

## **Le 11 raccomandazioni di Agid per uno smart working sicuro**

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