| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Indsæt navnet på den registrerede juridiske enhed her | | | | | | | |
| Dokumentnummer:<br>P34S | | | | | Dokumenttitel:<br>**Politik for mobile enheder og BYOD** | | | | | | | |
| Version:<br>1.0 | | Ikrafttrædelsesdato:<br>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 regler

| Standard/regulering | Klausul/artikel | Kommentar |
|---|---|---|
| ISO/IEC 27001:2022 | Klausul 5.1, 5.2, 6.1, 6.2, 8 | Generelle krav til ISMS og kontroller for mobile enheder/BYOD |
| ISO/IEC 27002:2022 | Kontroller 5.10–5.13 | Detaljerede kontroller for mobile enheder/BYOD og fjernadgang |
| NIST SP 800-53 Rev. 5 | AC-19, AC-20, CM-6, MP-7 | Føderale kontroller for enheder, medier og konfiguration |
| EU's GDPR | Artikel 5(1)(f) | Beskyttelse af personoplysninger/mobile endepunkter |
| EU's NIS2-direktiv | Artikel 21(2)(d) | Beskyttelse af forretningskritiske enheder, herunder BYOD |
| EU's DORA | Artikel 9, 10 | IKT-risiko/forretningskontinuitet for mobile endepunkter |
| COBIT 2019 | APO13, DSS01, DSS05 | It-styring, drift og kontroller for sikkerhedstjenester |

**1. Formål**

1.1. Denne politik fastsætter de obligatoriske sikkerhedskrav for brug af mobile enheder, herunder smartphones, tablets og bærbare computere, ved adgang til virksomhedens oplysninger, systemer eller tjenester.

1.2. Politikken regulerer også brugen af Bring Your Own Device (BYOD) for at sikre, at kunde- og virksomhedsdata beskyttes, uanset hvem der ejer enheden.

1.3. Politikken håndhæver ensartede sikkerhedskontroller for mobil adgang, understøtter målsætningerne for ISO/IEC 27001-certificering og forebygger tab af data eller kompromittering som følge af mistede, stjålne eller fejlbenyttede mobile endepunkter.

1.4. Den sikrer, at både tekniske og proceduremæssige sikkerhedsforanstaltninger anvendes ved mobil brug i SMV'er uden dedikerede it-teams, herunder i miljøer med fjernarbejde og cloudbaserede tjenester.

**2. Omfang**

**2.1. Denne politik gælder for alle medarbejdere, kontrahenter, praktikanter og tjenesteudbydere, der:**

2.1.1. bruger en mobil enhed til at tilgå, behandle eller lagre virksomhedsdata eller systemer

2.1.2. forbinder til virksomhedens tjenester, herunder e-mail, delte mapper, cloudapplikationer eller interne systemer via VPN

**2.2. Politikken omfatter:**

2.2.1. alle mobile enheder: smartphones, tablets og bærbare computere (virksomhedsudstedte eller personlige BYOD-enheder)

2.2.2. alle operativsystemer (f.eks. iOS, Android, Windows, macOS)

2.2.3. alle lokationer (kontor, hjem, fjernarbejde, offentlige steder)

2.3. Politikken gælder på tværs af alle arbejdsmiljøer og skal håndhæves uanset ejerskabet til enheden.

## 3. Mål

3.1. Forebygge datatab: Sikre, at mobil brug ikke udsætter følsomme virksomheds- eller kundedata for uautoriseret adgang, tyveri eller misbrug.

3.2. Fastlægge klare regler for BYOD: Fastsætte ensartede betingelser for brug af personlige enheder til arbejdsformål og sikre juridiske og tekniske sikkerhedsforanstaltninger.

3.3. Understøtte efterlevelse af krav: Opfylde krav efter ISO/IEC 27001, GDPR, NIS2 og andre retlige forpligtelser gennem ensartet praksis for mobil sikkerhed.

3.4. Minimere driftsrisiko: Reducere sandsynligheden for driftsforstyrrelser som følge af misbrug, kompromittering eller svigt i mobile enheder.

3.5. Opretholde kundernes tillid: Dokumentere over for kunder og partnere, at deres data forbliver beskyttet, også når de tilgås fra mobile eller personlige enheder.

## 4. Roller og ansvar

### 4.1. Direktøren:

4.1.1. Har det overordnede ansvar for denne politik.

4.1.2. Godkender al brug af mobil adgang og BYOD-adgang til virksomhedens systemer.

4.1.3. Sikrer, at BYOD-aftaler underskrives, opbevares og følges op.

4.1.4. Verificerer, at den eksterne it-tjenesteudbyder håndhæver de krævede beskyttelsesforanstaltninger for mobile enheder.

### 4.2. Udpeget medarbejder eller it-support:

4.2.1. Bistår med opsætning, registrering og konfiguration af mobile enheder, der anvendes til arbejde.

4.2.2. Håndhæver adgangsstyring relateret til mobile enheder, applikationsbegrænsninger og overvågningskrav.

4.2.3. Understøtter håndtering af sikkerhedshændelser relateret til mobile enheder (mistede, stjålne eller kompromitterede enheder).

[ ... 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. Årlig gennemgang

9.1.1. Direktøren skal gennemgå denne politik mindst én gang hver 12. måned.

9.1.2. Gennemgangen skal verificere fortsat tilpasning til kravene i ISO/IEC 27001, udviklingen i mobile teknologier og ændringer i forretningsdriften.

9.1.3. Opdateringer skal også tage højde for nylige hændelser, revisionsresultater eller regulatoriske ændringer (f.eks. GDPR, NIS2, DORA).

### 9.2. Udløsende forhold for mellemliggende gennemgang

#### 9.2.1. Denne politik skal opdateres straks, hvis et af følgende forhold indtræffer:

9.2.1.1. Større mobilrelateret sikkerhedshændelse (f.eks. brud via en mistet eller kompromitteret enhed)

9.2.1.2. Ændring i understøttede platforme eller værktøjer til styring af mobile enheder

9.2.1.3. Retlig eller regulatorisk ændring, der påvirker brugen af personlige enheder eller databeskyttelse

9.2.1.4. Indførelse af nye applikationer, tjenester eller tredjepartsværktøjer, der anvendes på mobile enheder

### 9.3. Dokumentation af ændringer

9.3.1. Alle gennemgange og opdateringer skal dokumenteres, herunder dato for gennemgang, gennemførte ændringer og direktørens godkendelse

9.3.2. En versionshistorik skal opbevares til revisionsformål

**9.4. Kommunikation og adgang**

9.4.1. Direktøren skal sikre, at alle brugere (medarbejdere, kontrahenter, tredjeparter) informeres om ændringer

9.4.2. Opdaterede versioner skal være let tilgængelige, f.eks. i delte mapper eller på interne platforme

**10. Relaterede politikker og sammenhænge**

**10.1. Denne politik indgår i den samlede politikportefølje for informationssikkerhed i SMV'er og skal implementeres sammen med følgende:**

10.1.1. P4S – Politik for adgangskontrol: Fastlægger krav til styring af sikker adgang til systemer, herunder systemer der tilgås via mobile enheder. Håndhæver adgangskodehygiejne og sessionskontroller.

10.1.2. P8S – Politik for informationssikkerhedsbevidsthed og uddannelse: Sikrer, at brugere modtager træning i sikker brug af mobile enheder, rapportering af hændelser og BYOD-betingelser.

10.1.3. P17S – Politik for databeskyttelse og privatliv: Fastlægger GDPR-kompatibel håndtering af personoplysninger og virksomhedsdata på mobile platforme, især når personlige enheder anvendes til arbejde.

10.1.4. P9S – Politik for fjernarbejde: Er tilpasset kravene til mobil brug ved arbejde uden for organisationens lokationer eller hjemmefra, herunder håndtering af enheder og sikkerhedsforanstaltninger for netværksadgang.

10.1.5. P30S – Politik for hændelseshåndtering: Fastlægger rammen for håndtering af mobilrelaterede hændelser, herunder kompromitterede eller mistede enheder.

10.2. Disse relaterede politikker udgør samlet et fuldstændigt sæt sikkerhedskontroller for mobile enheder i SMV'er uden dedikeret it-personale og sikrer håndhævelse, gennemsigtighed og revisionsberedskab.

**11. Referencestandarder og rammeværker**

11.1. Denne politik understøtter fuld tilpasning til følgende sikkerheds- og efterlevelsesstandarder:

**11.2. ISO/IEC 27001:**

11.2.1. Klausul 5.1 – Leadership and Commitment: Sikrer ledelsesmæssigt tilsyn og ansvarlighed for mobil adgang og BYOD-adgang

11.2.2. Klausul 6.1 – Actions to Address Risks: Kræver, at risici ved mobil sikkerhed vurderes og behandles

11.2.3. Klausul 8.1 – Operationel planlægning og styring: Kræver ensartede procedurer for mobil adgang for at beskytte virksomhedsdata

**11.3. ISO/IEC 27002:**

11.3.1. Kontroller 5.10 (Use of Mobile Devices), 5.11 (Teleworking), 5.12 (Remote Access) og 5.13 (BYOD): Giver implementeringsvejledning til styring af enhedsrisici i en mindre virksomhedskontekst

**11.4. NIST SP 800-53 Rev. 5:**

11.4.1. AC-19 – adgangskontrol for mobile enheder: Kræver sikkerhedsindstillinger for godkendt mobil brug

11.4.2. AC-20 – brug af eksterne systemer: Regulerer risici ved BYOD og fjernadgang

11.4.3. CM-6 – konfigurationsindstillinger: Håndhæver sikre standard- og tilpassede indstillinger på mobile platforme

11.4.4. MP-7 – brug af medier: Omhandler korrekt brug og begrænsninger for mobil lagring og dataadgang

**11.5. EU's GDPR (2016/679):**

11.5.1. Artikel 5(1)(f) – integritet og fortrolighed: Kræver beskyttelse af data gennem passende sikkerhed for personoplysninger, især på mobile platforme

11.5.2. Artikel 32 – behandlingssikkerhed: Forpligter til anvendelse af passende tekniske og organisatoriske foranstaltninger for at sikre data, der tilgås eller lagres på mobile enheder

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

11.6.1. Artikel 21(2)(d) – sikkerhedsforanstaltninger for enheder: Kræver sikkerhedskontroller for hardware og software, der anvendes til adgang til kritiske forretningssystemer, herunder personlige enheder

**11.7. EU's DORA (2022/2554):**

11.7.1. Artikel 9 – styringsramme for IKT-risiko: Kræver beskyttelse af mobile endepunkter, der anvendes til kritisk forretningskommunikation og cloudtjenester

11.7.2. Artikel 10 – IKT-forretningskontinuitet: Håndhæver fortsat sikker adgang til forretningssystemer, også under driftsforstyrrelser eller fjernarbejde

**11.8. COBIT 2019:**

11.8.1. APO13 – Manage Security: Kræver, at organisationen håndhæver politikker for mobile enheder og BYOD i overensstemmelse med virksomhedens risikobillede

11.8.2. DSS01 – Manage Operations: Sikrer teknisk implementering af mekanismer for sikker adgang

11.8.3. DSS05 – Manage Security Services: Regulerer tredjeparters involvering i opretholdelse af sikre mobile miljøer og koordinering af hændelseshåndtering