Bilag 6: Krav til IT-udstyr

1. PC-udstyr

Godkendte mærker
• Der må kun anvendes business-godkendte pc-mærker: HP og Lenovo (Varde Kommune benytter HP og Lenovo)

Operativsystem og opdateringer
• PC'er skal være opdateret til seneste tilgængelige Windows-version (pt. Windows 11).
• Sikkerhedsopdateringer skal installereres løbende.
• Kritiske sikkerhedsopdateringer skal installeres inden for 72 timer efter frigivelse.
• Øvrige opdateringer skal installeres inden for 30 dage.

Sikkerheds- og driftskrav
•Enheder skal være fuldt krypteret (BitLocker).
•Enheder må ikke kunne modificeres uden om producentens understøttede funktioner.
•Adgang til systemer må kun ske via sikre protokoller (TLS 1.2/1.3).
•Det er et krav, at leverandørens medarbejdere melder sig til og benytter 2-faktor godkendelse ved log on i form af Microsoft Authenticator app.
•For FMK og medicinhåndtering i Nexus skal brugeren autentificeres på NSIS-sikringsniveau Betydelig. - Dette opnås gennem MitID Erhverv med 2-faktor-autentifikation, som både sikrer identitetens troværdighed og opfylder NSIS-kravene for adgang til sundhedsfaglige funktioner.
•Der skal være en Geoblocking politik (Conditional Access), så man ikke kan tilgå systemet fra andre lande end Danmark og der skal være MFA politik når man tilgår fra Danmark.

2. Mobiltelefoner og iPads

2.1 Godkendte producenter

• Enheder fra kinesiske producenter må ikke anvendes.
• Tilladte producenter: Samsung, Google og Apple.

2.2 Generelle krav

• Android-tablets må ikke anvendes.
• Enheder skal som minimum være én OS- og sikkerhedsversion bagud i forhold til producentens seneste version.
• Enheder skal være personligt udleveret og må ikke anvendes privat.
• Enheder må ikke konfigureres som dele-enheder.

3. Sikkerhedskrav for PC og mobil/iPad

3.1 Adgangskontrol

• Pinkode på minimum 6 cifre.
• Skærmlås skal aktiveres efter senest 5 min ved inaktivitet.
• Pinkode må ikke kunne fjernes.
• Biometrisk login må kun bruges som supplement til PIN.

3.2 Systemintegritet

• Enheder må ikke kunne rootes eller køre uautoriserede versioner af OS.
• Jailbreak/root-detektion skal være aktiv og skal blokere adgang ved fund.

3.3 Kryptering og databeskyttelse

• Enheder skal være fuldt krypteret (Android FBE / iOS Data Protection / Bitlocker).
• Kryptering må ikke kunne deaktiveres.
• Kommunens data må ikke kunne kopieres til private apps eller tjenester.
• Det må ikke være muligt at opsætte private konti f.eks. Gmail- eller iCloud.
• Clipboard-deling mellem privat og arbejdsprofil skal være deaktiveret.

3.4 Applikationskontrol

• Installation af ikke-arbejdsrelaterede apps skal være blokeret.

3.5 Netværks- og kommunikationssikkerhed

• Adgang til kommunens systemer må kun ske via sikre forbindelser (TLS 1.2/1.3).
• Offentlige, usikre Wi-Fi-netværk må ikke anvendes til at tilgå systemer uden sikker tunnel/VPN

4. Krav til MDM-styring (mobil/iPad)

• Enheder skal administreres via et Mobile Device Management (MDM) system.
• Enheden skal være enroll'et før den anvendes til kommunal opgaveløsning.
• Brugeren må ikke kunne fjerne MDM-profilen eller deaktivere politikker.
• Enheden skal rapportere compliancestatus løbende.
• Manglende compliance skal automatisk blokere adgang til kommunens systemer.

5. Opdateringskrav for mobil/iPad

• Enheder skal være opdateret til seneste tilgængelige OS- og sikkerhedsopdateringer.
• Kritiske opdateringer: maks. 72 timer.
• Øvrige sikkerhedsopdateringer: maks. 30 dage.

6. Fjernsletning og hændelseshåndtering

• Enheder skal kunne fjernslettes med Mobile Device Management (MDM)
• Leverandøren skal straks og senest inden for 4 timer rapportere bortkomst, tyveri eller potentiel kompromittering.

• Leverandøren skal dokumentere og beskrive sin procedure for håndtering af sikkerhedshændelser, herunder hvordan hændelser opdages, klassificeres, eskaleres og indrapporteres

7. Leverandørens ansvar (NIS2)

7.1 Risikovurdering

• Leverandøren skal årligt gennemføre en IT-risikovurdering for medarbejdernes brug af udstyr og adgang til kommunens systemer.
• Dokumentation skal kunne fremvises på anmodning.

7.2 Beredskab og driftskontinuitet

• Leverandøren skal have en beredskabsplan og forretningskontinuitetsplan (BCP).
• Leverandøren skal kunne dokumentere, at arbejdet kan fortsætte ved enhedstab eller systemproblemer.
• Leverandøren skal sikre hurtig erstatning af defekte eller kompromitterede enheder.

7.3 Adgangsstyring

• Leverandøren skal sikre principper om least privilege.
• Medarbejdere må kun have adgang til de systemer, der er nødvendige for opgaven.
• Adgang skal straks fjernes når en medarbejder ikke længere udfører opgaven.

7.4 Logning og rapportering

• Leverandøren skal føre log over sikkerhedsrelevante hændelser.
• Logdata skal kunne udleveres til Varde Kommune ved forespørgsel.
• Leverandøren skal årligt indsende dokumentation for efterlevelse af kravene (compliance-erklæring).

7.5 Underleverandører

• Leverandøren skal oplyse brug af evt. underleverandører.
• Underleverandører skal leve op til samme sikkerhedskrav.
• Leverandøren er ansvarlig for underleverandørens efterlevelse.