					Indsæt navnet på den registrerede juridiske enhed her							
Dokumentnummer: P34					Dokumenttitel: **Politik for mobile enheder og BYOD**							
Version: 1.0		Ikrafttrædelsesdato: 01.01.2025			Dokumentejer:							
X	Politik		Standard		Procedure		Formular		Register		Andet	

Revisionshistorik				
Revisionsnummer	**Revisionsdato**	**Ændringer**	**Gennemgået af**	**Procesejer**

Godkendelser			
Navn	**Stilling**	**Dato**	**Underskrift**

Tilpasset relevante standarder og regulering

Standard/regulering	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	5.2, 6.1, 7.5, 8	Omfatter sikkerhedskontroller og krav til efterlevelse
ISO/IEC 27002:2022	5.10, 8.1, 8.5, 8	Indeholder detaljerede kontroller for styring af mobile enheder (MDM)
NIST SP 800-53 Rev.5	AC-19, AC-17, CM-7, MP-5, SC-12	Adgangsstyring, fjernadgang, konfiguration og sikkerhedskrav for mobile enheder
EU GDPR	5(1)(f), 25, 32	Obligatoriske krav til databeskyttelse, datakryptering og behandlingssikkerhed
EU NIS2	21(2)(d)	Tekniske og organisatoriske sikkerhedsforanstaltninger for mobil adgang
EU DORA	9, 10	Krav til styring af IKT-risici og sikkerhed for mobile enheder
COBIT 2019	APO13.02, DSS01.04, BAI09	Informationssikkerhedsplaner, aktivkonfiguration og kontroller for mobile miljøer

Formål

1.1 Denne politik fastsætter sikkerheds-, efterlevelses- og driftskrav for brug af mobile enheder og personligt udstyr (BYOD – Bring Your Own Device) ved adgang til organisationens systemer, applikationer eller data.

1.2 Formålet er at sikre fortrolighed, integritet og tilgængelighed af organisationens oplysninger, som tilgås eller behandles via mobile endepunkter, herunder smartphones, tablets, bærbare computere og hybride enheder.

1.3 Politikken fastsætter desuden de tekniske og proceduremæssige kontroller, der kræves for at begrænse risici såsom datalækage, uautoriseret adgang, tab eller tyveri af enheder samt kompromittering af mobile applikationer.

1.4 Denne politik understøtter regulatorisk og kontraktuel efterlevelse og muliggør samtidig sikker mobil adgang for medarbejdere, kontraktansatte og autoriserede tredjeparter.

2. Omfang

2.1 Denne politik gælder for alt personale, herunder medarbejdere, kontraktansatte, praktikanter og tredjepartsleverandører, som anvender mobile enheder til at få adgang til organisationens data, systemer, applikationer eller kommunikationsplatforme.

2.2 Politikken omfatter alle mobile it-enheder, herunder, men ikke begrænset til:

2.2.1 Smartphones og tablets (iOS, Android osv.)

2.2.2 Bærbare computere og ultrabooks (Windows, macOS, Linux)

2.2.3 Wearables og hybride smartenheder med mulighed for datasynkronisering

2.3 Politikken gælder, uanset om enheden ejes af organisationen eller er en privat enhed omfattet af en aftale om brug af BYOD.

2.4 Politikken omfatter alle adgangsveje, herunder VPN, virtuelle desktops, cloudapplikationer, e-mail, samarbejdsværktøjer (f.eks. SharePoint, Teams) og værktøjer til filsynkronisering (f.eks. OneDrive, Dropbox, hvor dette er godkendt).

2.5 Politikken gælder ved fjernarbejde, på organisationens lokationer, under rejser samt i hybride arbejdsformer.

3. Mål

3.1 At reducere risikoen for kompromittering, datalækage eller tab af data som følge af usikker brug af mobile enheder.

3.2 At håndhæve ensartede sikkerhedskontroller på tværs af alle mobile endepunkter, uanset ejerskabsmodel (organisationsejede enheder eller BYOD).

3.3 At sikre, at brugen af mobile enheder er i overensstemmelse med ISO/IEC 27001 og øvrige regulatoriske rammer, der gælder for databeskyttelse, informationssikkerhed og cybersikkerhed.

3.4 At understøtte sikker integration af mobile enheder i organisationens drifts-, kommunikations- og samarbejdsprocesser.

3.5 At fastlægge klart definerede ansvar og processer for styring af mobile enheder (MDM), herunder registrering, fjernsletning, kryptering, autentifikation og overvågning.

3.6 At beskytte privatlivsrettighederne for personer, der anvender deres egne enheder, samtidig med at organisationens følsomme oplysninger beskyttes.

4. Roller og ansvar

4.1 Chief Information Security Officer (CISO) / informationssikkerhedsansvarlig

4.1.1 Fastlægger politikken og de tekniske standarder for brug af mobile enheder og BYOD.

4.1.2 Fører tilsyn med efterlevelse, hændelseshåndtering og håndtering af undtagelser vedrørende kontroller for mobile enheder.

4.1.3 Koordinerer med Jura, Compliance og HR for at sikre, at håndhævelsen er juridisk holdbar og organisatorisk forankret.

4.2 it-administrator / MDM-administrator

4.2.1 Varetager klargøring af brugeradgang, registrering og konfiguration af mobile enheder gennem løsninger til styring af mobile enheder (MDM).

4.2.2 Håndhæver kontroller på enhedsniveau (f.eks. kryptering, PIN-koder og applikationskontroller).

4.2.3 Udfører fjernsletning, enhedslåsning og tilbagekaldelse af adgang, når dette er nødvendigt.

[... Afsnit 4.3–8 er ikke inkluderet i denne forhåndsvisning. Køb det fulde dokument for at få adgang til det komplette indhold. ...]

9. Krav til gennemgang og opdatering

9.1 Denne politik skal gennemgås mindst én gang årligt af CISO eller den udpegede informationssikkerhedsansvarlige for at sikre overensstemmelse med:

9.1.1 ændringer i mobile OS-platforme, MDM-teknologier eller autentifikationsstandarder

9.1.2 regulatoriske eller kontraktuelle ændringer, der påvirker beskyttelsen af mobile data (f.eks. GDPR, DORA, NIS2)

9.1.3 ændringer i kontrolsæt i ISO/IEC 27001:2022, ISO/IEC 27002:2022 eller NIST SP 800-53 Rev.5

9.1.4 feedback fra revisioner, gennemgange efter hændelser eller medarbejderrapporter

9.2 Mellemliggende gennemgange kan udløses af:

9.2.1 sikkerhedshændelser, der involverer mobile enheder eller BYOD-platforme

9.2.2 leverandørmeddelelser om højrisikosårbarheder i understøttede platforme

9.2.3 indførelse af nye mobile applikationer eller samarbejdsplatforme anvendt i driften

9.3 Opdateringer af politikken skal:

9.3.1 dokumenteres i politikkens versionshistorik

9.3.2 kommunikeres til alt personale og berørte kontraktansatte

9.3.3 bekræftes på ny med opdateret bekræftelse for alle BYOD-brugere

9.4 Alle gennemgange og revisioner af politikken skal godkendes formelt af direktionen og registreres i registeret over politikændringer.

10. Relaterede politikker og sammenhænge

10.1 Denne politik er afhængig af flere centrale politikker i organisationens ISMS-rammeværk. Væsentlige sammenhænge omfatter:

10.1.1 P1 – Informationssikkerhedspolitik: Fastlægger de overordnede styringsprincipper for alle informationssikkerhedskontroller, herunder kontroller for brug af mobile enheder.

10.1.2 P3 – Politik for acceptabel brug: Definerer tilladt adfærd og begrænsninger ved brug af teknologi, som direkte gælder for mobil adgang og BYOD-adgang.

10.1.3 P9 – Politik for fjernarbejde: Fastlægger yderligere sikkerhedsforpligtelser for mobile arbejdsmiljøer og supplerer de mobilespecifikke kontroller i denne politik.

10.1.4 P13 – Politik for dataklassificering og mærkning: Regulerer, hvordan data på mobile enheder skal håndteres på baggrund af klassificeringsniveau og har betydning for lagring, overførsel og håndhævelse af kryptering.

10.1.5 P22 – Lognings- og overvågningspolitik: Understøtter indsamling og gennemgang af logfiler for mobil adgang med henblik på at identificere anomalier eller overtrædelser.

10.1.6 P30 – Politik for hændelseshåndtering: Regulerer, hvordan mobilrelaterede hændelser (f.eks. tab af enhed, uautoriseret adgang) håndteres og eskaleres.

10.1.7 P33 – Politik for overvågning af revision og compliance: Danner grundlag for periodiske kontroller af efterlevelse af mobil sikkerhed, herunder efterlevelse af BYOD-politikken.

11. Referencestandarder og rammeværker

11.1 Denne politik er tilpasset internationalt anerkendte rammeværker for cybersikkerhed og gældende retlige forpligtelser for at sikre sikker brug af mobile enheder og personlige BYOD-teknologier i virksomhedsmiljøer.

11.2 ISO/IEC 27001:

11.2.1 Kontrol 5.10 – Acceptabel brug af information og andre tilknyttede aktiver: Kræver kontroller for ansvarlig brug af organisationens aktiver, herunder mobile enheder.

11.2.2 Kontrol 6.7 – Fjernarbejde: Regulerer sikker praksis ved adgang til systemer uden for organisationens lokationer.

11.2.3 Kontrol 6.8 – Hændelsesrapportering om informationssikkerhed: Understøtter rettidig rapportering af hændelser relateret til mobile enheder og BYOD.

11.2.4 Kontrol 8.1 – Brugeres slutenheder: Kræver risikobaserede kontroller for mobile endepunkter og BYOD-konfigurationer.

11.3 ISO/IEC 27002:2022:

11.3.1 Kontrollerne i ISO/IEC 27002:2022 giver detaljeret vejledning til implementering af sikkerhed for mobile endepunkter, håndhævelse af containerisering, overvågning af enheders integritet og sikring af databeskyttelsesunderstøttende konfigurationer ved brug af BYOD.

11.4 NIST SP 800-53 Rev.5:

11.4.1 AC-19 – Adgangsstyring for mobile enheder: Definerer grundlæggende beskyttelsesforanstaltninger, herunder kryptering, autentifikation og håndhævelse via MDM.

11.4.2 AC-17 – Fjernadgang: Kræver sikker autentifikation og beskyttelse af sessioner for mobile brugere med fjernadgang.

11.4.3 CM-7 – Mindst mulig funktionalitet: Understøtter fjernelse af unødvendige applikationer og funktioner fra mobile endepunkter for at reducere risiko.

11.4.4 MP-5 – Beskyttelse ved transport af medier: Regulerer sikker overførsel af data fra mobile systemer til eksterne destinationer eller cloudmiljøer.

11.4.5 SC-12 – Etablering og håndtering af kryptografiske nøgler: Kræver anvendelse af sikre kryptografiske protokoller til mobil kommunikation og lagring.

11.5 EU GDPR (2016/679):

11.5.1 Artikel 5(1)(f) – Integritet og fortrolighed: Kræver, at organisationer beskytter personoplysninger på mobile enheder mod uautoriseret eller ulovlig adgang.

11.5.2 Artikel 25 – Databeskyttelse gennem design og standardindstillinger: Kræver, at databeskyttelse indbygges i BYOD- og MDM-processer.

11.5.3 Artikel 32 – Behandlingssikkerhed: Kræver risikobaserede kontroller (f.eks. kryptering, autentifikation, adgangsstyring) for personoplysninger på mobile platforme.

11.6 EU NIS2-direktivet (2022/2555):

11.6.1 Artikel 21(2)(d): Kræver, at mobil adgang til kritiske systemer og oplysninger beskyttes gennem passende tekniske og organisatoriske foranstaltninger, såsom endepunktskontrol, kryptering og overvågning.

11.7 EU DORA (2022/2554):

11.7.1 Artikel 9 – Styringsramme for IKT-risici: Kræver, at virksomheder i den finansielle sektor begrænser risici ved mobil adgang og fjernadgang som led i operationel robusthed.

11.7.2 Artikel 10 – Sikkerhedskrav til IKT-systemer: Kræver sikker mobilarkitektur, overvågning og responsmekanismer for cybertrusler, der udspringer fra mobile enheder.

11.8 COBIT 2019:

11.8.1 APO13.02 – Etabler og vedligehold en informationssikkerhedsplan: Kræver, at brugen af mobile enheder, herunder BYOD, integreres i organisationens sikkerhedsstrategier.

11.8.2 DSS01.04 – Styr aktivkonfiguration og integritet: Gælder for konfigurationsstyring og sikker idriftsættelse af mobile enheder.

11.8.3 BAI09.01 – Etabler og vedligehold kontroller: Understøtter implementering af tekniske og proceduremæssige sikkerhedsforanstaltninger for sikker mobil drift og fjernarbejde.