AVVERTENZA: Il presente documento intende riassumere il Regolamento Informatico Aziendale (sempre esposto, nella sua ultima versione formalmente approvata, nelle bacheche aziendali) in **regole chiare e sintetiche**, il cui rispetto, da parte del personale, garantisce la conformità alle policy interne.

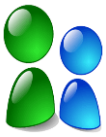
NORMATIVE DI RIFERIMENTO: Le seguenti regole aziendali sono implementate in conformità alle **vigenti normative** che regolano la materia, con particolare riferimento a: D.Lgs.196/2003 "Legge sulla Privacy"; Provv.Garante 01/03/2007 "Linee guida sull'utilizzo di internet/posta elettronica"; Art.4 L.300/70 "Statuto Lavoratori" così come modificato dal D.Lgs.151/2015.

FINALITÀ DI UTILIZZO: Gli strumenti informatici assegnati sono **strumenti di lavoro**; ogni utilizzo non inerente all'attività lavorativa è vietato perché può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.

USO RESPONSABILE: Si richiede l'utilizzo degli strumenti elettronici assegnati assicurandone l'integrità, la conservazione e la sicurezza, evitando comportamenti che possano compromettere la funzionalità, le impostazioni e la sicurezza delle macchine. Si richiede di non effettuare sostanziali modifiche del proprio ambiente informatico, con particolare riferimento all'installazione o disinstallazione di applicativi ed alla modifica delle impostazioni di sistema, se non preventivamente autorizzati.

PROTEZIONE DATABASE E PROPRIETA' DEI CONTENUTI: E' fatto divieto di distruggere, sottrarre, manipolare, divulgare il contenuto delle banche dati elettroniche aziendali se non espressamente connesso a legittime finalità lavorative o se non espressamente autorizzato dalla Direzione. Ogni materiale informatico (documenti, comunicazioni, elenchi, files, directory, database, ecc.) prodotto dagli utenti nel corso dell'attività lavorativa è da intendersi di **proprietà della società.**

PROCEDURE AUTENTICAZIONE: Il sistema assegna **estremi identificativi** (costituiti da user-name e password) ad ogni utente abilitato all'utilizzo di strumenti elettronici. Ogni utente deve garantire la segretezza delle proprie credenziali e la loro sostituzione periodica. La password scelta non dovrà avere meno di 8 caratteri e non dovrà contenere riferimenti diretti a nome/cognome dell'utente. In caso di allontanamento dalla postazione lavorativa si richiede di **bloccare il computer** (simbolo windows+l oppure Ctrl + Alt + Canc + Blocca).



ATTIVAZIONE / DISATTIVAZIONE UTENTI E PROFILI DI ACCESSO: Le procedure di autenticazione danno automaticamente accesso alle risorse informatiche ed ai dati necessari alla rispettive mansioni personali (definiti dalla direzione in fase di avvio attività). Gli utenti sono tenuti al rispetto dei profili assegnati: ogni eventuali modifica deve essere richiesta e motivata alla direzione. In caso di **cessazione del rapporto** l'utente sarà disabilitato ed i relativi dati potranno essere legittimamente utilizzati dalla società.

UTILIZZO DI SUPPORTI DI MEMORIA E PERSONAL CLOUD: L'utilizzo incontrollato di supporti di memorizzazione removibili (chiavette USB, HD esterni, CD/DVD, ecc.) o di storage on-line (dropbox, google drive, ecc.) può comportare significativi rischi sulla sicurezza dei dati e divenire un vettore di perdita o accesso non autorizzato alle informazioni. Gli utenti sono pertanto tenuti a confrontarsi con la direzione in relazione all'uso di tali strumenti, che devono comunque essere sempre utilizzati con particolare cautela (in conformità al regolamento informatico interno) onde evitare che il loro contenuto possa essere accessibile a terzi non autorizzati. Se non necessarie porte USB e lettori CD/DVD sono disabilitati.

UTILIZZO DI MOBILE DEVICE: Anche ai mobile devices (smartphone/tablet) si applicano le prescrizioni del regolamento informatico, con particolare cautela per le criticità insite negli strumenti in oggetto. **In particolare si richiede di**: non modificare le impostazioni di sistema; segnalare immediatamente eventuali anomalie; prestare particolare attenzione alla custodia dello strumento e segnalare immediatamente lo smarrimento o il furto; prestare attenzione all'utilizzo in luoghi pubblici in cui potrebbero essere intercettate informazioni; evitare di collegare lo strumento a dispositivi non aziendali.

UTILIZZO DI INTERNET / POSTA ELETTRONICA / PEC: La casella di posta elettronica e la navigazione in internet sono **strumenti di lavoro**, è pertanto vietato qualsiasi utilizzo a fini personali. Gli assegnatari di tali strumenti sono responsabili del loro corretto utilizzo. Si sottolinea che è strettamente vietata qualsiasi attività che preveda il download/upload di contenuti: diffamatori, osceni, violenti, discriminatori; lesivi per l'immagine e la reputazione aziendale; illeciti con particolare riferimento al diritto d'autore ed alla pirateria informatica; fonte di disservizio all'operatività aziendale.
Gli incaricati autorizzati a gestire la **posta elettronica certificata** aziendale, porranno massima attenzione nell'utilizzo di questo strumento al quale la legge italiana riconosce lo stesso valore legale di una raccomandata con avviso di ricevimento tradizionale, garantendone così il non ripudio. Lo strumento PEC non assegna valore legale al contenuto del messaggio ed eventuali allegati, ma certifica semplicemente il processo di trasmissione/ricezione: l'utilizzatore è pertanto responsabile di quanto include nel messaggio in corpo testo o allegato.

ATTIVITA' DI CONTROLLO: Gli strumenti elettronici forniti per fini lavorativi consentono l'archiviazione di dati relativi al loro utilizzo, che possono ricondurre a comportamenti dell'utente (log-management). Si informa che, in conformità alle recenti disposizioni normative (Jobs Act), tali dati **possono raccolti ed archiviati in conformità alle vigenti normative privacy e possono essere utilizzati a qualsiasi fine connesso al rapporto di lavoro**. Nell'attività di verifica (effettuata esclusivamente dagli AdS appositamente nominati ed istruiti) sarà osservato il principio di gradualità, operando, qualora possibile, controlli su dati aggregati. In nessun caso verranno compiuti controlli prolungati, costanti o indiscriminati. Resta fermo il diritto del datore di lavoro di effettuare controlli identificativi quando ciò sia dettato da:
- riscontri di mancato rispetto del presente regolamento;
- oggettivi indizi di commissione di reato;
- specifiche richieste delle forze dell'ordine;
- segnalazione di circostanze sospette da parte della struttura di protezione della rete.

PROFILI SANZIONATORI: La contravvenzione alle regole contenute nel presente regolamento da parte di un utente, comporta l'immediata revoca delle autorizzazioni ad accedere alla Rete Informatica ed ai servizi/programmi precedentemente autorizzati, fatte salve le sanzioni più gravi previste dalle norme vigenti e dai regolamenti interni. Ricordiamo che, in relazione all'inosservanza da parte del lavoratore degli obblighi di diligenza, di osservanza e di fedeltà, al datore di lavoro è attribuito dall'ordinamento il potere di irrogare **sanzioni disciplinari**, graduate secondo la gravità dell'infrazione e nel rispetto delle previsioni contenute nei contratti collettivi di lavoro (art. 2106 cod. civ.).
L'irrogazione delle suddette sanzioni non preclude, né pregiudica l'azione giudiziaria del datore di lavoro: di denuncia di atti illeciti di rilevanza penale; di risarcimento civile per danni al patrimonio o all'immagine della Società o di soggetti terzi.

Eventuali chiarimenti o richieste di modifica al presente regolamento possono essere indirizzati alla direzione aziendale.