					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: P34S					Dokumenttitel: **Policy för mobila enheter och Bring Your Own Device (BYOD)**							
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**

Anpassning till standarder och regelverk där tillämpligt

Standard/regelverk	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Klausulerna 5.1, 5.2, 6.1, 6.2, 8	Övergripande krav för ISMS samt kontroller för mobila enheter/BYOD
ISO/IEC 27002:2022	Kontrollerna 5.10–5.13	Detaljerade kontroller för mobila enheter/BYOD och fjärråtkomst
NIST SP 800-53 Rev.5	AC-19, AC-20, CM-6, MP-7	Kontroller för enheter, medier och konfiguration
EU:s dataskyddsförordning (GDPR)	Artikel 5.1 f	Skydd av personuppgifter och mobila slutpunkter
EU:s NIS2-direktiv	Artikel 21.2 d	Skydd av verksamhetskritiska enheter, inklusive BYOD
EU:s DORA-förordning	Artiklarna 9, 10	IKT-riskhantering och verksamhetskontinuitet för mobila slutpunkter
COBIT 2019	APO13, DSS01, DSS05	IT-styrning, drift och kontroller för säkerhetstjänster

1. Syfte

1.1. Denna policy fastställer bindande säkerhetskrav för användning av mobila enheter, inklusive smarttelefoner, surfplattor och bärbara datorer, vid åtkomst till organisationens information, system eller tjänster.

1.2. Policyn reglerar även användning av Bring Your Own Device (BYOD) för att säkerställa att kunddata och verksamhetsinformation skyddas, oavsett vem som äger enheten.

1.3. Policyn säkerställer ett enhetligt skydd för mobil åtkomst, stödjer certifieringsmålen enligt ISO/IEC 27001 och förebygger dataförlust eller kompromettering till följd av förlorade, stulna eller felanvända mobila slutpunkter.

1.4. Policyn säkerställer att både tekniska och administrativa skyddsåtgärder tillämpas vid mobil användning i små och medelstora företag utan dedikerade IT-team, inklusive i distansarbetsmiljöer och molntjänster.

2. Omfattning

2.1. Denna policy gäller för alla anställda, entreprenörer, praktikanter, tredjepartstjänsteleverantörer och andra tjänsteleverantörer som:

2.1.1. använder en mobil enhet för att få åtkomst till, behandla eller lagra organisationsdata eller system

2.1.2. ansluter till organisationens tjänster, inklusive e-post, delade mappar, molnapplikationer eller interna system via VPN

2.2. Policyn omfattar:

2.2.1. alla mobila enheter: smarttelefoner, surfplattor och bärbara datorer (organisationsägda eller personliga BYOD-enheter)

2.2.2. alla operativsystem (t.ex. iOS, Android, Windows, macOS)

2.2.3. alla platser (kontor, hem, distansarbetsplatser, offentliga miljöer)

2.3. Policyn gäller i alla arbetsmiljöer och ska tillämpas oavsett vem som äger enheten.

3. Mål

3.1. Förebygga dataförlust: Säkerställa att mobil användning inte exponerar känsliga organisationsdata eller kunddata för obehörig åtkomst, stöld eller missbruk.

3.2. Fastställa tydliga regler för BYOD: Ange bindande villkor för användning av personliga enheter i arbetet och säkerställa rättsliga och tekniska skyddsåtgärder.

3.3. Stödja regelefterlevnad: Uppfylla krav enligt ISO/IEC 27001, EU:s dataskyddsförordning (GDPR), EU:s NIS2-direktiv och andra rättsliga skyldigheter genom bindande säkerhetsrutiner för mobila enheter.

3.4. Minimera operativ risk: Minska sannolikheten för driftstörningar orsakade av felaktig användning, kompromettering eller fel i mobila enheter.

3.5. Upprätthålla kundernas förtroende: Visa för kunder och partner att deras data förblir skyddade även när de nås via mobila eller personliga enheter.

4. Roller och ansvar

4.1. Verkställande direktör (GM):

4.1.1. Har det övergripande ansvaret för denna policy.

4.1.2. Godkänner all mobil åtkomst och all BYOD-åtkomst till organisationens system.

4.1.3. Säkerställer att BYOD-avtal undertecknas, lagras och följs upp.

4.1.4. Verifierar att externa IT-tjänsteleverantörer tillämpar de skyddsåtgärder för mobila enheter som krävs.

4.2. Utsedd medarbetare eller IT-support:

4.2.1. Ansvarar för installation, registrering och konfiguration av mobila enheter som används i arbetet.

4.2.2. Tillämpar åtkomstkontroller, appbegränsningar och övervakningskrav kopplade till mobila enheter.

4.2.3. Stödjer incidenthantering för mobila enheter vid förlust, stöld eller kompromettering.

[... 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

9.1.1. Verkställande direktör (GM) ska granska denna policy minst en gång var tolfte månad.

9.1.2. Granskningen ska verifiera fortsatt anpassning till kraven i ISO/IEC 27001, utvecklingen inom mobil teknik och förändringar i verksamheten.

9.1.3. Uppdateringar ska även beakta nyligen inträffade incidenter, revisionsresultat eller regulatoriska förändringar (t.ex. EU:s dataskyddsförordning (GDPR), EU:s NIS2-direktiv, EU:s DORA-förordning).

9.2. Utlösande händelser för mellanliggande granskning

9.2.1. Denna policy ska uppdateras omedelbart om något av följande inträffar:

9.2.1.1. större mobilrelaterad säkerhetsincident (t.ex. incident till följd av en förlorad eller hackad enhet)

9.2.1.2. förändring av plattformar eller verktyg för hantering av mobila enheter som stöds

9.2.1.3. rättslig eller regulatorisk förändring som påverkar användning av personliga enheter eller dataskydd

9.2.1.4. införande av nya appar, tjänster eller verktyg från tredje part som används på mobila enheter

9.3. Dokumentation av ändringar

9.3.1. Alla granskningar och uppdateringar ska dokumenteras, inklusive granskningsdatum, genomförda ändringar och GM:s godkännande.

9.3.2. Versionshistorik ska bevaras för revisionsändamål.

9.4. Kommunikation och åtkomst

9.4.1. GM ska säkerställa att alla användare (anställda, entreprenörer, tredje part) informeras om ändringar.

9.4.2. Uppdaterade versioner ska göras lätt tillgängliga, exempelvis i delade mappar eller interna plattformar.

10. Relaterade policyer och kopplingar

10.1. Denna policy utgör en del av den övergripande policysamlingen för informationssäkerhet för SME och ska tillämpas tillsammans med följande:

10.1.1. P4S – Policy för åtkomstkontroll: Fastställer krav för hantering av säker åtkomst till system, inklusive system som nås via mobila enheter. Policyn ställer krav på lösenordshygien och sessionskontroller.

10.1.2. P8S – Policy för informationssäkerhetsmedvetenhet och utbildning: Säkerställer att användare utbildas i säker användning av mobila enheter, incidentrapportering och villkor för BYOD.

10.1.3. P17S – Policy för dataskydd och integritet: Fastställer hantering av personuppgifter och organisationsdata på mobila plattformar i enlighet med EU:s dataskyddsförordning (GDPR), särskilt när personliga enheter används i arbetet.

10.1.4. P9S – Policy för distansarbete: Samordnar krav och förväntningar på mobil användning vid arbete utanför organisationens lokaler eller hemifrån, inklusive hantering av enheter och skyddsåtgärder för nätverksåtkomst.

10.1.5. P30S – Policy för incidenthantering: Anger ramverket för hantering av mobilrelaterade incidenter, inklusive komprometterade eller förlorade enheter.

10.2. Dessa relaterade policyer samverkar för att utgöra en komplett uppsättning kontroller för säkerhet för mobila enheter i små och medelstora företag utan dedikerad IT-personal och säkerställer att kraven kan tillämpas, är transparenta och stödjer certifieringsberedskap.

11. Referensstandarder och ramverk

11.1. Denna policy stödjer fullständig anpassning till följande säkerhets- och regelefterlevnadsstandarder:

11.2. ISO/IEC 27001:

11.2.1. Klausul 5.1 – Ledarskap och åtagande: Säkerställer ledningens tillsyn och ansvar för mobil åtkomst och BYOD-åtkomst

11.2.2. Klausul 6.1 – Åtgärder för att hantera risker: Kräver att risker för mobila enheter bedöms och behandlas

11.2.3. Klausul 8.1 – Operativ planering och styrning: Kräver enhetliga rutiner för mobil åtkomst för att skydda verksamhetsinformation

11.3. ISO/IEC 27002:

11.3.1. Kontrollerna 5.10 (användning av mobila enheter), 5.11 (distansarbete), 5.12 (fjärråtkomst) och 5.13 (BYOD): Ger vägledning för genomförande av hantering av enhetsrisker i mindre verksamheter

11.4. NIST SP 800-53 Rev.5:

11.4.1. AC-19 – Åtkomstkontroll för mobila enheter: Kräver säkerhetsinställningar för godkänd mobil användning

11.4.2. AC-20 – Användning av externa system: Styr risker kopplade till BYOD och fjärråtkomst

11.4.3. CM-6 – Konfigurationsinställningar: Kräver säkra standardinställningar och anpassade inställningar på mobila plattformar

11.4.4. MP-7 – Användning av medier: Omfattar korrekt användning av och begränsningar för mobil lagring och dataåtkomst

11.5. EU:s dataskyddsförordning (GDPR) (2016/679):

11.5.1. Artikel 5.1 f – integritet och konfidentialitet: Kräver skydd av personuppgifter genom lämplig säkerhet, särskilt på mobila plattformar

11.5.2. Artikel 32 – Säkerhet i behandlingen: Kräver lämpliga tekniska och organisatoriska åtgärder (TOM) för att skydda data som nås eller lagras på mobila enheter

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

11.6.1. Artikel 21.2 d – Säkerhetsåtgärder för enheter: Kräver säkerhetskontroller för hårdvara och programvara som används för åtkomst till verksamhetskritiska system, inklusive personliga enheter

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

11.7.1. Artikel 9 – Ramverk för IKT-riskhantering: Kräver skydd av mobila slutpunkter som används för verksamhetskritisk kommunikation och molntjänster

11.7.2. Artikel 10 – IKT-verksamhetskontinuitet: Kräver fortsatt säker åtkomst till verksamhetssystem även vid störningar eller distansarbete

11.8. COBIT 2019:

11.8.1. APO13 – Manage Security: Kräver att organisationen tillämpar policyer för mobila enheter och BYOD i linje med verksamhetens risker

11.8.2. DSS01 – Manage Operations: Säkerställer tekniskt genomförande av mekanismer för säker åtkomst

11.8.3. DSS05 – Manage Security Services: Styr tredje parts medverkan i att upprätthålla säkra mobila miljöer och samordning av incidenthantering