					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: P34					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**

Juridiskt meddelande (upphovsrätt och användningsbegränsningar)

(C) 2025 Clarysec LLC. All rights reserved.

Detta dokument är Clarysec LLC:s immateriella egendom. Ingen del av detta dokument får kopieras, återanvändas, distribueras eller ändras för kommersiella eller implementeringsändamål utan uttryckligt skriftligt förhandstillstånd.
Obehörig användning är strängt förbjuden och kan leda till rättsliga åtgärder.
För licensiering, kontakta: info@clarysec.com

Anpassning till standarder och regelverk

Standard/regelverk	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	5.2, 6.1, 7.5, 8	Tillämpar säkerhetskontroller och krav på regelefterlevnad
ISO/IEC 27002:2022	5.10, 8.1, 8.5, 8	Tillhandahåller detaljerade kontroller för hantering av mobila enheter
NIST SP 800-53 Rev.5	AC-19, AC-17, CM-7, MP-5, SC-12	Åtkomstkontroll, fjärråtkomst, konfiguration och säkerhetskrav för mobila enheter
EU:s GDPR	5(1)(f), 25, 32	Obligatoriska krav för dataskydd, kryptering och säker behandling
EU:s NIS2-direktiv	21(2)(d)	Tekniska och organisatoriska skyddsåtgärder för mobil åtkomst
EU:s DORA-förordning	9, 10	IKT-riskhantering och säkerhetskrav för mobil användning
COBIT 2019	APO13.02, DSS01.04, BAI09	Planer för informationssäkerhet, tillgångskonfiguration och kontroller för mobila miljöer

1. Syfte

1.1 Denna policy fastställer säkerhetsmässiga, regulatoriska och operativa krav för användning av mobila enheter och personliga enheter (BYOD – Bring Your Own Device) vid åtkomst till organisationens system, applikationer eller data.

1.2 Syftet är att säkerställa konfidentialitet, riktighet och tillgänglighet för organisationens information som nås eller behandlas via mobila slutpunkter, inklusive smarttelefoner, surfplattor, bärbara datorer och hybridenheter.

1.3 Policyn fastställer även de tekniska kontroller och rutiner som krävs för att begränsa risker såsom dataläckage, obehörig åtkomst, förlust eller stöld av enheter samt kompromettering av mobila applikationer.

1.4 Denna policy stödjer efterlevnad av regulatoriska krav och avtalskrav samt möjliggör säker mobil produktivitet för anställda, konsulter, tredjepartsleverantörer och andra behöriga tredje parter.

2. Omfattning

2.1 Denna policy gäller för all personal, inklusive anställda, konsulter, praktikanter och tredjepartsleverantörer, som använder mobila enheter för att få åtkomst till organisationens data, system, applikationer eller kommunikationsplattformar.

2.2 Den omfattar all mobil datorutrustning, inklusive men inte begränsat till:

2.2.1 Smarttelefoner och surfplattor (iOS, Android etc.)

2.2.2 Bärbara datorer och ultrabooks (Windows, macOS, Linux)

2.2.3 Bärbara enheter och hybrida smarta enheter med funktion för datasynkronisering

2.3 Den gäller oavsett om enheten ägs av organisationen eller är privatägd enligt en BYOD-överenskommelse.

2.4 Policyn omfattar samtliga åtkomstvägar, inklusive VPN, virtuella skrivbord, molnapplikationer, e-post, samarbetsplattformar (t.ex. SharePoint, Teams) och verktyg för filsynkronisering (t.ex. OneDrive, Dropbox där detta är godkänt).

2.5 Den omfattar användning vid distansarbete, arbete på plats, under resor eller inom ramen för hybridarbete.

3. Mål

3.1 Att minska risken för kompromettering, läckage eller förlust av data till följd av osäker användning av mobila enheter.

3.2 Att tillämpa enhetliga och bindande säkerhetskontroller på alla mobila slutpunkter, oavsett ägandemodell (organisationens eller BYOD).

3.3 Att säkerställa att användning av mobila enheter uppfyller kraven i ISO/IEC 27001 och andra regulatoriska ramverk som är tillämpliga på dataskydd och cybersäkerhet.

3.4 Att möjliggöra säker integration av mobila enheter i organisationens operativa arbetsflöden samt kommunikations- och samarbetsflöden.

3.5 Att tillhandahålla tydligt definierade ansvar och processer för hantering av mobila enheter (MDM), inklusive registrering, fjärradering, kryptering, autentisering och övervakning.

3.6 Att skydda integritetsrättigheter för individer som använder sina egna enheter samtidigt som organisationens känsliga information skyddas.

4. Roller och ansvar

4.1 Informationssäkerhetschef (CISO) / IT-säkerhetsansvarig

4.1.1 Fastställer policy och tekniska standarder för mobil användning och BYOD.

4.1.2 Utövar tillsyn över regelefterlevnad, incidenthantering och hantering av undantag för kontroller av mobila enheter.

4.1.3 Samordnar med juridisk funktion och HR för att säkerställa att tillämpningen är rättsligt hållbar och organisatoriskt förankrad.

4.2 IT-administratör / MDM-administratör

4.2.1 Hanterar tilldelning av åtkomst, registrering och konfiguration av mobila enheter genom MDM-lösningar.

4.2.2 Tillämpa kontroller på enhetsnivå (t.ex. kryptering, PIN-koder och applikationskontroller).

4.2.3 Utför fjärradering, låsning av enheter och återkallelse av behörigheter vid behov.

[... 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 informationssäkerhetschef (CISO) eller utsedd informationssäkerhetsansvarig för att säkerställa anpassning till:

9.1.1 Förändringar i plattformar för mobila operativsystem, MDM-teknik eller autentiseringsstandarder

9.1.2 Regulatoriska ändringar eller avtalsändringar som påverkar skydd av mobila data (t.ex. GDPR, DORA, NIS2)

9.1.3 Revideringar av kontrolluppsättningar i ISO/IEC 27001:2022, ISO/IEC 27002:2022 eller NIST SP 800-53 Rev.5

9.1.4 Återkoppling från revisioner, granskningar efter incidenter eller rapporter från anställda

9.2 Mellanliggande granskningar kan utlösas av:

9.2.1 Säkerhetsincidenter som involverar mobila enheter eller BYOD-plattformar

9.2.2 Avisering från leverantör om högriskssårbarheter i plattformar som stöds

9.2.3 Införande av nya mobila applikationer eller samarbetsplattformar som används i verksamheten

9.3 Uppdateringar av policyn ska:

9.3.1 Dokumenteras i policyns versionshistorik

9.3.2 Kommuniceras till all personal och berörda konsulter och tredjepartsleverantörer

9.3.3 Bekräftas på nytt genom uppdaterad policybekräftelse för alla BYOD-användare

9.4 Alla granskningar och revideringar ska formellt godkännas av verkställande ledning och loggas i registret för policyändringar.

10. Relaterade policyer och kopplingar

10.1 Denna policy har beroenden till flera centrala policyer inom organisationens ISMS-ramverk. Viktiga kopplingar omfattar:

10.1.1 P1 – Informationssäkerhetspolicy: Fastställer de övergripande styrningsprinciperna för samtliga informationssäkerhetskontroller, inklusive dem som styr användning av mobila enheter.

10.1.2 P3 – Policy för godtagbar användning: Definierar tillåtna beteenden och begränsningar vid användning av teknik, vilket direkt gäller för mobil åtkomst och BYOD-åtkomst.

10.1.3 P9 – Policy för distansarbete: Beskriver ytterligare säkerhetskrav för mobila arbetsmiljöer och kompletterar de mobilspecifika kontroller som definieras i denna policy.

10.1.4 P13 – Policy för dataklassificering och märkning: Styr hur data på mobila enheter ska hanteras utifrån klassificeringsnivå, vilket påverkar lagring, överföring och tillämpning av kryptering.

10.1.5 P22 – Loggnings- och övervakningspolicy: Stödjer insamling och granskning av loggar för mobil åtkomst för att upptäcka avvikelser eller överträdelser.

10.1.6 P30 – Policy för incidenthantering (P30): Styr hur mobilrelaterade incidenter (t.ex. förlust av enhet eller obehörig åtkomst) ska hanteras och eskaleras.

10.1.7 P33 – Policy för revisions- och regelefterlevnadsövervakning: Ger grund för periodiska kontroller av efterlevnad av mobil säkerhet, inklusive efterlevnad av BYOD-policyn.

11. Referensstandarder och ramverk

11.1 Denna policy är anpassad till internationellt erkända ramverk för cybersäkerhet och rättsliga skyldigheter för att säkerställa säker användning av mobila enheter och personliga enheter (BYOD) i företagsmiljöer.

11.2 ISO/IEC 27001:

11.2.1 Klausul 5.10 – Godtagbar användning av information och andra tillgångar: Kräver kontroller för ansvarsfull användning av organisationens tillgångar, inklusive mobila enheter.

11.2.2 Klausul 5.11 – Distansarbete: Reglerar säkra arbetssätt vid åtkomst till system utanför organisationens lokaler.

11.2.3 Klausul 5.12 – Användning av mobila enheter: Kräver riskbaserade kontroller för mobila slutpunkter och BYOD-konfigurationer.

11.2.4 Klausul 5.13 – Informationsöverföring: Kräver skydd av information som överförs via mobila kanaler.

11.3 ISO/IEC 27002:2022 – Kontroller 5.10 till 5.13:

11.3.1 Bilaga A, kontroller 5.10 till 5.13: Anger hur mobil åtkomst, kryptering, övervakning och förlustförebyggande åtgärder ska tillämpas inom ett ISMS. Dessa kontroller ger detaljerad vägledning för genomförande för att skydda mobila slutpunkter, tillämpa containerisering, övervaka enheters integritet och säkerställa integritetsmedvetna konfigurationer för BYOD-användning.

11.4 NIST SP 800-53 Rev.5:

11.4.1 AC-19 – Åtkomstkontroll för mobila enheter: Definierar baskrav för skydd, inklusive kryptering, autentisering och MDM-krav.

11.4.2 AC-17 – Fjärråtkomst: Kräver säker autentisering och sessionsskydd för användare som använder mobil fjärråtkomst.

11.4.3 CM-7 – Principen om minsta funktionalitet: Stödjer borttagning av onödiga appar och funktioner från mobila slutpunkter för att minska risk.

11.4.4 MP-5 – Skydd vid transport av medier: Reglerar säker överföring av data från mobila system till externa destinationer eller destinationer i molnmiljö.

11.4.5 SC-12 – Etablering av kryptografiska nycklar: Kräver användning av säkra kryptografiska protokoll för mobil kommunikation och lagring.

11.5 EU:s GDPR (2016/679):

11.5.1 Artikel 5(1)(f) – Integritet och konfidentialitet: Kräver att organisationer skyddar personuppgifter på mobila enheter mot obehörig eller olaglig åtkomst.

11.5.2 Artikel 25 – Inbyggt dataskydd och dataskydd som standard: Kräver att integritetsskydd byggs in i BYOD- och MDM-processer.

11.5.3 Artikel 32 – Säkerhet i samband med behandling: Kräver riskbaserade kontroller (t.ex. kryptering, autentisering och åtkomstkontroll) för personuppgifter på mobila plattformar.

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

11.6.1 Artikel 21(2)(d): Kräver att mobil åtkomst till kritiska system och information skyddas genom lämpliga tekniska och organisatoriska åtgärder, såsom slutpunktskontroll, kryptering och övervakning.

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

11.7.1 Artikel 9 – Ramverk för IKT-riskhantering: Kräver att finansiella entiteter begränsar risker kopplade till mobil åtkomst och fjärråtkomst som en del av operativ resiliens.

11.7.2 Artikel 10 – Säkerhetskrav för IKT-system: Kräver säker mobil arkitektur, övervakning och responsmekanismer för cyberhot som härrör från mobila enheter.

11.8 COBIT 2019:

11.8.1 APO13.02 – Upprätta och underhåll en plan för informationssäkerhet: Kräver att användning av mobila enheter, inklusive BYOD, integreras i organisationens säkerhetsstrategier.

11.8.2 DSS01.04 – Hantera konfiguration och integritet för tillgångar: Gäller styrning av konfiguration och säker driftsättning av mobila enheter.

11.8.3 BAI09.01 – Upprätta och underhåll kontroller: Stödjer införande av tekniska skyddsåtgärder och rutiner för säker mobil användning och säker fjärroperation.