REGOLAMENTO INTERNO PRIVACY

Ed.0 del 05.12.2019

1. GESTIONE DEI DATI PERSONALI E AZIENDALI

1.1. Ogni Utente è responsabile dei dati personali e aziendali dei quali entra in possesso per lo svolgimento della sua attività lavorativa. Deve quindi trattare i dati e le informazioni adottando ogni idonea misura di sicurezza al fine di tutelarne la riservatezza, la sicurezza, l'integrità ed il corretto utilizzo.

1.2. I dati personali e aziendali potranno essere comunicati a terze parti esclusivamente nell'ambito della propria funzione e secondo le finalità connesse alla propria attività lavorativa.

1.3. È vietata la comunicazione di dati e informazioni verso terzi che possano arrecare danno all'immagine, alla reputazione, alla produttività, alla proprietà intellettuale e del *know-how* ed alla redditività aziendale o che possano violare i vincoli contrattuali e di legge connessi al rapporto di lavoro.

1.4. È assolutamente vietata la divulgazione a terzi di dati personali, informazioni riservate, confidenziali o comunque di proprietà del Titolare. In caso di violazione, il Titolare si riserva di avviare i relativi provvedimenti disciplinari, nonché le azioni civili e penali consentite.

1.5. Si ricorda, inoltre, che la diffusione illecita di dati personali e aziendali potrebbe configurare, oltre alla violazione del presente Regolamento, la violazione di norme con conseguenze sia civili che penali a carico del responsabile dell'illecita diffusione, nonché la violazione della normativa che regola il rapporto di lavoro.

2. POSTAZIONI DI LAVORO

2.1. L'**utilizzo** della postazione di lavoro e il conseguente accesso ai documenti, atti e archivi è consentito nei limiti della propria funzione e dei propri incarichi.

2.2. Scrivania pulita. La propria scrivania deve essere mantenuta in ordine, verificando di non lasciare documenti e atti riservati senza un proprio controllo all'accesso di terzi, in momenti di pausa, terminata la giornata di lavoro e/o in periodi di assenza.

2.3. Reception. L'ufficio segreteria deve sempre essere presente nella sua postazione durante l'orario d'ufficio, nel caso di assenza è necessario cercare una sostituzione.

3. MISURE FISICHE DI CUSTODIA DI DOCUMENTI E ATTI CARTACEI

3.1. I dati cartacei ed i supporti cartacei necessari per lo svolgimento delle mansioni lavorative devono essere custoditi in armadi o cassettiere chiusi a chiave nel contesto organizzativo in cui si opera.

3.2. Tutti gli archivi sono ad accesso limitato, per cui è possibile accedervi nei limiti della necessità per prelevare e riporre i documenti necessari per lo svolgimento delle mansioni lavorative, previa autorizzazione della Direzione. I documenti dovranno essere riposti correttamente durante i periodi di temporanea assenza ed al termine dell'attività lavorativa negli appositi archivi. Gli archivi di documenti e atti contenenti dati personali dovranno essere custoditi in armadi chiusi a chiave.

3.3. L'**eliminazione fisica** di ogni documento cartaceo o supporto informatico contenente dati e informazioni aziendali e/o personali deve essere effettuata solo utilizzando gli appositi strumenti.
3.4. E' vietato lasciare documenti incustoditi presso i **dispositivi di stampa,** per cui è fatto obbligo di recuperare le stampe appena effettuate.

4. STRUMENTI INFORMATICI

4.1. L'utilizzo degli strumenti informatici in dotazione è di carattere professionale.
4.2. Tutti gli strumenti dovranno essere bloccati e protetti da password, per evitare un accesso illegittimo e non consentito di terzi.
4.3. Gli strumenti dovranno essere automaticamente spenti o messi in modalità a basso consumo se non usati per più di un'ora, a meno di motivate esigenze di lavoro.

5. CUSTODIA DEGLI STRUMENTI INFORMATICI

5.1. Gli strumenti informatici di proprietà di UNINFORM devono essere custoditi dall'Utente con cura e diligenza prevenendo possibili danneggiamenti che ne compromettano il corretto funzionamento ed evitando di lasciarli incustoditi in ambienti pubblici.
5.1.1. Qualora l'utente sia dotato di un PC portatile, egli è responsabile di custodirlo con diligenza sia se l'utilizzo avviene fuori sede sia durante l'utilizzo nel luogo di lavoro.
5.1.2. I PC portatili utilizzati all'esterno devono essere custoditi con diligenza, adottando tutti i provvedimenti che le circostanze rendono necessari per evitare danni o sottrazioni, nonché l'accesso illegittimo e non consentito da parte di terzi.
5.1.3. Si ricorda che lasciare un elaboratore incustodito può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne l'indebito uso.
5.2. In caso di furto o danneggiamento di beni, l'Utente dovrà informare immediatamente la Direzione e l'Amministratore del Sistema, presentare formale denuncia alle autorità di pubblica sicurezza e consegnarne copia al Titolare del Trattamento per l'attivazione degli atti formali di scarico e di attivazione delle coperture assicurative, nonché per la valutazione della attivazione del processo di Data Breach.
5.3. Tutti i supporti magnetici rimovibili (hard disk, CD e DVD riscrivibili, supporti USB, ecc.), contenenti dati personali nonché informazioni costituenti know-how aziendale, devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere accessibile illegittimamente, trafugato o alterato e/o distrutto o, successivamente alla cancellazione, recuperato.
5.3.1. I supporti magnetici contenenti dati personali devono essere adeguatamente custoditi dagli utenti in armadi chiusi.
5.3.2. Per motivi di sicurezza informatica, è vietato l'utilizzo di supporti magnetici rimovibili personali.

6. GESTIONE DELLE CREDENZIALI DI ACCESSO E DELLE PASSWORD

6.1. Le credenziali di autenticazione per l'accesso alla rete e per altri servizi vengono assegnate dall'Amministratore del Sistema e consegnate all'Utente; esse consistono in un codice per l'identificazione dell'Utente (username), associato ad una parola chiave (password) riservata che dovrà venir custodita dall'Utente con la massima diligenza e non divulgata. Ogni Utente è responsabile della sicurezza e di qualunque operazione effettuata utilizzando le proprie credenziali.
6.1.1. È proibito accedere alla rete e ai programmi con credenziali diverse dalle proprie o in maniera anonima.
6.1.2. In nessun caso devono essere annotate password in chiaro sia su supporto cartaceo che informatico.
6.2. Qualora l'intestatario della password ritenga che un soggetto non autorizzato possa essere venuto a conoscenza della propria password, dovrà provvedere immediatamente a darne comunicazione all'Amministratore del Sistema e alla Direzione.
6.3 Sulla base della normativa vigente, le password degli Utenti devono essere cambiate almeno ogni sei mesi.

7. GESTIONE E PROTEZIONE DEI DATI

7.1. L'accesso ai dati è consentito nei limiti della propria funzione organizzativa e della propria attività lavorativa.
7.2. La rete informatica di UNINFORM è un'area di condivisione di informazioni strettamente professionali e non può in alcun modo essere utilizzata per scopi diversi. Pertanto qualunque file che non sia inerente all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità vengono svolte regolari attività di controllo, amministrazione e backup da parte del personale incaricato.
7.3. Il personale incaricato può in qualunque momento procedere alla rimozione di ogni file o applicazione che reputerà pericolosa per la sicurezza sia sugli strumenti informatici degli Utenti, sia sulle unità di rete: di tale intervento ne è informato l'Utente e il suo diretto Responsabile.
7.3.1. Solo il **backup** dei PC in rete viene effettuato ogni 6 mesi su un hard disk esterno. Pertanto, gli Utenti che trattengono dati di UNINFORM in aree diverse dai PC di rete, sono responsabili del salvataggio degli stessi e di eventuali danni a UNINFORM o a terzi anche di natura civilistica causati dalla loro perdita o sottrazione.
7.3.2. È vietato il salvataggio di dati e informazioni di carattere aziendale in sistemi di ***cloud pubblica*** non autorizzati dagli Amministratori di Sistema e/o dal Titolare del Trattamento.

8. GESTIONE DELLA POSTA ELETTRONICA

8.1 L'assegnazione di una casella di posta elettronica di UNINFORM (da ora "e-mail UNINFORM") è di carattere professionale.
8.1.1. In deroga a tale principio UNINFORM autorizza un moderato e ragionevole utilizzo privato.
8.1.2. Tale utilizzo deve essere limitato ed ispirato a criteri di buon senso e non dovrà ostacolare l'utilizzo professionale.

8.1.3. Lo spazio della risorsa affidata utilizzato a fini “privati” dovrà perciò essere limitato e non dovrà precludere e limitare quello dedicato all’utilizzo professionale.
8.2. La UNINFORM, in conformità alla disciplina in materia di privacy, prevede che ad ogni messaggio in uscita sia automaticamente aggiunto un breve testo di avviso al ricevente della natura potenzialmente riservata del messaggio.
8.3. Gli Utenti delle e-mail UNINFORM sono responsabili dell’utilizzo della stessa e devono mantenere un corretto comportamento nell’utilizzo della posta elettronica. In particolare, gli Utenti devono seguire le seguenti disposizioni:

- non inviare né conservare messaggi di posta elettronica e/o allegati dal contenuto offensivo, molesto, volgare, blasfemo, xenofobo, razziale, pornografico o comunque inappropriato o illegale, salvo specifiche esigenze aziendali;
- prestare la massima attenzione nell’inoltro di e-mail riportanti contenuti e indirizzi e-mail di precedenti comunicazioni;
- prestare la massima attenzione ad e-mail sospette, avvisando l’Amministratore di Sistema in caso di dubbi sulla provenienza/contenuto delle stesse;
- creare una sezione denominata “Posta personale” all’interno della propria casella di posta, alla quale gli Amministratori di Sistema e/o il Titolare del Trattamento non potranno accedere se non per gravi motivi di sicurezza informatica.

8.4. Per motivi di sicurezza informatica ed in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all’attività lavorativa, l’accesso alla casella di posta dell’Utente potrà essere gestita dagli Amministratori di Sistema su richiesta del Titolare del Trattamento dell’Utente al fine di verificare il contenuto dei messaggi e ad inoltrare al Titolare del Trattamento quelli ritenuti rilevanti per lo svolgimento dell’attività lavorativa.
8.5. Per motivi di sicurezza informatica è assolutamente vietato connettersi alla propria casella di posta elettronica utilizzando strumenti informatici diversi da quelli forniti dalla Società, siano essi PC desktop, PC portatili, tablet, smartphone e ogni altro strumento informatico.
8.6. La **Posta Elettronica Certificata (PEC)** può essere utilizzata dagli Incaricati solamente per motivi professionali.
8.7. La **Firma Digitale** può essere utilizzata esclusivamente dal proprietario della firma e per motivi strettamente aziendali.

9. UTILIZZO DELLA NAVIGAZIONE INTERNET

9.1. L’accesso a Internet è fornito principalmente per scopo professionale, per accedere a informazioni e contenuti necessari allo svolgimento dell’attività lavorativa. Essendo uno strumento di lavoro, gli Utenti cui si attribuisce l’accesso sono responsabili del suo corretto utilizzo.
9.2. Come per la posta elettronica, UNINFORM ne autorizza un moderato e ragionevole utilizzo privato, limitato ed ispirato a criteri di buon senso senza ostacoli all’attività professionale e curando la gestione e e/o la cancellazione della cronologia.

9.3. Gli Utenti devono seguire le seguenti regole di navigazione della rete Internet:

- è tassativamente vietato scaricare materiale e programmi in violazione della legislazione sui diritti di autore, che siano essi appartenenti a persone o aziende, coperti da copyright, brevetto o proprietà intellettuale, ivi compresa l'installazione o la distribuzione di software che non sia specificatamente licenziato per essere utilizzato all'interno di UNINFORM;
- è tassativamente vietato navigare siti e scaricare materiale pericolosi/vietati o aventi contenuti illegali (contenuto offensivo, molesto, volgare, blasfemo, xenofobo, razziale, pornografico, pedopornografico, terrorismo o comunque inappropriato o illegale), salvo specifiche esigenze di lavoro;
- è vietato effettuare copia non autorizzata di materiale coperto da copyright compreso ma non limitato a digitalizzazione e distribuzione di foto da riviste, libri o altre fonti, musica o materiale video;
- è vietato utilizzare l'infrastruttura tecnologica di UNINFORM per procurarsi e diffondere materiale in violazione con le normative vigenti;
- è vietato effettuare attività che possano generare dei problemi di sicurezza o danneggiare le comunicazioni sulla rete;
- è vietato eseguire qualsiasi forma di monitoraggio della rete che permetta di catturare dati non espressamente inviati all'host dell'Utente (sniffing) a meno che questa attività non faccia parte dei compiti dell'Utente e quindi formalmente autorizzata dagli amministratori di sistema;
- è vietato aggirare le procedure di autenticazione o la sicurezza di qualunque host, rete, account.

10. COMUNICAZIONE DI DATI E INFORMAZIONI ATTRAVERSO SOCIAL MEDIA

10.1. È assolutamente vietato pubblicare in internet attraverso social media personali, forum, chat, blog, siti internet, dati personali ed informazioni di carattere aziendale (informazioni, documenti, appunti, commenti personali o di terzi, foto, video, audio, ecc..) e/o dati personali ed informazioni inerenti i dipendenti di UNINFORM e dei suoi partner, salvo espressa autorizzazione degli interessati.

10.2. E' fatto in ogni caso espresso divieto di pubblicazione e/o diffusione di dati personali ed informazioni di carattere aziendale che possano arrecare danno all'immagine, alla reputazione, alla produttività, alla proprietà intellettuale e del know-how ed alla redditività di UNINFORM o che possano violare i vincoli contrattuali e di legge connessi al rapporto di lavoro.

10.3. È assolutamente vietato divulgare notizie false.

10.4. È invece autorizzata la divulgazione di informazioni già rese pubbliche da UNINFORM.

11. CESSAZIONE DEL RAPPORTO DI LAVORO

11.1. In caso di cessazione del rapporto con UNINFORM, valgono le seguenti regole operative:

a) Le credenziali per l'accesso ai sistemi e alla posta elettronica vengono disattivate;

b) È facoltà di UNINFORM effettuare eventuali operazioni di conservazione di e-mail di carattere professionale di Utenti non più appartenenti all'organizzazione. Le e-mail nella "Posta personale" saranno, al contrario, cancellate.

Tali attività sono effettuate dagli Amministratori di Sistema autorizzati alla gestione della posta elettronica, che potranno pertanto avere accesso, per esclusive ragioni di carattere tecnico e solo ove non sia evitabile, a dati personali conservati all'interno delle caselle di posta.

11.2. Con il dovuto anticipo, l'Utente è tenuto ad attivare il risponditore automatico per notificare ad eventuali fornitori, partner, clienti od altri soggetti interessati, l'interruzione del proprio rapporto con UNINFORM e - se del caso - per proporre un contatto interno alternativo.

11.3. Per quanto riguarda la restituzione degli strumenti informatici di proprietà di UNINFORM, valgono le seguenti regole operative:

a) Gli smartphone e tutti gli altri strumenti informatici devono essere restituiti alla Direzione.
b) Il lavoratore non dovrà divulgare notizie attinenti alla organizzazione, ai metodi di produzione e a tutto quant'altro inerente la UNINFORM
c) Il lavoratore non dovrà divulgare informazioni e/o dati personali inerenti i dipendenti, i dirigenti e/o terzi di cui sia venuto a conoscenza durante il rapporto di lavoro.

12. RIPRESE VIDEO-AUDIO-FOTOGRAFICHE ALL'INTERNO DI UNINFORM

12.1. Qualsiasi ripresa video-audio-fotografica deve essere realizzata rispettando i diritti delle singole persone coinvolte.

12.2. Per ragioni connesse alla propria attività lavorativa le riprese video-audio-fotografiche devono essere autorizzate dal Titolare del Trattamento. Tali riprese possono essere utilizzate esclusivamente per finalità lavorative e non possono essere divulgate al di fuori del contesto istituzionale in cui sono state realizzate.

12.3. Al di fuori di questa casistica è vietato effettuare riprese video-audio-fotografiche in qualunque area di UNINFORM, salvo preventiva e formale autorizzazione del proprio Titolare del Trattamento.

12.4. Gli Utenti interni potranno essere fotografati e/o ripresi in occasione di eventi, seminari e momenti di formazione. In questi casi, le immagini e le riprese potranno essere utilizzate per scopi e comunicazioni istituzionali.

13. SPECIFICI DIVIETI

Di seguito sono riportati specifici divieti per gli Utenti:

- alterare documenti informatici, pubblici o privati, aventi efficacia probatoria;
- accedere abusivamente al sistema informatico o telematico di soggetti pubblici o privati;
- accedere abusivamente al proprio sistema informatico o telematico al fine di alterare e /o cancellare dati e/o informazioni;
- detenere e utilizzare abusivamente codici, parole chiave o altri mezzi idonei all'accesso al proprio sistema informatico o telematico o di soggetti concorrenti, pubblici o privati al fine di acquisire informazioni riservate;

- svolgere attività di approvvigionamento e/o produzione e/o diffusione di apparecchiature e/o software allo scopo di danneggiare un sistema informatico o telematico di soggetti, pubblici o privati, le informazioni, i dati o i programmi in esso contenuti, ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento;
- svolgere attività fraudolenta di intercettazione, impedimento o interruzione di comunicazioni;
- svolgere attività di modifica e/o cancellazione di dati, informazioni o programmi di soggetti privati o soggetti pubblici o comunque di pubblica utilità;
- svolgere attività di danneggiamento di informazioni, dati e programmi informatici o telematici altrui;
- distruggere, danneggiare, rendere inservibili sistemi informatici o telematici di pubblica utilità;
- caricare programmi non provenienti da una fonte certa e autorizzata dall'Associazione;
- utilizzare illegalmente password di computer, codici di accesso o informazioni simili per compiere una delle condotte sopra indicate;
- utilizzare strumenti o apparecchiature, inclusi programmi informatici, per decriptare software o altri dati informatici;
- distribuire il software aziendale a soggetti terzi;
- accedere illegalmente e duplicare banche dati;
- utilizzare in qualsiasi modo, in assenza di specifica ed autorizzata attività, dati personali dei dipendenti della UNINFORM, dei partner e del personale dirigente.