Le 11 raccomandazioni di AgID per uno Smart working sicuro
FONTE https://www.agid.gov.it/

1. Segui prioritariamente le policy e le raccomandazioni dettate dalla tua Amministrazione
2. Utilizza i sistemi operativi per i quali attualmente è garantito il supporto
3. Effettua costantemente gli aggiornamenti di sicurezza del tuo sistema operativo
4. Assicurati che i software di protezione del tuo sistema operativo (Firewall, Antivirus, ecc) siano abilitati e costantemente aggiornati
5. Assicurati che gli accessi al sistema operativo siano protetti da una password sicura e comunque conforme alle password policy emanate dalla tua Amministrazione
6. Non installare software proveniente da fonti/repository non ufficiali
7. Blocca l'accesso al sistema e/o configura la modalità di blocco automatico quando ti allontani dalla postazione di lavoro
8. Non cliccare su link o allegati contenuti in email sospette
9. Utilizza l'accesso a connessioni Wi-Fi adeguatamente protette
10. Collegati a dispositivi mobili (pen-drive, hdd-esterno, etc) di cui conosci la provenienza (nuovi, già utilizzati, forniti dalla tua Amministrazione)
11. Effettua sempre il log-out dai servizi/portali utilizzati dopo che hai concluso la tua sessione lavorativa.

Approfondimenti:

Direttiva 1/2020 "Misure incentivanti per il ricorso a modalità flessibili di svolgimento della prestazione lavorativa"