**ISTITUTO COMPRENSIVO STATALE SAN VERO MILIS**
Via Umberto I n. 12 - 09070 - SAN VERO MILIS
Tel. 0783 53670– C.F. 90027760959 codice univoco UFG2N4
Codice iPA istsc_oric81200v e-mail oric81200v@istruzione.it pec oric81200v@pec.istruzione.it
sito web: www.icsanveromilis.edu.it

ISTSC_ORIC81200V.A660A55.REGISTRO PROTOCOLLO.U.0005893.02-05-2026

# Norme di comportamento del dipendente nelle attività lavorative svolte nella modalità di lavoro agile

Si portano a conoscenza del personale che svolge la propria attività in modalità di lavoro agile le raccomandazioni elaborate da Cert-PA di AgID per il rispetto delle misure minime di sicurezza informatica per le pubbliche amministrazioni fissate dalla circolare 17 marzo 2017, n. 1 che devono essere garantite anche dal personale che svolge la propria attività lavorativa da remoto:

1. Seguire prioritariamente le policy e le raccomandazioni dettate dalla propria Amministrazione
2. Utilizzare i sistemi operativi per i quali attualmente è garantito il supporto (non utilizzare, ad esempio, macchine con sistema operativo windows XP o windows 7 di cui microsoft ha terminato il supporto)
3. Effettuare costantemente gli aggiornamenti di sicurezza del tproprio sistema operativo
4. Assicurarsi che i software di protezione del proprio sistema operativo (Firewall, Antivirus, ecc) siano abilitati e costantemente aggiornati
5. Assicurarsi che gli accessi al sistema operativo siano protetti da una password sicura di almeno 8 caratteri contenente almeno una lettera maiuscola, un numero ed un carattere speciale
6. Non installare software proveniente da fonti/repository non ufficiali
7. Bloccare l'accesso al sistema e/o configurare la modalità di blocco automatico quando ti allontani dalla postazione di lavoro
8. Non cliccare su link o allegati contenuti in email sospette
9. Utilizzare l'accesso a connessioni Wi-Fi adeguatamente protette
10. Collegarsi a dispositivi mobili (pen-drive, hdd-esterno, etc) di cui si conosce la provenienza (nuovi, già utilizzati, forniti dalla propria Amministrazione)
11. Effettuare sempre il log-out dai servizi/portali utilizzati dopo aver concluso la sessione lavorativa.

Si coglie l'occasione per dare le seguenti ulteriori disposizioni:

- Assicurarsi che il sistema operativo e tutti i software utilizzati per lo svolgimento del lavoro, compresi gli antivirus, siano sempre aggiornati all'ultima versione disponibile. Gli aggiornamenti di sicurezza sono cruciali per proteggere i dati da nuove minacce e vulnerabilità.

- Nel caso in cui si utilizzi un PC personale per svolgere l'attività lavorativa, prima del suo primo utilizzo, installare un buon antivirus e fare una accurata scansione preventiva per rimuovere qualunque software malevolo
- Non memorizzare sui dispositivi le password di accesso alle piattaforme ed ai sistemi utilizzati per il lavoro a distanza
- Non memorizzare sul client di posta elettronica le credenziali di accesso alle caselle istituzionali
- Accertarsi di aver impostato una password sicura sul router utilizzato per l'accesso ad Internet (accertarsi di non aver lasciato la password di default proposta dal costruttore e nota a qualunque malintenzionato)
- Se si utilizza una connessione wifi, accertarsi di adottare una password sicura per il suo accesso (mai lasciare accessi liberi alla rete wifi)