Riktlinjer

2025-01-20

Diarienummer: 2024/637

Mittuniversitetet
MID SWEDEN UNIVERSITY

Riktlinjer för den digitala arbetsplatsen

Publicerad: 2025-01-27

Beslutsfattare: Helena Wallskog

Ansvarig funktion: Chef för infrastrukturavdelningen

Handläggare: Sonja Balaz

Beslutsdatum: 2025-01-23

Giltighetstid: Tills vidare

Senaste översyn: Ny anpassad riktlinje

Sammanfattning: Den digitala arbetsplatsen på Mittuniversitetet samlar de verktyg, applikationer och plattformar som medarbetare behöver för att arbeta effektivt, oavsett enhet eller plats. I och med att användningen av digitala enheter – såsom smarta telefoner, surfplattor, skärmar, bärbara och stationära datorer – ökar, ställs högre krav på hur dessa enheter hanteras. Eftersom de möjliggör arbete utanför universitetets IT-infrastruktur, är det avgörande att säkerställa en korrekt och säker hantering för att skydda både information och enheter.

Tidigare versioner: Dokumentet ersätter Riktlinjer för mobila enheter, dnr 2019/1975 och Regler för Mittuniversitetets arbetsredskap 2015/1226.

Riktlinjer

Datum: 2025-01-20

Diarienummer: 2024/637

Innehållsförteckning

Inledning

Den digitala arbetsplatsen på Mittuniversitetet samlar de verktyg, applikationer och plattformar som medarbetare behöver för att arbeta effektivt, oavsett enhet eller plats. I och med att användningen av digitala enheter – såsom smarta telefoner, surfplattor, skärmar, bärbara och stationära datorer – ökar, ställs högre krav på hur dessa enheter hanteras. Eftersom de möjliggör arbete utanför universitetets IT-infrastruktur, är det avgörande att säkerställa en korrekt och säker hantering för att skydda både information och enheter.

Enligt Myndigheten för samhällsskydd och beredskaps föreskrifter om säkerhetsåtgärder i informationssystem för statliga myndigheter (MSBFS 2020:7), § 21 ska myndigheten skydda den utrustning som informationssystem består av mot skador och obehörig åtkomst, genom att ha interna regler för hur digitala enheter ska skyddas.

Riktlinjerna för den digitala arbetsplatsen gäller för samtliga medarbetare på Mittuniversitet. Till riktlinjerna finns råd och rekommendationer på medarbetarsidorna på miun.se, som beskriver hur du som användare bör agera och hantera din utrustning i olika situationer.

1 Efterlevnad och uppföljning

Riktlinjerna följs upp av Infrastrukturavdelningen genom interna kontroller. Infrastrukturavdelningen ansvarar för förvaltningen och uppdateringen av riktlinjerna.
Prefekt/chef/motsvarande ansvar för att informera om och följa upp efterlevnad av riktlinjerna vid sin institution eller avdelning. Detta gäller även om annan intern eller extern part anlitas för uppdrag.

2 Från anskaffning till avveckling

En säker hantering av utrustningar omfattar hela enhetens livscykel, från anskaffning till avveckling. Alla inköp ska göras enligt riktlinjer för inköp och hanteras via universitetets serviceportal (NSP). För avveckling (utrangering) finns stöd och information i serviceportalen.

- Ett standardsortiment för digitala enheter finns för personal, och beställningar sker via Infrastrukturavdelningen
- Alla enheter och skärmar ska vara stöldskyddsmärkta
- Stöldbegärliga förbrukningsinventarier ska alltid registreras i myndighetens inventariesystem
- Privat inköp av denna utrustning får inte ske utanför Mittuniversitetets rutiner

- Utrustning som inte längre används ska återlämnas till Servicecenter för återanvändning eller avveckling
- Vid tjänstledighet längre än sex månader eller avslut av anställning ska all utrustning återlämnas

Infrastrukturavdelningen ansvarar för att skrota utrangerade enheter på ett säkert och hållbart sätt.

3 Installation och konfiguration

Alla tekniska arbetsredskap från Mittuniversitetet har en grundkonfiguration som utgår från användarens behov och universitetets säkerhetsriktlinjer.

- Digitala enheter (t.ex. mobiltelefoner, surfplattor, datorer) manageras centralt. Detta innebär hantering av applikationer, inställningar, inventering, samt fjärrensning av enheter eller specifika data vid behov
- I grundkonfigurationen ingår bland annat verktyg för licensinventering och kontroll av installerade applikationer
- Om det finns behov av program eller IT-tjänster utöver standardprogrammen ska en beställning göras i serviceportalen för att säkerställa rätt licensiering
- Vid särskilda behov kan administrationsrättigheter på användarens dator aktiveras, men detta kräver en ansökan. Administratören ansvarar för att datorn och eventuella egeninstallerade program hanteras i enlighet med Mittuniversitets riktlinjer
- Användare får endast ladda ner applikationer från officiella källor

4 Användning och lagring

Medarbetare ska vara medvetna om hur de får använda sina digitala enheter. En digital enhet ska betraktas som ett osäkert media att lagra information på. Medarbetaren ansvarar för att information på enheten hanteras och skyddas på ett säkert sätt.

- Digitala enheter är avsedda för tjänsterelaterade aktiviteter
- Utrustningen får inte användas enbart för privat bruk och får inte lånas ut
- Användare som använder privat utrustning för åtkomst till Mittuniversitetets tjänster ansvarar för att följa gällande riktlinjer
- Information ska hanteras och lagras enligt Mittuniversitetets fastställda rutiner
- Handlingar som är av ringa betydelse eller har överförts till annan mediabärare ska gallras enligt Mittuniversitetets Informationshanteringsplan, med stöd av RA-FS 2021:6

5 Mobilabonnemang

Mobilabonnemang som tillhandahålls av Mittuniversitetet ska användas enligt följande riktlinjer:

- Samtliga mobilabonnemang är spärrade för betalsamtal
- Arbetsmobilen ska vara kopplad till ett arbetsmobilabonnemang
- Telefonnummer måste visas vid utgående samtal
- Vidarekoppling av arbetsnummer till privat telefon under längre perioder är inte tillåtet
- Röstbrevlådan ska avlyssnas kontinuerligt
- Internetdelning får inte användas som privat internetanslutning eller för att ge internetaccess till personer utanför Mittuniversitetet
- Stora avvikelser i förbrukning följs upp av närmsta chef/prefekt/motsvarande

6 Säkerhet

För att skydda information som lagras på digitala enheter ska säkerhetsåtgärder vidtas:

- Enheterna ska skyddas med ett säkert skärmlås
- Utrustning ska inte anslutas till okända trådlösa nätverk. Eduroam är ofta tillgängligt på andra lärosäten, flygplatser, järnvägsstationer och liknande platser, och bör användas som ett säkert alternativ
- Enheterna ska uppdateras när tillgängliga uppdateringar finns
- Manipulering av enhetens grundfunktionalitet för att få högre behörighet är förbjudet
- Vid förlust eller misstänkt manipulering ska IT-support omedelbart kontaktas, och lösenord ska bytas
- Universitetets VPN-tjänst bör användas vid anslutning från externa nätverk

6.1 Resor

- Följ gällande rutiner för hantering av digitala enheter vid resor
- Tänk på kostnadsbilden för datatjänster och mobiltelefoni vid resor utomlands

6.2 Särskilda regler för resor till högriskländer

- Vid tjänsteresor till länder med osäkra eller högriskmiljöer får inte befintlig utrustning tas med då det finns en stor risk att dessa enheter kan bli föremål för inspektion, dataavläsning eller cyberattacker
- Inför resan kan specialpreparerade enheter från IT-support lånas ut Detta genom att lägga en beställning i Serviceportalen

- Lånad utrustning ska återlämnas omedelbart efter hemkomst
- Under inga omständigheter får dessa enheter kopplas upp mot Mittuniversitetets nätverk