PIANO DELLA PRIVACY dell'ISTITUTO STORICO ITALIANO PER IL MEDIO EVO (ISIME)

Il dipendente è tenuto alla più assoluta riservatezza sui dati e sulle informazioni in suo possesso e/o disponibili sul sistema informativo istituzionale e conseguentemente dovrà adottare – in relazione alla particolare modalità della prestazione di lavoro da remoto – ogni provvedimento idoneo a garantire tale riservatezza. Con riferimento alle modalita del "lavoro da remoto", si richiama l'attenzione sui seguenti punti di cui alle citate istruzioni:

- dovere di porre ogni cura per evitare che ai dati possano accedere persone non autorizzate presenti presso l'abitazione;
- dovere di procedere a bloccare l'elaboratore in caso di allontanamento dalla postazione di lavoro, anche per un intervallo molto limitato di tempo;
- alla conclusione della prestazione lavorativa giornaliera è obbligatorio che il dipendente conservi e tuteli i documenti eventualmente stampati, riponendoli in armadi, cassetti o altri contenitori muniti di serratura.

Viene inoltre raccomandato di:

- Utilizzare sistemi operativi per i quali attualmente è garantito il supporto;
- Disporre di un pc con sistema operativo aggiornato;
- Assicurarsi che i software di protezione del sistema operativo (firewall, antivirus è Kaspersky ecc.) siano abilitati e costantemente aggiornati;
- Assicurarsi che gli accessi al sistema operativo siano protetti da una password sicura;
- Bloccare l'accesso al sistema e/o configurare la modalità di blocco automatico quando ci si allontana dalla postazione di lavoro;
- Utilizzare l'accesso a connessioni Wi-Fi adeguatamente protette;
- Disconnettersi sempre dai servizi e dai portali dell'Isime dopo aver concluso la sessione lavorativa;
- Creare un account specifico per l'uso dei dispositivi nei momenti di lavoro da remoto, se gli stessi sono utilizzati anche da familiari o conviventi;
- Non visitare siti web poco attendibili o dal contenuto inappropriato e/o non sicuro;
- Controllare sempre e con la massima attenzione che l'indirizzo del sito web visitato corrisponda effettivamente alla risorsa ufficiale che si vuole consultare;
- Prima di visitare una risorsa presente in una email ricevuta, accertarsi che il collegamento sia effettivamente quello dichiarato dal mittente;
- Effettuare regolarmente una copia di backup dei propri dati di lavoro sugli strumenti ufficiali messi a disposizione dall'Isime;
- Non caricare su dispositivi forniti in disposizione dall'Isime materiale di natura personale o privata;
- Non condividere sui social network informazioni, immagini o screenshot inerenti la propria attività istituzionale;
- Nel caso in cui si dovesse verificare una violazione di dati personali, si rimanda a quanto previsto dalla Legge vigente cui fa riferimento il presente Piano di conformità privacy, pubblicato sul sito dell'Isime alla sezione "Amministrazione Trasparente";
- Occorre porre l'attenzione in merito all'archiviazione, sui propri dispositivi, di documenti contenenti dati personali, che può avere implicazioni rispetto alle corrette modalità di trattamento previste dalla normativa vigente. È, pertanto, altamente raccomandabile non salvare la documentazione su archivi personali, ma elaborarla e gestirla esclusivamente attraverso gli strumenti web messi a disposizione dall'Isime. Nel caso in cui siano stati salvati documenti di ufficio sul pc personale (specie se contengono informazioni personali), quest'attività dovrebbe essere temporanea e, immediatamente dopo la fine dell'attività lavorativa, deve seguire la cancellazione dei documenti informatici;
- Per quanto concerne la gestione dei documenti, considerato che anche la gestione cartacea dei documenti può comportare rischi per la riservatezza dei dati personali, soprattutto se la prestazione lavorativa è svolta presso la propria abitazione, si raccomanda di gestire la predetta documentazione in

modo tale da impedire l'accesso di soggetti terzi non autorizzati al trattamento dei dati personali. Bisogna, pertanto, porre l'attenzione sulla corretta conservazione dei documenti che contengono dati personali; tali documenti, inoltre, devono essere archiviati con misure di sicurezza che permettano l'accesso solo ai soggetti formalmente autorizzati al relativo trattamento. Si raccomanda, pertanto, di non lasciare in vista la documentazione che contiene dati personali e di custodirla all'interno di fascicoli che nascondano il contenuto dei documenti stessi. Inoltre, si consiglia di operare solo con la documentazione necessaria e per il tempo strettamente necessario alla finalità lavorativa, al fine di limitare i rischi di violazione dei dati personali. Nel caso in cui siano stati utilizzati per finalità lavorativa, documenti stampati, si raccomanda di porre attenzione alla distruzione di tali documenti, specie se contenenti dati personali, al termine dell'attività lavorativa così da eliminare ogni dato personale contenuto nel documento e garantire il massimo livello di sicurezza, minimizzando i rischi.

Per ogni opportuno approfondimento delle materie trattate nelle presenti raccomandazioni, si rinvia alla documentazione pubblicata sul sito www.isime.it al seguente link: https://www.isime.it/amministrazione-trasparente/