



Riktlinje för användning för mobila enheter

Riktlinjen är ett komplement till förvaltningens riktlinjer för informationssäkerhet.

Beslutat av: Omsorgsdirektör
Datum: 20220110
Revideras av: Administrativa avdelningen
Dokumentets giltighet: 2021 - tillsvidare
Dokumentet gäller för: Alla verksamheter
Dokumentansvarig: Administrativa avdelningen

Inledning

Information som Vård- och omsorgsförvaltningen behöver för att lösa sina uppgifter är många gånger både känslig och kritisk till sin natur och finns i alla våra verksamheter. Vård- och omsorgsförvaltningens kunder förväntar sig att vi behandlar information på ett betryggande sätt och att vi har tillgång till nödvändig information även i händelse av krissituationer.

Vård- och omsorgsförvaltningen äger de mobila enheter* som tillhandahålls medarbetaren för användning i tjänsten.

Arbetsgivaren har rätt att ta del av information i enheter tillhörande Vård- och omsorgsförvaltningen – t.ex. e-post, sms, foton och kalenderanteckningar – om det är nödvändigt för att förvaltningen ska uppfylla sin skyldighet enligt offentlighets- och sekretesslagen.

Förvaltningen kan även ta del av de uppgifter som finns i den mobila enheten om det är nödvändigt vid fara för informationssäkerhetsbrott, t.ex. vid virus- eller hackerattacker eller för att utreda eller förhindra brott.

Riktlinje för användning av mobil enhet

Ansvar och uppföljning

- Tillämpning och uppföljning av Riktlinje för användning av mobil enhet tillfaller chefer på alla nivåer.

Instruktion

- Innan mobil enhet lämnas ut till medarbetare ska denne genomgått Grundutbildning GDPR och Digital informationssäkerhet för alla - DISA på HBG Learns.
- Den mobila enheten ska hanteras på ett sätt som minimerar risken för att obehöriga får tillgång till den, att den stjäls eller går förlorad. Anmäl omedelbart förlust av mobil enhet till närmaste chef.
- Den mobila enheten ska skyddas av unikt lösenord/pinkod och får inte tas bort.
- Användaridentiteter, PIN-kod, lösenord är personliga och får inte lånas ut.
- Vid misstanke om att ett lösenord eller PIN-kod kommit i fel händer eller tappats bort ska du omgående rapportera till din närmaste chef så att de kan spärras och bytas ut.
- Installera bara appar som behövs i tjänsten
- Känsliga personuppgifter och annan information som omfattas av sekretess får endast hanteras i appar som har godkänts för ändamålet.
- Använd aldrig din privata mail i arbetet.
- Använd aldrig din tjänstemail i privata syften
- Samtal som rör känsliga personuppgifter och annan information som omfattas av sekretess ska utföras så att inte obehöriga kan ta del av samtalet.

* mobiltelefon, surfplattor, etc.