UNIVERSITÀ
DEGLI STUDI DI TRIESTE

Smart Working

RICHIAMO ALLE ISTRUZIONI PER LA SICUREZZA E LA PROTEZIONE DEI DATI PERSONALI

1.) UTILIZZA UN SISTEMA OPERATIVO PER IL QUALE È ATTUALMENTE GARANTITO IL SUPPORTO

Mantieni aggiornato il tuo sistema operativo.

2.) UTILIZZA E AGGIORNA L'ANTIVIRUS

A tutti i dipendenti viene messo a disposizione un antivirus e i relativi aggiornamenti da scaricare gratuitamente sul pc in uso durante l'espletamento dell'attività in smart working.

3.) FAI MOLTA ATTENZIONE ALLE EMAIL

Non cliccare su link o allegati contenuti in email sospette.

4.) NON SALVARE FILE SUL TUO PC

A maggior ragione se l'utilizzo del PC non ha carattere di esclusività. Non salvare nemmeno su storage/cloud personali.

5.) EVITA LA RIPRODUZIONE SU CARTA

Se non puoi farne a meno, cura la custodia costante dei documenti affinchè nessun'altra persona presente presso l'abitazione ne possa prendere visione.

UNIVERSITÀ
DEGLI STUDI DI TRIESTE

6.) USA WIFI E RETI ADEGUATAMENTE PROTETTE

Non utilizzare connessioni Wi-Fi che non conosci.
Utilizza solo connessioni Wi-Fi protette da password.
Se necessario aumenta la sicurezza della password e la protezione della rete wireless.

7.) UTILIZZA LA VPN DELL'ATENEO

Collegati attraverso il FortiClient o attraverso il servizio WebVPN prima di iniziare a lavorare.

8.) PROTEGGI L'ACCESSO AL PC

Assicurati che l'accesso al PC sia protetto da una password sicura e **non utilizzare un account con privilegio di amministratore** durante l'attività lavorativa

9.) DISCONNETTI IL DESKTOP REMOTO QUANDO INTERROMPI L'ATTIVITÀ

Se lavori tramite desktop remoto disconnettiti in caso di interruzione anche breve dell'attività lavorativa e configura la modalità di blocco automatico dello schermo quando ci si allontana dalla postazione di lavoro.

10.) CONSULTA LE INDICAZIONI DELL'ATENEO

Segui le ulteriori indicazioni del tuo Ateneo qui:
https://www2.units.it/divisioneisi/smartwork/