Dispositivi mobili

CCR_SEC_04
Rev. 01 24/08/2025

Questo documento stabilisce prescrizioni o linee guida per l'utilizzo di strumenti informatici di tipo mobile (smartphone, tablet, portatili) di proprietà personale o di terzi (BYOD) o forniti dall'INFN (COPE) per accedere a risorse informatiche dell'INFN.

L'obiettivo è di preservare la sicurezza informatica, la conformità al disciplinare e l'utilizzo responsabile delle risorse informatiche dell'INFN, garantendo al contempo la massima flessibilità per il lavoro delle persone.

1. Ambito

Il presente Disciplinare si applica a tutti coloro cui sia stato consentito l'accesso alle risorse informatiche dell'INFN e che accedono a tali risorse attraverso l'uso di dispositivi COPE o BYOD.

2. Disposizioni generali

È consentito l'utilizzo di dispositivi BYOD per svolgere attività lavorative, inclusi l'accesso alla posta elettronica, a documenti e servizi, alle reti wired e wireless delle strutture, nel rispetto delle linee guida sotto riportate.

I dispositivi COPE possono essere utilizzati per attività personali nei limiti descritti nel disciplinare di utilizzo delle risorse informatiche dell'INFN.

Nell'uso dei dispositivi COPE (sempre) e dei dispositivi BYOD quando connessi alle reti INFN (cablata, wireless o tramite VPN) è obbligatorio rispettare integralmente le prescrizioni riportate nel disciplinare di utilizzo delle risorse informatiche dell'INFN, in particolare in relazione al divieto di svolgere attività illegali o contrarie alle consuetudini d'uso delle reti e servizi acceduti o attività che possano nuocere alla reputazione dell'Ente.

Ove non esplicitamente indicato, le seguenti disposizioni vanno intese come obbligatorie per i dispositivi COPE, e come linee guida consigliate per i dispositivi BYOD.

3. **Protezione del dispositivo**

- non è consentito creare utenze oltre a quella personale sul dispositivo;
  nel caso di dispositivo BYOD è fortemente sconsigliata la creazione di altre utenze privilegiate;
- l'account non deve essere condiviso (obbligatorio anche per dispositivi BYOD).
- l'accesso al dispositivo deve essere protetto da password o da PIN adeguatamente complessi o da autenticazione biometrica (obbligatorio anche per dispositivi BYOD);
- l'accesso al dispositivo deve essere bloccato se lasciato incustodito, e deve essere configurata la modalità di blocco automatico per inattività (obbligatorio anche per dispositivi BYOD);
- il furto o la perdita del dispositivo COPE devono essere immediatamente segnalati al team responsabile delle risorse informatiche di riferimento;
  nel caso di dispositivi BYOD la segnalazione deve essere fatta solo se il dispositivo è stato registrato per la connessione diretta alle reti INFN

4. Sicurezza del sistema e del software

- Il sistema operativo e le app installate sul dispositivo devono essere sempre aggiornati all'ultima release disponibile;
- l'installazione delle app deve avvenire da repository certificati, come ad esempio, Apple Store, Windows Store e Google Play;
- il dispositivo COPE deve essere associato alla piattaforma di protezione Microsoft XDR dell'INFN secondo le istruzioni del team responsabile delle risorse informatiche di riferimento;
  sul dispositivo BYOD è fortemente consigliata l'installazione di uno strumento di protezione da virus/malware;
- non è consentito aggirare le configurazioni di sicurezza del dispositivo;

5. Sicurezza dei dati

- sul dispositivo ove possibile deve essere configurata la criptazione del disco e dei dati;
- l'accesso a dati e documenti INFN deve essere fatto esclusivamente utilizzando protocolli o app sicuri (obbligatorio anche per BYOD);
- non è consentito salvare documenti e dati INFN su cloud esterne non autorizzate (obbligatorio anche per BYOD);
- è consentito salvare copie di backup del dispositivo e di dati e configurazioni ivi contenuti solo in forma criptata end-to-end;
  se il backup del dispositivo include dati, documenti o credenziali INFN, la disposizione è obbligatoria anche per dispositivi BYOD;

6. Accesso alla rete

- È sconsigliato l'utilizzo di reti wireless non crittografate per accedere a risorse dell'INFN; in caso di necessità è consentito farne uso a patto di attivare una connessione VPN messa a disposizione dall'INFN o di utilizzare per l'accesso a risorse INFN esclusivamente protocoli criptati
- L'accesso a reti locali cablate è consentito solo previa identificazione del dispositivo (es: registrazione del MAC address) o dell'utente (es: 802.1X), secondo le procedure definite dal team responsabile delle risorse informatiche di riferimento (anche per device BYOD);