# Mobile Devices

| CCR_SEC_04 |
| --- |
| Rev. 01 24/08/2025 |

This document establishes requirements and guidelines for the use of mobile computing devices (smartphones, tablets, laptops), whether personally owned or owned by third parties (BYOD – Bring Your Own Device) or provided by INFN (COPE – Corporate-Owned, Personally Enabled), for accessing INFN IT resources.

Its objective is to preserve information security, ensure compliance with the INFN IT Resources Regulation, and promote responsible use of INFN IT resources, while at the same time ensuring maximum flexibility for staff work activities.

## 1. Scope

This Regulation applies to all individuals who have been granted access to INFN IT resources and who access such resources via COPE or BYOD devices.

## 2. General Provisions

The use of BYOD devices for work-related activities is permitted, including access to email, documents and services, to the wired and wireless networks of INFN Operating Units, in compliance with the guidelines set out below.

COPE devices may be used for personal activities within the limits defined in the INFN Regulation on the Use of IT Resources.

When using COPE devices (at all times) and BYOD devices when connected to INFN networks (wired, wireless, or via VPN), it is mandatory to fully comply with the provisions set out in the INFN Regulation on the Use of IT Resources, in particular with regard to the prohibition of illegal activities, activities contrary to accepted network and service usage practices, or activities that may harm the reputation of the Institute.

Unless explicitly stated otherwise, the following provisions shall be considered mandatory for COPE devices and recommended guidelines for BYOD devices.

## 3. Device protection

- it is not permitted to create user accounts other than the personal account on the device;
- accounts must not be shared (mandatory also for BYOD devices);
- in the case of BYOD devices, the creation of additional privileged accounts is strongly discouraged;
- access to the device must be protected by a sufficiently complex password or PIN, or by biometric authentication (mandatory also for BYOD devices);
- the device must be locked when left unattended, and automatic lock due to inactivity must be configured (mandatory also for BYOD devices);
- the theft or loss of a COPE device must be immediately reported to the relevant IT resources responsible team; in case of BYOD devices, reporting is required only if the device has been registered for direct connection to INFN networks.

## 4. System and Software Security

- the operating system and applications installed on the device must always be kept up to date with the latest available releases.
- applications must be installed exclusively from certified repositories, such as the Apple App Store, Microsoft Store, or Google Play.
- COPE devices must be associated with the INFN Microsoft XDR protection platform in accordance with the instructions provided by the relevant IT resources responsible team.
  For BYOD devices, the installation of antivirus/anti-malware protection software is strongly recommended.
- it is not permitted to circumvent the security configurations of the device.

## 5. Data Security

- where possible, disk and data encryption must be configured on the device;
- access to INFN data and documents must be carried out exclusively using secure protocols or applications (mandatory also for BYOD devices);
- it is not permitted to store INFN documents and data on unauthorized external cloud services (mandatory also for BYOD devices);
- backup copies of the device and of the data and configurations contained therein may be stored only in end-to-end encrypted form.
  Where device backups include INFN data, documents, or credentials, this requirement is mandatory also for BYOD devices.

## 6. Network access

- the use of unencrypted wireless networks to access INFN resources is discouraged.
  Where necessary, such networks may be used provided that an INFN-provided VPN connection is activated or that access to INFN resources is carried out exclusively through encrypted protocols;

- access to wired local networks is permitted only following identification of the device (e.g. MAC address registration) or of the user (e.g. 802.1X), in accordance with the procedures defined by the relevant IT resources responsible team (mandatory also for BYOD devices).