Allegato all'Accordo individuale

Comune di Carbonia

Disciplina lavoro a distanza

SICUREZZA DELLA RETE E DEI DATI DELL'AMMINISTRAZIONE

Si consiglia di **limitare l'esportazione** dei dati dagli applicativi del Comune e valutare se è necessario estrarre i dati oppure **se è possibile trattarli senza esportarli**. I dati presenti negli applicativi del Comune sono ad accesso protetto da password.

Quando si esportano i dati da un qualsiasi sistema, se ne sta creando una copia. Anche se il database da cui proviene era protetto, la copia scaricata potrebbe non esserlo.
È rischiosa l'esportazione e l'archiviazione di dati personali su ogni supporto mobile (computer portatili, pendrive, etc.).

I periodi di conservazione dei dati si applicano anche ai dati esportati, ai dati presenti nelle e-mail, su chiavette, su pc. I dati devono essere conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati e nel rispetto dei tempi di conservazione

È consigliabile non conservare i dati del Comune sul proprio dispositivo.
Nel caso in cui sia necessario trattarli per attività lavorative devono essere cancellati terminata l'attività.

Non è possibile svolgere attività lavorative in luoghi che non assicurano a mantenere il segreto e il massimo riserbo su tutte le informazioni relative all'attività prestata. **Fare attenzione alle telefonate in luogo pubblico o alla comunicazione o diffusione a terzi**, con o senza strumenti elettronici, di notizie, informazioni o dati appresi in relazione a fatti e circostanze di cui si è a conoscenza.

Segnalare con tempestività al proprio responsabile di ufficio o all'indirizzo PEC comcarbonia@pec.comcarbonia.org eventuali anomalie, incidenti, furti, perdite accidentali di dati, al fine di attivare, nei casi di presenza di un rischio grave per i diritti e le libertà delle persone fisiche, le procedure di comunicazione delle violazioni di dati al Garante privacy e ai soggetti interessati. È sempre consigliato il cambio password di tutti i servizi.

ACCORGIMENTI:

- Proteggere i dispositivi con password e conservarle in luogo sicuro.
- Non memorizzare le credenziali di accesso.
- Evitare l'utilizzo di connessioni internet non sicure.
- Utilizzare canali criptati (https o VPN).
- Proteggere i dispositivi con adeguate applicazioni di protezione, antivirus e mantenerli aggiornati.

- Ove possibile utilizzare il blocco a distanza del device e la crittografa.
- Non lasciare incustodito ed accessibile lo strumento elettronico durante una sessione di trattamento senza avere preventivamente bloccato il PC (premere contemporaneamente i tasti CTRL+ALT+CANC e selezionare l'opzione).
- Prima della dismissione definitiva del dispositivo, procedere alla cancellazione sicura dei dati.
- Nel caso di utilizzo di dispositivi condivisi, mantenere separati i dati del Comune dai dati trattati per finalità personali.
- Accertarsi sempre della provenienza dei messaggi di posta elettronica contenenti allegati; nel caso che il mittente dia origine a dubbi, cancellare direttamente il messaggio senza aprire gli allegati.

TRASMETTERE I DATI IN SICUREZZA

Quando si trasmettono dati ci sono rischi potenziali.

I dati dovrebbero lasciare il Comune solo quando necessario. Ogni volta che trasmettiamo i dati forniamo al destinatario una copia che può scaricare o trasmettere e diventa sempre più difficile garantire il rispetto della cancellazione. Risulta particolarmente a rischio la trasmissione di dati particolari, carte d'identità, passaporti e codici IBAN, codici di accesso che potrebbero esser facilmente carpiti.

Risulta pertanto importante:

- Mantenere alta l'attenzione sull'individuazione dei destinatari.
- Crittografare i documenti (la crittografia è disponibile attraverso applicativi di uso comune quali Office o Adobe Pdf e gli strumenti per. comprimere e crittografare: WinZip, 7-zip, WinRAR etc…) con una corretta gestione dello scambio password (assicurarsi che le password siano costruite in modo sicuro e inviarle separatamente).
- Si può utilizzare il servizio, Google Drive, in modo da caricare il file (crittografato e protetto con password) sul proprio spazio e condividerlo solo con un account scelto.