

Premesso che tutti gli autorizzati devono sempre rispettare i principi di base già definiti dai nostri regolamenti interni. L'autorizzato deve adottare adeguati comportamento per garantire il trattamento legittimo, corretto, lecito, trasparente, proporzionale, di necessità e di tutela della riservatezza e dei diritti degli interessati.



Con la presente si vuole ricordare gli standard da rispettare per l'eventuale trattamento dei dati con utilizzo di DEVICE ANCHE PERSONALI.

Può essere previsto che alcune persone possono utilizzare temporaneamente, o per alcuni periodi di tempo dei DEVICE personali (pratica altrimenti detta BYOD=Bring Your Own Device). L'uso deve avvenire in modo libero e non obbligatorio. Il lavoratore è tenuto ad utilizzarlo come definito negli accordi di lavoro e il reparto IT sarà tenuto a definire delle specifiche per la rete di collegamento.



L'UTILIZZATORE **DEVE**:

- proteggere i dati come definito nel sistema (dotare il device di un Antivirus/firewall secondo quanto stabilito dal reparto IT).
- conoscere le regole di protezione dei dati che dovrà applicare anche da casa
- in caso di perdita o furto del device personale dovrà avvisare immediatamente il reparto IT e il responsabile della privacy
- in caso di interruzione del rapporto di lavoro dovrà far visionare il device dal reparto IT affinché questi verifichi l'assenza di dati non autorizzati
- i collegamenti devono avvenire solo con sistema in remoto con le credenziali ed in VPN o altro sistema "sicuro" autorizzato dalla azienda.
- Usare sistemi operativi per i quali **NON è stato interrotto** il rilascio degli aggiornamenti di sicurezza.
- Garantire la riservatezza e non permettere che altri trattino e/o vedano/sentano dati di persone (si invita a ritirarsi in un luogo non accessibile a familiari o soggetti terzi).
- Tenere in ordine la postazione di lavoro senza lasciare incustoditi appunti, fascicoli, documenti con dati di persone.



L'UTILIZZATORE NON È AUTORIZZATO A E/O **NON DEVE**:

- stampare documenti aziendali presso la propria abitazione o all'esterno dell'azienda (non essendo provvisto di distruggi documenti)
- salvare in locale nel proprio device personale ALCUN riferimento a dati o attività affidategli con particolare attenzione se riferite a dati di persone fisiche. Se si rende necessario salvare in locale un file, dopo l'aggiornamento in rete, deve essere eliminato.
- far utilizzare il proprio device personale da persone diverse non autorizzate.
- far visionare i dati a persone non autorizzate
- memorizzare le password di accesso alla rete aziendale
- Salvare le credenziali di accesso alle Risorse remote. Esse non devono essere memorizzate nello strumento, tramite funzionalità che permettono di "salvare" la password di accesso per non doverla digitare nuovamente al successivo accesso (divieto di funzioni di log-in automatico).
- Salvare documenti e atti di lavoro sui propri Strumenti Personali o su memorie rimovibili personali (Chiavette USB, Memory Card ecc.).



L'ORGANIZZAZIONE CERCA UNA SOLUZIONE CHE CONSENTA DI:

- Fornire agli utenti l'accesso sicuro ai dati e alle risorse aziendali dall'esterno della rete aziendale.
- Consentire agli utenti l'accesso sicuro alle risorse di rete da remoto.
- Eliminare i conflitti di versione che si verificano perché vengono create più versioni dei file quando gli utenti lavorano sulle copie locali mentre si trovano all'esterno della rete.
- Evitare perdite e/o violazioni di dati

