DECALOGO DELLO SMART WORKER

1. Assicurarsi che il sistema operativo utilizzato sia aggiornato

2. Verificare che il PC utilizzato abbia un antivirus e che lo stesso sia aggiornato

3. Assicurarsi che per accedere al PC personale sia impostata una password di accesso e che questa sia di tipo complessa

4. Non memorizzare le password di accesso all'utilizzo delle risorse dell'amministrazione su postazioni personali ed evitare di scrivere le password utilizzate su post-it e/o fogli lasciati in prossimità della postazione

5. Non effettuare salvataggi sui dispositivi personali e utilizzare preferibilmente le risorse messe a disposizione dall'amministrazione (es. G-Suite, Registro elettronico o altre piattaforme utilizzate)

6. Limitare il ricorso a dispositivi USB pen e flash memory per archiviare dati e documenti

7. Bloccare la postazione in casi di assenza, seppur temporanea e impostare lo sblocco tramite password di accesso

8. Adottare ogni cautela a protezione del dispositivo utilizzato e rispettare le procedure interne su privacy e sicurezza adottate dall'amministrazione

9. Non gettare nella spazzatura documenti cartacei utilizzati per l'attività lavorativa contenenti dati personali se non dopo averli triturati o resi illeggibili

10. Comunicare senza ritardo ogni tipo di incidente da cui potrebbe derivare una violazione di dati personali

Per qualsiasi informazione o necessità è possibile rivolgersi al Responsabile della Protezione dei Dati all'indirizzo: privacy@liquidlaw.it