Riktlinjer

2025-01-20

Reference number: 2024/637

Mittuniversitetet
MID SWEDEN UNIVERSITY

Guidelines for the Digital Workplace

Published: 2025-01-27

Policy makers: Helena Wallskog

Responsible function: Head of Infrastructure Department

Administrator: Sonja Balaz

Date of decision: 2025-01-23

Duration: For the time being

Last review: New adapted guideline

Summary: The digital workplace at Mid Sweden University brings together the tools, applications and platforms that employees need to work efficiently, regardless of device or location. As the use of digital devices – such as smartphones, tablets, screens, laptops and desktops – increases, there are higher demands on how these devices are managed. As they enable work outside the University's IT infrastructure, it is crucial to ensure proper and secure management to protect both information and devices.

Previous versions: The document replaces the Guidelines for Mobile Devices, ref. 2019/1975 and the Rules for Mid Sweden University's Work Tools 2015/1226.

Riktlinjer
Date 2025-01-20
Reference number: 2024/637

Contents

Introduction

The digital workplace at Mid Sweden University brings together the tools, applications and platforms that employees need to work efficiently, regardless of device or location. As the use of digital devices – such as smartphones, tablets, screens, laptops and desktops – increases, there are higher demands on how these devices are managed. As they enable work outside the University's IT infrastructure, it is crucial to ensure proper and secure management to protect both information and devices.

According to the Swedish Civil Contingencies Agency’s regulations on security measures in information systems for state authorities (MSBFS 2020:7), Section 21, the authority must protect the equipment that constitutes information systems against damage and unauthorised access by having internal rules for how digital devices are to be protected.

The guidelines for the digital workplace apply to all employees at Mid Sweden University. The guidelines contain advice and recommendations

on the employee pages at miun.se, which describe how you as a user should act and manage your equipment in different situations.

1 Compliance and follow-up

The guidelines are followed up by the Infrastructure Department through internal controls. The Infrastructure Department is responsible for the management and updating of the guidelines.
Head of department/manager/corresponding responsibility for informing about and following up on compliance with the guidelines at their department or department. This also applies if another internal or external party is engaged for assignments.

2 From acquisition to decommissioning

The safe handling of equipment covers the entire life cycle of the unit, from procurement to decommissioning. All purchases must be made in accordance with purchasing guidelines and handled through the University's service portal (NSP). For decommissioning (decommissioning) support and information is available in the service portal.

- A standard range of digital devices is available for staff, and orders are placed via the Infrastructure Department
- All devices and screens must be anti-theft marked
- Theft-prone consumables must always be registered in the authority’s inventory system
- Private purchase of this equipment may not take place outside Mid Sweden University's routines
- Equipment that is no longer in use shall be returned to the Service Center for reuse or decommissioning
- In the event of leave of absence of more than six months or termination of employment, all equipment shall be returned:

The Infrastructure Department is responsible for scrapping decommissioned units in a safe and sustainable manner.

3 Installation and configuration

All technical work tools from Mid Sweden University have a basic configuration based on the user's needs and the University's safety guidelines.

- Digital devices (e.g. mobile phones, tablets, computers) are centrally managed. This involves managing applications, settings, inventory, as well as remotely wiping devices or specific data when needed

- The basic configuration includes tools for license inventory and control of installed applications
- If there is a need for software or IT services in addition to the standard software, an order must be placed in the service portal to ensure proper licensing
- In case of special needs, administration rights on the user's computer can be activated, but this requires an application. The administrator is responsible for ensuring that the computer and any self-installed programs are managed in accordance with Mid Sweden University's guidelines.
- Users may only download applications from official sources

4 Use and storage

Employees should be aware of how they are allowed to use their digital devices. A digital device shall be regarded as an insecure medium on which to store information. The employee is responsible for ensuring that information on the device is handled and protected in a safe manner.

- Digital devices are intended for service-related activities
- The equipment may not be used solely for private purposes and may not be lent
- Users who use private equipment to access Mid Sweden University's services are responsible for following current guidelines
- Information shall be handled and stored in accordance with Mid Sweden University's established procedures
- Documents that are of minor importance or have been transferred to another media carrier must be screened in accordance with Mid Sweden University's Information Management Plan, with the support of RA-FS 2021:6

5 Mobile subscriptions

Mobile subscriptions provided by Mid Sweden University shall be used according to the following guidelines:

- All mobile subscriptions are blocked for paid calls
- Work mobile must be linked to a work mobile subscription
- Phone numbers must be displayed on outgoing calls
- Forwarding of work numbers to private telephone for extended periods is not allowed
- The voice mail shall be continuously intercepted
- Internet sharing may not be used as a private internet connection or to provide internet access to people outside Mid Sweden University
- Large discrepancies in consumption are followed up by the nearest manager/head of department/equivalent

6 Security

In order to protect information stored on digital devices, security measures shall be taken:

- Devices should be protected with a secure screen lock
- Equipment should not be connected to unknown wireless networks. Eduroam is often available at other universities, airports, railway stations and similar locations, and should be used as a safe alternative
- The devices shall be updated when available updates are available
- Manipulation of the basic functionality of the device to gain higher privileges is prohibited
- In case of loss or suspected tampering, IT support should be contacted immediately, and passwords should be changed
- The University's VPN service should be used when connecting from external networks

6.1 Travel

- Follow current procedures for managing digital devices when travelling
- Consider the cost of data services and mobile telephony when travelling abroad

6.2 Special rules for travel to high-risk countries

- During missions to countries with unsafe or high-risk environments, existing equipment may not be included as there is a high risk that these devices may be subject to inspection, data reading or cyber-attacks.
- Before the trip, specially prepared devices from IT support can be lent This by placing an order in the Service Portal
- Borrowed equipment must be returned immediately upon return
- Under no circumstances may these devices be connected to Mid Sweden University's network