapporteringsskyldigheter.

10.1.3. P9S – Policy för distansarbete: Reglerar användning av organisationens system utanför ordinarie arbetsplats eller i hemmiljö.

10.1.4. P17S – Policy för dataskydd och integritet: Fastställer regler för behandling av personuppgifter som samverkar med övervakning av godtagbar användning och BYOD.

10.1.5. P30S – Policy för incidenthantering: Styr processer för att utreda och hantera missbruk eller överträdelser av reglerna för godtagbar användning.

11. Referensstandarder och ramverk

11.1. ISO/IEC 27001

11.1.1. Klausul 5.10 – Kräver att organisationer definierar och tillämpar godtagbar användning av organisationens tillgångar.

11.2. ISO/IEC 27002

11.2.1. Kontroll 5.10 – Ger vägledning om godtagbar användning av system, inklusive tillåtna och förbjudna beteenden.

11.3. NIST SP 800-53 Rev.5

11.3.1. AC-19 – Behandlar kontroll av systemanvändning, inklusive personligt ägda enheter.

11.3.2. AC-20 – Kräver godkännande och övervakning av externa system.

11.3.3. AT-2 – Betonar utbildning av användare i praxis för godtagbar användning.

11.4. EU:s GDPR

11.4.1. Artikel 5(1)(f) – Kräver integritet och konfidentialitet för personuppgifter, vilket kan äventyras genom användarmissbruk.

11.4.2. Artikel 32 – Kräver införande av tekniska och organisatoriska säkerhetsåtgärder för att skydda system och data.

11.5. EU:s NIS2-direktiv

11.5.1. Artikel 21(2)(b) – Kräver lämpliga säkerhetspolicyer, inklusive regler för godtagbar användning, för att minska cyberhot.

11.6. DORA-förordningen

11.6.1. Artikel 9 – Kräver policyer för IKT-riskhantering, vilket omfattar användningskontroller och mekanismer för tillämpning.

11.7. COBIT 2019

11.7.1. DSS05 – Hantera säkerhetstjänster: Betonar policybaserad styrning av användarbeteende.

11.7.2. BAI08 – Hantera kunskap: Behandlar medvetenhet om policyansvar och utbildning i godtagbar användning.