Allegato B- Prescrizioni sulle modalità organizzative, operative e comportamentali che devono essere adottate per garantire la riservatezza e la sicurezza delle informazioni con particolare riferimento a quelle personali

1 Prescrizioni tecnico-organizzative per il lavoro agile e distanza

Ferme restando le indicazioni già ricevute dal Lavoratore con la nomina ad addetto del trattamento dei dati personali, Il Titolare informa il Lavoratore che anche in caso di prestazioni rese a distanza, permangono e, quindi, vigono gli obblighi generali di:

- non violare il segreto e la riservatezza delle informazioni trattate;
- proteggere i dati contro i rischi di distruzione o perdita, di accesso non autorizzato o di trattamento non consentito;
- rispettare e applicare le misure di sicurezza fisiche, informatiche, organizzative, logistiche e procedurali;
- utilizzare soltanto per rendere la prestazione lavorativa gli eventuali strumenti tecnologici comunali, quali computer, smartphone, ecc., che il Titolare abbia concesso in uso anche al di fuori della struttura;
- contattare il Titolare o l'amministratore di sistema per qualsiasi dubbio, sospetto di incidente o di violazione che possa compromettere i dati aziendali o dello studio professionale.

Il Titolare inoltre informa il Lavoratore che deve adottare specifiche cautele in relazione alla propria postazione di lavoro al fine di preservare la riservatezza e dell'integrità delle informazioni comunali, tra cui rientrano i dati personali trattati in esecuzione delle proprie mansioni.

In particolare, devono essere evitate situazioni di promiscuità, evitando di lavorare in uno stato di contiguità con altri soggetti.

Se il Lavoratore non dispone di un dispositivo fornito dal Comune per eseguire la prestazione lavorativa, deve aver cura di:

- utilizzare un dispositivo, se possibile, ad uso esclusivo personale;
- creare un account personale nel caso in cui il dispositivo sia ad uso condiviso con i familiari e in modo che il lavoratore acceda ad una partizione a suo uso esclusivo;
- proteggere l'accesso al dispositivo (o alla propria partizione) con credenziali conosciute soltanto del lavoratore, evitando qualsiasi forma di condivisione;
- evitare il ricorso a credenziali facilmente intuibili o ricostruibili;
- verificare che il dispositivo sia aggiornato quanto a misure di protezione, quali antivirus, antimalware, e firewall e a tal fine il Datore di lavoro dovrà indicare i tool di sicurezza più adatti;
- verificare che il device sia aggiornato con l'ultima versione disponibile del sistema operativo su cui gira;
- non salvare i "documenti comunali" nella memoria del proprio dispositivo o in altre periferiche personali laddove siano disponibili funzioni di salvataggio su server aziendali;
- non aprire allegati o link che destino sospetti;
- non scaricare programmi di dubbia provenienza;
- disconnettersi accuratamente a fine sessione dagli applicativi aziendali.

Se il lavorare è dotato di dispositivi di lavoro forniti dal Titolare, lo strumento è dotato, per quanto riguarda la sicurezza, delle informazioni di:

- sistema operativo aggiornato;

- misure di protezione da intrusioni (antivirus, firewall, patch di sicurezza) aggiornate. Il lavoratore deve comunque scaricare gli opportuni aggiornamenti e/o non alterare gli automatismi a riguardo che il datore di lavoro abbia eventualmente implementato.
- configurazione dell'accesso remoto ai sistemi aziendali;
- configurazione del pacchetto di applicativi autorizzati;

Il lavoratore deve seguire le procedure specificamente previste dal Titolare per l'utilizzo degli strumenti di lavoro, per quanto compatibili ed è tenuto al:

- divieto di modifica delle impostazioni pre-configurate dal datore;
- divieto assoluto di condivisione del dispositivo e delle credenziali di accesso;
- divieto di installazione software o applicativi non autorizzati;
- divieto di navigazione in siti non attinenti al lavoro e poco sicuri, sempre che il Titolare non abbia impostato appositi filtri;
- divieto di accedere ad eventuali webmail personali;
- divieto di apertura di allegati sospetti;
- divieto di archiviazione e/o conservazione in locale o su sopporti mobili di qualsivoglia documento o file contenente dati personali.

In caso di anomalie o blocchi dovuti a virus o malware, il Lavoratore deve sospendere ogni operazione, chiudere il sistema e le relative applicazioni, nonché informare immediatamente le funzioni IT del Comune.

Per accedere ai sistemi informatici comunali il lavoratore deve utilizzare la seguente modalità di connessione e di accesso:

_____

_____

Il Lavoratore, comunque, per quanto riguarda la linea con si connette da remoto ai sistemi informatici del Comune:

- deve evitare di attingere la connettività domestica da Wi-Fi altrui, o da hot spot sconosciuti oppure pubblici;
- deve assicurare che la linea stessa sia essere protetta da credenziali adeguate (nome di rete non associabile alla persona e password sufficientemente complessa);
- deve verificare che il firmware del proprio router sia debitamente aggiornato (seguendo le istruzioni del fornitore della rete o del modem) perché un modem fuori produzione o privo di update automatici può degradare la connettività e, soprattutto, offrire vulnerabilità che consentono agli hacker di violare l'infrastruttura cui fornisce collegamento.

Il Lavoratore, inoltre, deve prestare la massima attenzione alla provenienza delle e-mail, verificando se l'organizzazione cui appartiene il mittente esiste davvero, cercando conferme sul web o sui social media, il tenore del testo, in quanto da una semplice ma attenta lettura, è possibile cogliere incongruenze logiche, spesso dovute a traduttori automatici, nonché la presenza di link sconosciuti o di allegati sospetti. In caso di dubbio su tali situazioni, il lavoratore deve essere chiedere il da farsi ai propri referenti IT, evitando qualsiasi iniziativa personale.

Il Lavoratore deve, inoltre, prestare attenzione a non inviare per errore informazioni comunali o soggette al segreto professionale a terzi, non autorizzati a riceverle.