

Regolamento Sistemi Informatici

Versione 1.1 | Entrata in vigore: 15/04/2025

Sommario

1. PREMESSA	3
2. OGGETTO E FINALITÀ	3
3. PRINCIPI GENERALI E DI RISERVATEZZA NELLE COMUNICAZIONI	4
4. TUTELA DEL LAVORATORE	4
5. CAMPO DI APPLICAZIONE	5
6. GESTIONE, ASSEGNAZIONE E REVOCA DELLE CREDENZIALI DI ACCESSO	5
6.1 ASSEGNAZIONE	5
6.2 COMPILAZIONE DELLA RICHIESTA DI ASSEGNAZIONE.....	5
6.3 ROBUSTEZZA PASSWORD	5
7. UTILIZZO INFRASTRUTTURA DI RETE E FILESYSTEM	6
7.1 ACCESSO ALLA RETE E CONDIVISIONE DI FILE.....	6
7.2 DEVICE ESTERNI DI ARCHIVIAZIONE FILE	6
7.3 PULIZIA DEGLI ARCHIVI FILE.....	6
7.4 VPN.....	6
7.5 Wi-Fi.....	7
7.5.1 Tipologia di reti.....	7
7.5.2 Accesso da parte di persone esterne all'azienda.....	7
7.5.3 Interruzione della rete	7
8. UTILIZZO DEGLI STRUMENTI ELETTRONICI (PC, NOTEBOOK E ALTRI STRUMENTI CON RELATIVI SOFTWARE E APPLICATIVI).....	7
9. UTILIZZO DI INTERNET.....	9
10. UTILIZZO DELLA POSTA ELETTRONICA.....	10
11. UTILIZZO DEI TELEFONI, FAX, FOTOCOPIATRICI, SCANNER E STAMPANTI.....	12
12. ASSISTENZA AGLI UTENTI E MANUTENZIONI.....	12
13. CONTROLLI SUGLI STRUMENTI	13
13.1 CONTROLLI PER LA TUTELA DEL PATRIMONIO, NONCHÉ PER LA SICUREZZA E LA SALVAGUARDIA DEL SISTEMA INFORMATICO. CONTROLLI PER ULTERIORI MOTIVI TECNICI E/O MANUTENTIVI (AD ES. AGGIORNAMENTO/SOSTITUZIONE/IMPLEMENTAZIONE DI PROGRAMMI, MANUTENZIONE HARDWARE, ETC.)	14
13.2 CONTROLLI PER ESIGENZE PRODUTTIVE E DI ORGANIZZAZIONE	14
14. CONSERVAZIONE DEI DATI	15
15. PARTECIPAZIONI A SOCIAL MEDIA	15
16. PUBBLICAZIONE E MESSA A DISPOSIZIONE	16
17. SANZIONI DISCIPLINARI.....	16

1. Premessa

Questo Regolamento è stato predisposto per fornire ai dipendenti e collaboratori, indicati anche come incaricati o utenti, le linee guida necessarie per una gestione corretta e appropriata delle informazioni, in particolare tramite l'uso dei sistemi, delle applicazioni e degli strumenti informatici della Società.

Tutti i dipendenti e collaboratori sono obbligati a rispettare quanto previsto dal Regolamento, che è accessibile attraverso le modalità descritte al punto 16.

Si specifica che gli strumenti utilizzati dai lavoratori, inclusi PC, notebook, risorse, e-mail e altri dispositivi con i relativi software e applicativi (di seguito denominati "Strumenti"), sono forniti dalla Società esclusivamente per l'esecuzione dell'attività lavorativa. Questi strumenti, insieme alle reti aziendali accessibili tramite essi, costituiscono il domicilio informatico della Società.

I dati personali e le informazioni raccolte o registrate tramite l'utilizzo degli Strumenti vengono trattati per finalità organizzative e produttive, per garantire la sicurezza sul lavoro e per proteggere il patrimonio aziendale. Tale protezione comprende anche la sicurezza informatica e la salvaguardia del sistema informatico. Le informazioni raccolte possono essere utilizzate per tutte le finalità legate al rapporto di lavoro, in quanto questo Regolamento fornisce un'informazione chiara sulle modalità di utilizzo degli strumenti e sull'effettuazione di eventuali controlli, nel pieno rispetto del Regolamento Europeo 679/16, noto come "General Data Protection Regulation" (GDPR).

Infine, si sottolinea che sui sistemi informatici in uso agli utenti non sono installati né configurati hardware o software finalizzati al controllo a distanza dell'attività lavorativa.

2. Oggetto e finalità

Il presente Regolamento è redatto:

- alla luce della Legge 20.5.1970, n. 300, recante "Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro e norme sul collocamento";
- in attuazione del Regolamento Europeo 679/16 "General Data Protection Regulation" (d'ora in avanti Reg. 679/16 o GDPR);
- ai sensi delle "Linee guida del Garante per posta elettronica e internet" in Gazzetta Ufficiale n. 58 del 10 marzo 2007;
- alla luce dell'articolo 23 del D.Lgs. n. 151/2015 (c.d. Jobs Act) che modifica e rimodula il divieto dei controlli a distanza, nella consapevolezza di dover tener conto, nell'attuale contesto produttivo, oltre agli impianti audiovisivi, anche degli altri strumenti «dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori» e di quelli «utilizzati dal lavoratore per rendere la prestazione lavorativa».

L'obiettivo è quello di diffondere tra tutto il personale una solida "cultura informatica", garantendo che l'utilizzo degli strumenti informatici e telematici messi a disposizione dalla Società, come la posta elettronica, internet e i computer con i relativi software, avvenga in modo appropriato e in conformità alle finalità aziendali e alla normativa vigente. Si intende fornire a ogni dipendente le indicazioni necessarie per prevenire qualsiasi abuso o uso improprio, partendo dal principio che prevenire i problemi è sempre preferibile rispetto a doverli affrontare e correggere successivamente.

3. Principi generali e di riservatezza nelle comunicazioni

I principi che sono a fondamento del presente Regolamento sono gli stessi espressi nel GDPR, e, precisamente:

- il **principio di necessità**, secondo cui i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi in relazione alle finalità perseguite (art. 5 e 6 del Reg. 679/16);
- il **principio di correttezza**, secondo cui le caratteristiche essenziali dei trattamenti devono essere rese note ai lavoratori. Le tecnologie dell'informazione (in modo più marcato rispetto ad apparecchiature tradizionali) permettono di svolgere trattamenti ulteriori rispetto a quelli connessi ordinariamente all'attività lavorativa. Ciò, all'insaputa o senza la piena consapevolezza dei lavoratori, considerate anche le potenziali applicazioni di regola non adeguatamente conosciute dagli interessati;
- i **trattamenti devono essere effettuati per finalità determinate**, esplicite e legittime (art.5 commi 1 e 2), osservando il principio di pertinenza e non eccedenza. Il datore di lavoro deve trattare i dati "nella misura meno invasiva possibile"; le attività di monitoraggio devono essere svolte solo da soggetti preposti ed essere "mirate sull'area di rischio, tenendo conto della normativa sulla protezione dei dati e, se pertinente, del principio di segretezza della corrispondenza".

È riconosciuto al datore di lavoro di potere svolgere attività di monitoraggio, che nella fattispecie saranno svolte solo dall'Amministratore di Sistema o dal personale delegato dall'Amministratore di Sistema, sempre nel rispetto della succitata normativa.

Il dipendente si attiene alle seguenti regole di trattamento:

- È vietato comunicare a soggetti non specificatamente autorizzati i dati personali comuni, sensibili, giudiziari, sanitari o altri dati, elementi e informazioni dei quali il dipendente / collaboratore viene a conoscenza nell'esercizio delle proprie funzioni e mansioni all'interno della Società. In caso di dubbio, è necessario accertarsi che il soggetto cui devono essere comunicati i dati sia o meno autorizzato a riceverli, mediante richiesta preventiva al proprio Responsabile di area/funzione.
- È vietata l'estrazione di originali e/o copie cartacee ed informatiche per uso personale di documenti, manuali, fascicoli, lettere, database e quant'altro.
- È vietato lasciare incustoditi documenti, lettere, fascicoli, appunti e quant'altro possa contenere dati personali e/o informazioni quando il dipendente/collaboratore si allontana dalla postazione di lavoro. È vietato lasciare sulla postazione di lavoro (scrivania, bancone ecc.) materiali che non siano inerenti alla pratica che si sta trattando in quel momento. Ciò vale soprattutto nel caso di lavoratori con mansioni di front office e di ricezione di clienti / fornitori o colleghi di lavoro.
- Per le riunioni e gli incontri con clienti, fornitori, consulenti e collaboratori della Società è necessario utilizzare le eventuali zone / sale dedicate.

4. Tutela del lavoratore

Alla luce dell'art. 4, comma 1, L.n. 300/1970, la regolamentazione della materia indicata nel presente Regolamento non è finalizzata all'esercizio di un controllo a distanza dei lavoratori da parte del datore di lavoro ma solo a permettere a quest'ultimo di utilizzare sistemi

informatici per fare fronte ad esigenze produttive od organizzative e di sicurezza nel trattamento dei dati personali.

È garantito al singolo lavoratore il controllo sui propri dati personali secondo quanto previsto dagli articoli 15-16-17-18-20-21-77 del Reg. 679/16.

5. Campo di applicazione

Il presente regolamento si applica a tutti i dipendenti, senza distinzione di ruolo e/o di livello, nonché a tutti i collaboratori della Società a prescindere dal rapporto contrattuale con la stessa intrattenuto.

Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche e telematiche, per "utente" deve intendersi ogni dipendente e collaboratore in possesso di specifiche credenziali di autenticazione.

Tale figura potrà anche venir indicata in questo testo come "incaricato del trattamento" o più semplicemente come "incaricato".

6. Gestione, assegnazione e revoca delle credenziali di accesso

6.1 Assegnazione

Le credenziali di autenticazione per l'accesso alle risorse informatiche vengono assegnate dall'Amministratore di Sistema, previa formale richiesta del Responsabile dell'ufficio nell'ambito del quale verrà inserito ed andrà ad operare il nuovo utente. Questo è valido anche per fornitori esterni che, per necessità, devono accedere alle risorse informatiche.

6.2 Compilazione della richiesta di assegnazione

La richiesta di attivazione delle credenziali dovrà essere completa di generalità dell'utente ed elenco dei sistemi informatici per i quali deve essere abilitato l'accesso. Ogni successiva variazione delle abilitazioni di accesso ai sistemi informatici dovrà essere richiesta formalmente all'Amministratore di Sistema o al Responsabile di riferimento.

Le credenziali di autenticazioni consistono in un codice per l'identificazione dell'utente (altresì nominati username, nome utente o user id), assegnato dall'Amministratore di Sistema, ed una relativa password. La password è personale e riservata e dovrà essere conservata e custodita dall'incaricato con la massima diligenza senza divulgarla.

6.3 Robustezza password

La password deve essere di adeguata robustezza: deve essere lunga, formata da lettere maiuscole e minuscole e/o numeri ed eventualmente simboli. Non deve contenere riferimenti agevolmente riconducibili all'utente (username, nomi o date relative alla persona o ad un familiare).

È necessario procedere alla modifica della password a cura dell'utente al primo accesso e, successivamente, almeno ogni sei mesi. Nel caso in cui l'utente svolga mansioni che, in astratto, possano comportare il trattamento di dati personali sensibili, è obbligatorio il cambio password almeno ogni tre mesi.

Nel caso di cessazione del rapporto di lavoro con il dipendente/collaboratore, il Responsabile dell'Ufficio/area di riferimento dovrà comunicare formalmente e preventivamente all'Amministratore di Sistema la data effettiva a partire dalla quale le credenziali saranno disabilitate.

7. Utilizzo infrastruttura di rete e FileSystem

7.1 Accesso alla rete e condivisione di file

Per l'accesso alle risorse informatiche della Società attraverso la rete locale, ciascun utente deve essere in possesso di credenziali di autenticazione secondo l'art. 6.1.

È assolutamente proibito accedere alla rete ed ai sistemi informatici utilizzando credenziali di altre persone.

L'accesso alla rete garantisce all'utente la disponibilità di condivisioni di rete (cartelle su server) nelle quali vanno inseriti e salvati i file di lavoro, organizzati per area o ufficio o per diversi criteri o per obiettivi specifici di lavoro. Tutte le cartelle di rete, siano esse condivise o personali, possono ospitare esclusivamente contenuti professionali. Pertanto, è vietato il salvataggio sui server della Società, ovvero sugli Strumenti, di documenti non inerenti all'attività lavorativa, quali a titolo esemplificativo documenti, fotografie, video, musica, pratiche personali, sms, mail personali, film e quant'altro.

Ogni materiale personale rilevato dall'Amministratore di Sistema a seguito di interventi di sicurezza informatica ovvero di manutenzione/aggiornamento su server ed anche su Strumenti viene rimosso secondo le regole previste nel successivo punto 13 del presente Regolamento, ferma ogni ulteriore responsabilità civile, penale e disciplinare.

Tutte le risorse di memorizzazione che fanno parte materialmente del corpo dello Strumento informatico, diverse da quelle citate al punto precedente, non sono sottoposte al controllo regolare dell'Amministratore di Sistema e non sono oggetto di backup periodici. A titolo di esempio e non esaustivo si citano: il disco C o altri dischi locali dei singoli PC, la cartella "Documenti" o "Desktop" dell'utente. Tutte queste aree di memorizzazione non devono ospitare dati di interesse, poiché non sono garantite la sicurezza e la protezione contro la eventuale perdita di dati. Pertanto, la responsabilità dei salvataggi dei dati ivi contenuti è a carico del singolo utente.

7.2 Device esterni di archiviazione file

Senza il consenso del Titolare, è vietato trasferire documenti elettronici dai sistemi informatici e Strumenti della Società a device esterni (hard disk, USB-pendrive, CD, DVD e altri supporti). Senza il consenso dell'Amministratore di Sistema è vietato salvare documenti elettronici della Società (ad esempio pervenuti via mail o salvati sul Server o sullo Strumento in dotazione) su repository esterne (quali ad esempio Dropbox, GoogleDrive, OneDrive, ecc.) ovvero inviandoli a terzi via posta elettronica o con altri sistemi.

7.3 Pulizia degli archivi file

Con regolare periodicità (almeno una volta al mese), ciascun utente provvede alla pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati, essendo infatti necessario evitare un'archiviazione ridondante.

7.4 VPN

La Società, nei casi ritenuti utili ai fini lavorativi, mette a disposizione dei propri utenti la possibilità di accedere alle proprie risorse informatiche anche dall'esterno mediante rete VPN (Virtual Private Network), un canale privato e criptato verso la rete interna.

L'accesso mediante VPN viene concesso a consulenti, professionisti, tecnici e fornitori che nell'ambito di un rapporto contrattuale con la Società necessitano di accedere a determinate risorse informatiche. Viene concesso, altresì, a dipendenti e funzionari della Società che

necessitano di svolgere compiti specifici, pur non essendo presenti in sede. Le richieste di abilitazione all'accesso mediante VPN dovranno seguire le prescrizioni del punto 6.1.

7.5 Wi-Fi

7.5.1 Tipologia di reti

All'interno delle sedi societarie è resa disponibile anche una rete senza fili, comunemente definito "Wi-Fi". Esistono più reti disponibili: Vfm_Net (attraverso la quale si può accedere a tutti i livelli, compreso il server – è la soluzione utilizzata dall'Amministratore di Sistema e da pochi addetti), Vfm_Mob (attraverso la quale si può accedere solo alla rete aziendale – è la soluzione tipica degli utenti pc); Vfm_Guest (attraverso la quale si può accedere solo ad internet – è la soluzione tipica per i collaboratori esterni o per chi non ha necessità di entrare nella rete).

Tali reti consentono l'accesso alle risorse e ad internet per i dispositivi non connessi alla rete LAN mediante cavo.

7.5.2 Accesso da parte di persone esterne all'azienda

L'accesso mediante rete Wi-Fi viene concesso a consulenti, professionisti, tecnici e fornitori che nell'ambito di un rapporto contrattuale con la Società necessitano di accedere a determinate risorse informatiche. Viene concesso, altresì, a dipendenti e funzionari della Società che necessitano di svolgere compiti specifici che non possono essere svolti dalle postazioni fisse. L'impostazione della connessione Wi-Fi sarà effettuata dall'Amministratore di Sistema.

7.5.3 Interruzione della rete

L'Amministratore di Sistema si riserva la facoltà di negare o interrompere l'accesso alla rete mediante dispositivi non adeguatamente protetti e/o aggiornati, che possano costituire una concreta minaccia per la sicurezza informatica.

I log relativi all'uso del File System e della intranet, nonché i file salvati o trattati su Server o Strumenti, sono registrati e possono essere oggetto di controllo da parte del Titolare del trattamento, attraverso l'Amministratore di Sistema, per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio.

I controlli possono avvenire secondo le disposizioni previste al successivo punto 13 del presente Regolamento.

Le informazioni così raccolte sono altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, compresa la verifica del rispetto del presente Regolamento, che costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli ai sensi del Regolamento Europeo 679/16 "General Data Protection Regulation".

8. Utilizzo degli Strumenti elettronici (PC, notebook e altri strumenti con relativi software e applicativi)

Il dipendente/collaboratore è consapevole che gli Strumenti forniti sono di proprietà della Società e devono essere utilizzati esclusivamente per rendere la prestazione lavorativa. Ognuno è responsabile dell'utilizzo delle dotazioni informatiche ricevute in assegnazione. Ogni utilizzo non inerente all'attività lavorativa è vietato in quanto può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. Ciascun dipendente /collaboratore si deve quindi attenere alle seguenti regole di utilizzo degli Strumenti.

L'accesso agli Strumenti è protetto da password; per l'accesso devono essere utilizzati Username e password assegnate dall'Amministratore di Sistema (cfr. punto 6). A tal proposito si rammenta che essi sono strettamente personali e l'utente è tenuto a conservarli nella massima segretezza.

Il Personal Computer, notebook, tablet ed ogni altro hardware deve essere custodito con cura da parte degli assegnatari evitando ogni possibile forma di danneggiamento e segnalando tempestivamente all'Amministratore di Sistema ogni malfunzionamento e/o danneggiamento. Non è consentita l'attivazione della password d'accensione (BIOS), senza preventiva autorizzazione da parte dell'Amministratore di Sistema.

Non è consentito all'utente modificare le caratteristiche hardware e software impostate sugli Strumenti assegnati, salvo preventiva autorizzazione da parte dell'Amministratore di Sistema. L'utente è tenuto a scollegarsi dal sistema, o bloccare l'accesso, ogni qualvolta sia costretto ad assentarsi dal locale nel quale è ubicata la stazione di lavoro (PC) o nel caso ritenga di non essere in grado di presidiare l'accesso alla medesima: lasciare un PC incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso.

Le informazioni archiviate sul PC locale devono essere esclusivamente quelle necessarie all'attività lavorativa assegnata.

La gestione dei dati su PC è demandata all'utente utilizzatore che dovrà provvedere a memorizzare sulle condivisioni i dati che possono essere utilizzati anche da altri utenti, evitando di mantenere l'esclusività su di essi. Non è consentita l'installazione di programmi diversi da quelli autorizzati dall'Amministratore di Sistema.

L'Amministratore di Sistema può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosa per la sicurezza dei PC, per la rete locale e server, nonché potrà cambiare tutte le impostazioni eventualmente configurate che possano interferire con il corretto funzionamento dei servizi informatici.

È obbligatorio consentire l'installazione degli aggiornamenti di sistema che vengono proposti automaticamente, al primo momento disponibile, in modo tale da mantenere il PC sempre protetto.

È vietato utilizzare il PC per l'acquisizione, la duplicazione e/o la trasmissione illegale di opere protette da copyright.

È vietato l'utilizzo di supporti di memoria (USB-pendrive, CD, DVD o altri supporti) per il salvataggio di dati trattati tramite gli Strumenti, salvo che il supporto utilizzato sia stato fornito dall'Amministratore di Sistema. In tale caso, il supporto fornito può essere utilizzato esclusivamente per finalità lavorative.

È assolutamente vietato connettere al PC qualsiasi periferica non autorizzata preventivamente dall'Amministratore di Sistema.

È assolutamente vietato connettere alla rete locale qualsiasi dispositivo (PC esterni, router, switch, modem, etc.) non autorizzato preventivamente dall'Amministratore di Sistema.

Nel caso in cui l'utente dovesse notare comportamenti anomali del PC, l'utente è tenuto a comunicarlo tempestivamente all'Amministratore di Sistema.

I log relativi all'utilizzo di Strumenti, reperibili nella memoria degli Strumenti stessi ovvero sui Server o sui router, nonché i file con essi trattati sono registrati e possono essere oggetto di controllo da parte del Titolare del trattamento, attraverso l'Amministratore di Sistema, per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio.

Le informazioni così raccolte sono altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, compresa la verifica del rispetto del presente Regolamento, che costituisce adeguata

informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli ai sensi del Regolamento Europeo 679/16 “General Data Protection”.

9. Utilizzo di internet

Le regole di seguito specificate sono adottate anche ai sensi delle “Linee guida del Garante per posta elettronica e internet” pubblicate in Gazzetta Ufficiale n. 58 del 10 marzo 2007. Ciascun dipendente /collaboratore si deve attenere alle seguenti regole di utilizzo della rete Internet e dei relativi servizi.

È ammessa solo la navigazione in siti considerati correlati con la prestazione lavorativa. L'accesso è consentito dal proxy con le sue policy di sicurezza debitamente implementate e aggiornate, ad es. i siti istituzionali, i siti degli Enti locali, di fornitori e partner.

È vietato compiere azioni che siano potenzialmente in grado di arrecare danno alla Società, ad esempio, il download o l'upload di file audio e/o video, l'uso di servizi di rete con finalità ludiche o, comunque, estranee all'attività lavorativa.

È vietato a chiunque il download di qualunque tipo di software gratuito (freeware) o shareware prelevato da siti Internet, se non espressamente autorizzato dagli Amministratori di Sistema. La Società si riserva di bloccare l'accesso a siti “a rischio” attraverso l'utilizzo di blacklist pubbliche in continuo aggiornamento e di predisporre filtri, basati su sistemi euristici di valutazione del livello di sicurezza dei siti web remoti, tali da prevenire operazioni potenzialmente pericolose o comportamenti impropri. In caso di blocco accidentale di siti di interesse, potrà contattare l'Amministratore di Sistema per uno sblocco selettivo.

Nel caso in cui, per ragioni di servizio, si necessiti di una navigazione libera dai filtri, è necessario richiedere lo sblocco mediante una mail indirizzata all'Amministratore di Sistema, ed in copia alla Direzione Generale, nella quale siano indicati chiaramente: motivo della richiesta, utente e postazione da cui effettuare la navigazione libera, intervallo di tempo richiesto per completare l'attività. L'utente, nello svolgimento delle proprie attività, deve comunque tenere presente in modo particolare il punto 13 del presente regolamento. Al termine dell'attività l'Amministratore di Sistema ripristinerà i filtri alla situazione iniziale.

È tassativamente vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, salvo i casi direttamente autorizzati dalla Direzione Generale e dall'Amministratore di Sistema, con il rispetto delle normali procedure di acquisto.

È assolutamente vietato l'utilizzo di abbonamenti privati per effettuare la connessione a Internet tranne in casi del tutto eccezionali e previa autorizzazione dell'Amministratore di Sistema e della Direzione Generale.

È assolutamente vietata la partecipazione a Forum non professionali, ai Social Network, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames).

È consentito l'uso di strumenti di messaggistica istantanea, per permettere una efficace e comoda comunicazione tra i colleghi, mediante i soli strumenti autorizzati dall'Amministratore di Sistema. Tali strumenti hanno lo scopo di migliorare la collaborazione tra utenti aggiungendo un ulteriore canale comunicativo rispetto agli spostamenti fisici, alle chiamate telefoniche ed e-mail. È consentito un utilizzo legato esclusivamente a scopi professionali. Anche su tali strumenti di messaggistica istantanea è attivo il monitoraggio e la registrazione dell'attività degli utenti, secondo le disposizioni del punto 13 del presente regolamento.

Per motivi tecnici e di buon funzionamento del sistema informatico è buona norma, salvo comprovata necessità, non accedere a risorse web che impegnino in modo rilevante banda, come a titolo esemplificativo: filmati (tratti da youtube, siti di informazione, siti di streaming ecc) o web radio, in quanto possono limitare e/o compromettere l'uso della rete agli altri utenti.

Si informa che la Società, per il tramite dell'Amministratore di Sistema, non effettua la memorizzazione sistematica delle pagine web visualizzate dal singolo utente, né controlla con sistemi automatici i dati di navigazione dello stesso.

10. Utilizzo della posta elettronica

Le regole di seguito specificate sono adottate anche ai sensi delle "Linee guida del Garante per posta elettronica e internet" pubblicate in Gazzetta Ufficiale n. 58 del 10 marzo 2007. Ciascun dipendente/collaboratore si deve attenere alle seguenti regole di utilizzo dell'indirizzo di Posta elettronica.

Ad ogni utente viene fornito un account e-mail nominativo, generalmente coerente con il modello nome.cognome@vefim.it.

L'utilizzo dell'e-mail deve essere limitato esclusivamente a scopi lavorativi, ed è assolutamente vietato ogni utilizzo di tipo privato. L'utente a cui è assegnata una casella di posta elettronica è responsabile del corretto utilizzo della stessa.

La Società fornisce, altresì, delle caselle di posta elettronica associate a ciascuna unità organizzativa, ufficio o gruppo di lavoro il cui utilizzo è da preferire rispetto alle e-mail nominative qualora le comunicazioni siano di interesse collettivo: questo per evitare che degli utenti singoli mantengano l'esclusività su dati.

L'iscrizione a mailing-list o newsletter esterne con l'indirizzo ricevuto è concessa esclusivamente per motivi professionali e dopo richiesta accettata dall'Amministratore di Sistema. Prima di iscriversi occorre verificare anticipatamente l'affidabilità del sito che offre il servizio.

Allo scopo di garantire sicurezza alla rete, evitare di aprire messaggi di posta in arrivo da mittenti di cui non si conosce l'identità o con contenuto sospetto o insolito, oppure che contengano allegati di tipo *.exe, *.com, *.vbs, *.htm, *.scr, *.bat, *.js e *.pif. È necessario porre molta attenzione, inoltre, alla credibilità del messaggio e del mittente per evitare casi di phishing o frodi informatiche.

In qualunque situazione di incertezza contattare l'Amministratore di Sistema per una valutazione dei singoli casi.

Non è consentito diffondere messaggi del tipo "catena di S. Antonio" o di tipologia simile anche se il contenuto sembra meritevole di attenzione; in particolare gli appelli di solidarietà e i messaggi che informano dell'esistenza di nuovi virus. In generale è vietato l'invio di messaggi pubblicitari di prodotti di qualsiasi tipo.

Nel caso fosse necessario inviare allegati "pesanti" (fino a 10 MB) è opportuno ricorrere prima alla compressione dei file originali in un archivio di formato .zip o equivalenti. Nel caso di allegati ancora più voluminosi è necessario rivolgersi all'Amministratore di Sistema.

Nel caso in cui fosse necessario inviare a destinatari esterni messaggi contenenti allegati con dati personali o dati personali sensibili, è obbligatorio che questi allegati vengano preventivamente resi inintelligibili attraverso crittazione con apposito software (archiviazione e compressione con password). La password di crittazione deve essere comunicata al destinatario attraverso un canale diverso dalla mail (ad esempio per lettera o per telefono) e

mai assieme ai dati criptati. Tutte le informazioni, i dati personali e/o sensibili di competenza le possono essere inviati soltanto a destinatari - persone o Enti – qualificati e competenti. Non è consentito l’invio automatico di e-mail all’indirizzo e-mail privato (attivando per esempio un “inoltrato” automatico delle e-mail entranti), anche durante i periodi di assenza (es. ferie, malattia, infortunio ecc.). In questa ultima ipotesi, è raccomandabile utilizzare un messaggio “Out of Office” facendo menzione di chi, all’interno della Società, assumerà le mansioni durante l’assenza, oppure indicando un indirizzo di mail alternativo preferibilmente di tipo collettivo, tipo ufficio....@vefim.it. Rivolgersi all’Amministratore di Sistema per tale eventualità.

In caso di assenza improvvisa o prolungata e per improrogabili necessità legate all’attività lavorativa, qualora non fosse possibile attivare la funzione autoreply o l’inoltrato automatico su altre caselle e si debba conoscere il contenuto dei messaggi di posta elettronica, il titolare della casella di posta ha la facoltà di delegare un altro dipendente (fiduciario) per verificare il contenuto di messaggi e per inoltrare al Titolare del trattamento quelli ritenuti rilevanti per lo svolgimento dell’attività lavorativa.

Sarà compito del Dirigente responsabile assicurarsi che sia redatto un verbale attestante quanto avvenuto e che si sia informato il lavoratore interessato alla prima occasione utile. La diffusione massiva di messaggi di posta elettronica deve essere effettuata esclusivamente per motivi inerenti al servizio, su autorizzazione del Dirigente responsabile competente. Per evitare che le eventuali risposte siano inoltrate a tutti, generando traffico eccessivo ed indesiderato, i destinatari dovranno essere messi in copia nascosta (Bcc o Ccn) se la tipologia del messaggio lo consente.

È vietato inviare messaggi di posta elettronica in nome e per conto di un altro utente, salvo sua espressa autorizzazione.

La casella di posta elettronica personale deve essere mantenuta in ordine, cancellando messaggi e documenti la cui conservazione non è più necessaria. Anche la conservazione di messaggi con allegati pesanti è da evitare per quanto possibile, preferendo, in alternativa, il salvataggio dell’allegato sulle condivisioni.

I messaggi in entrata vengono sistematicamente analizzati alla ricerca di virus e malware e per l’eliminazione dello spam. I messaggi che dovessero contenere virus vengono eliminati dal sistema e il mittente/destinatario viene avvisato mediante messaggio specifico.

Si informa che la Società, per il tramite dell’Amministratore di Sistema, non controlla sistematicamente il flusso di comunicazioni mail né è dotato di sistemi per la lettura o analisi sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio e-mail.

Tuttavia, in caso di assenza improvvisa o prolungata del dipendente ovvero per imprescindibili esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio ovvero per motivi di sicurezza del sistema informatico, la Società tramite l’Amministratore di Sistema può, secondo le procedure indicate successivo punto 13 del presente Regolamento, accedere all’account di posta elettronica, prendendo visione dei messaggi, salvando o cancellando file.

Si informa che, in caso di cessazione del rapporto lavorativo, la mail affidata all’incaricato verrà sospesa per un periodo limitato e successivamente disattivata. Nel periodo di sospensione l’account rimarrà attivo e visibile ad un soggetto incaricato dalla Società solo in ricezione, che tratterà i dati e le informazioni pervenute per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio, trasmettendone il contenuto ad altri dipendenti (se il messaggio ha contenuto lavorativo) ovvero

cancellandolo (se il messaggio non ha contenuto lavorativo). Il sistema in ogni caso genererà una risposta automatica al mittente, invitandolo a reinviare il messaggio ad altro indirizzo mail.

Le informazioni eventualmente raccolte sono altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, compresa la verifica del rispetto del presente Regolamento, che costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli ai sensi del Regolamento Europeo 679/16 “General Data Protection Regulation”.

11. Utilizzo dei telefoni, fax, fotocopiatrici, scanner e stampanti

Il dipendente è consapevole che gli strumenti di stampa, così come anche il telefono, sono di proprietà della Società e sono resi disponibili all'utente per rendere la prestazione lavorativa. Pertanto, ne viene concesso l'uso esclusivamente per tale fine.

Il telefono affidato all'utente è uno strumento di lavoro. Ne viene concesso l'uso esclusivamente per lo svolgimento dell'attività lavorativa e non sono quindi consentite comunicazioni a carattere personale e/o non strettamente inerenti all'attività lavorativa stessa. La ricezione o l'effettuazione di comunicazioni a carattere personale è consentito solo nel caso di comprovata necessità ed urgenza.

Qualora venisse assegnato un cellulare all'utente, quest'ultimo sarà responsabile del suo utilizzo e della sua custodia. Ai cellulari e smartphone si applicano le medesime regole sopra previste per gli altri dispositivi informatici, per quanto riguarda il mantenimento di un adeguato livello di sicurezza informatica. In particolare, si raccomanda il rispetto delle regole per una corretta navigazione in Internet, se consentita.

Per gli smartphone è vietata l'installazione e l'utilizzo di applicazioni (o altresì denominate “app” nel contesto degli smartphone) diverse da quelle autorizzate dall'Amministratore di Sistema.

È vietato l'utilizzo dei fax per fini personali, tanto per spedire quanto per ricevere documentazione, fatta salva esplicita autorizzazione da parte del Responsabile di Ufficio.

È vietato l'utilizzo delle fotocopiatrici per fini personali, salvo preventiva ed esplicita autorizzazione da parte del Responsabile di Ufficio.

Per quanto concerne l'uso delle stampanti gli utenti sono tenuti a:

- Stampare documenti solo se strettamente necessari per lo svolgimento delle proprie funzioni
- Prediligere le stampanti di rete condivise, rispetto a quelle locali/personali, per ridurre l'utilizzo di materiali di consumo (toner ed altri consumabili);
- Prediligere la stampa in bianco/nero e fronte/retro al fine di ridurre i costi, se possibile.

Le stampanti e le fotocopiatrici devono essere spente ogni sera prima di lasciare gli uffici o in caso di inutilizzo prolungato.

Nel caso in cui si rendesse necessaria la stampa di informazioni riservate l'utente dovrà presidiare il dispositivo di stampa per evitare la possibile perdita o divulgazione di tali informazioni e persone terze non autorizzate.

12. Assistenza agli utenti e manutenzioni

L'Amministratore di Sistema può accedere ai dispositivi informatici sia direttamente, sia mediante software di accesso remoto, per i seguenti scopi:

- verifica e risoluzione di problemi sistemistici ed applicativi, su segnalazione dell'utente finale;

- verifica del corretto funzionamento dei singoli dispositivi in caso di problemi rilevati nella rete;
- richieste di aggiornamento software e manutenzione preventiva hardware e software.

Gli interventi tecnici possono avvenire previo consenso dell'utente, quando l'intervento stesso richiede l'accesso ad aree personali dell'utente stesso. Qualora l'intervento tecnico in loco o in remoto non necessiti di accedere mediante credenziali utente, l'Amministratore di Sistema è autorizzato ad effettuare gli interventi senza il consenso dell'utente cui la risorsa è assegnata.

L'accesso in teleassistenza sui PC della rete richiesto da terzi (fornitori e/o altri) deve essere autorizzato dall'Amministratore di Sistema, per le verifiche delle modalità di intervento per il primo accesso. Le richieste successive, se effettuate con la medesima modalità, possono essere gestite autonomamente dall'utente finale.

Durante gli interventi in teleassistenza da parte di operatori terzi, l'utente richiedente o l'Amministratore di Sistema deve presenziare la sessione remota, in modo tale da verificare ed impedire eventuali comportamenti non conformi al presente regolamento.

13. Controlli sugli Strumenti

Poiché in caso di violazioni contrattuali e giuridiche, sia il datore di lavoro, sia il singolo lavoratore sono potenzialmente perseguibili con sanzioni, anche di natura penale, la Società verificherà, nei limiti consentiti dalle norme legali e contrattuali, il rispetto delle regole e l'integrità del proprio sistema informatico. Il datore di lavoro, infatti, può avvalersi legittimamente di sistemi che consentono indirettamente il controllo a distanza (cosiddetto controllo preterintenzionale) e determinano un trattamento di dati personali riferiti o riferibili ai lavoratori. Resta ferma la necessità di rispettare le procedure di informazione e di consultazione di lavoratori e sindacati in relazione all'introduzione o alla modifica di sistemi automatizzati per la raccolta e l'utilizzazione dei dati, nonché in caso di introduzione o di modificazione di procedimenti tecnici destinati a controllare i movimenti o la produttività dei lavoratori. I controlli devono essere effettuati nel rispetto del presente Regolamento e dei seguenti principi:

- **Proporzionalità:** il controllo e l'estensione dello stesso dovrà rivestire, in ogni caso, un carattere adeguato, pertinente e non eccessivo rispetto alla/alle finalità perseguite, ma resterà sempre entro i limiti minimi.
- **Trasparenza:** l'adozione del presente Regolamento ha l'obiettivo di informare gli utenti sui diritti ed i doveri di entrambe le parti.
- **Pertinenza e non eccedenza:** ovvero evitando un'interferenza ingiustificata sui diritti e sulle libertà fondamentali dei lavoratori, così come la possibilità di controlli prolungati, costanti o indiscriminati.

L'uso degli Strumenti Informatici della Società può lasciare traccia delle informazioni sul relativo uso, come analiticamente spiegato nel presente Regolamento. Tali informazioni, che possono contenere dati personali eventualmente anche sensibili dell'utente, possono essere oggetto di controlli da parte della Società, per il tramite dell'Amministratore di Sistema, volti a garantire esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio, nonché per la sicurezza e la salvaguardia del sistema informatico, per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento / sostituzione / implementazione di programmi, manutenzione hardware, etc.). Gli interventi di controllo sono di due tipi (di seguito descritti al punto 13.1 e 13.2) e possono permettere alla Società di prendere indirettamente cognizione dell'attività svolta con gli Strumenti.

13.1 Controlli per la tutela del patrimonio, nonché per la sicurezza e la salvaguardia del sistema informatico. Controlli per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, etc.).

Qualora per le finalità qui sopra descritte risulti necessario l'accesso agli Strumenti e alle risorse informatiche e relative informazioni il Responsabile del trattamento dei dati personali per il tramite dell'Amministratore di Sistema, si atterrà al processo descritto qui di seguito (se e in quanto compatibile con lo Strumento oggetto di controllo).

- 1) Avviso generico a tutti i dipendenti della presenza di comportamenti anomali che possono mettere a rischio la sicurezza del sistema informativo e richiamo all'esigenza di attenersi al rispetto del presente Regolamento.
- 2) Successivamente, dopo almeno 7 giorni, se il comportamento anomalo persiste, la Società potrà autorizzare il personale addetto al controllo, potendo così accedere alle informazioni con possibilità di rilevare files trattati, siti web visitati, software installati, documenti scaricati, statistiche sull'uso di risorse ecc. nel corso dell'attività lavorativa. Tale attività potrà essere effettuata in forma anonima ovvero tramite controllo del numero IP, dell'utente e con l'identificazione del soggetto che non si attiene alle istruzioni impartite.
- 3) Qualora il rischio di compromissione del sistema informativo sia imminente e grave a tal punto da non permettere l'attesa dei tempi necessari per i passaggi procedurali descritti ai punti 1 e 2, il Responsabile del Trattamento, unitamente all'Amministratore di Sistema, potrà intervenire senza indugio sullo strumento da cui proviene la potenziale minaccia.

13.2 Controlli per esigenze produttive e di organizzazione

Per esigenze produttive e di organizzazione si intendono – fra le altre – l'urgente ed improrogabile necessità di accedere a file o informazioni lavorative di cui si è ragionevolmente certi che siano disponibili su risorse informatiche di un utente (quali file salvati, posta elettronica, chat, SMS, ecc) che non sia reperibile, in quanto ad esempio assente, temporaneamente irreperibile, ovvero cessato.

Qualora risulti necessario l'accesso alle risorse informatiche e relative informazioni il Responsabile del trattamento dei dati personali, per il tramite dell'Amministratore di Sistema, si atterrà alla procedura descritta qui di seguito (se e in quanto compatibile con lo Strumento oggetto di controllo).

- 1) Redazione di un atto da parte del Direttore e/o Responsabile Area che comprovi le necessità produttive e di organizzazione che richiedano l'accesso allo Strumento.
- 2) Incarico all'Amministratore di sistema di accedere alla risorsa con credenziali di Amministratore ovvero tramite l'azzeramento e la contestuale creazione di nuove credenziali di autenticazione dell'utente interessato, con avviso che al primo accesso alla risorsa, lo stesso dovrà inserire nuove credenziali.
- 3) Redazione di un verbale che riassume i passaggi precedenti.
- 4) In ogni caso l'accesso ai documenti presenti nella risorsa è limitato a quanto strettamente indispensabile alle finalità produttive e di organizzazione del lavoro.
- 5) Qualora indirettamente si riscontrino file o informazioni anche personali, esse potranno essere altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, considerato che il presente Regolamento costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli, sempre nel rispetto di quanto disposto dal Regolamento Europeo 679/16 "General Data Protection Regulation".

Tutti i controlli sopra descritti avvengono nel rispetto del principio di necessità e non eccedenza rispetto alle finalità descritte nel presente Regolamento. Dell'attività sopra descritta viene redatto verbale, sottoscritto dal Responsabile del Trattamento e dall'Amministratore di Sistema che ha svolto l'attività.

In caso di nuovo accesso da parte dell'utente allo Strumento informatico oggetto di controllo, lo stesso dovrà avvenire previo rilascio di nuove credenziali (salvo diverse esigenze tecniche). Qualora indirettamente si riscontrino file o informazioni anche personali, esse potranno essere altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, considerato che il presente Regolamento costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli, sempre nel rispetto di quanto disposto dal Regolamento Europeo 679/16 "General Data Protection Regulation".

14. Conservazione dei dati

In riferimento agli articoli 5 e 6 del Reg. 679/16 e in applicazione ai principi di diritto di accesso, legittimità, proporzionalità, sicurezza ed accuratezza e conservazione dei dati, le informazioni relative all'accesso ad Internet e dal traffico telematico (log di sistema e del server proxy), la cui conservazione non sia necessaria, saranno cancellati entro tre mesi dalla loro produzione.

In casi eccezionali – ad esempio: per esigenze tecniche o di sicurezza; o per l'indispensabilità dei dati rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria o, infine, all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria – è consentito il prolungamento dei tempi di conservazione limitatamente al soddisfacimento delle esigenze sopra esplicitate. La Società si impegna ad applicare le misure di sicurezza nel trattamento e nella conservazione di tale tipologia di dati alla luce di quanto stabilito dal Legislatore.

15. Partecipazioni a Social Media

L'utilizzo a fini promozionali e commerciali di blog, forum (anche professionali) o, in generale, siti o social media è gestito ed organizzato esclusivamente dalla Società attraverso specifiche direttive ed istruzioni operative al personale a ciò espressamente addetto, rimanendo escluse iniziative individuali da parte dei singoli utenti o collaboratori.

Fermo restando il diritto della persona alla libertà di espressione, la Società ritiene comunque opportuno indicare agli utenti alcune regole comportamentali, al fine di tutelare tanto la propria immagine ed il patrimonio, anche immateriale, quanto i propri collaboratori, i propri clienti e fornitori, gli altri partners, oltre che gli stessi utenti utilizzatori dei social media, fermo restando che è vietata la partecipazione agli stessi social media durante l'orario di lavoro.

Il presente articolo deve essere osservato dall'utente sia che utilizzi dispositivi messi a disposizione dalla Società, sia che utilizzi propri dispositivi, sia che partecipi ai social media a titolo personale, sia che lo faccia per finalità professionali, come dipendente della Società.

La condivisione dei contenuti nei social media deve sempre rispettare e garantire la segretezza sulle informazioni considerate dalla Società riservate ed in genere, a titolo esemplificativo e non esaustivo, sulle informazioni inerenti attività, dati contabili, finanziari, progetti, procedimenti svolti o in svolgimento presso gli uffici. Inoltre, ogni comunicazione e divulgazione di contenuti dovrà essere effettuata nel pieno rispetto dei diritti di proprietà industriale e dei diritti d'autore, sia di terzi che della Società. L'utente, nelle proprie comunicazioni, non potrà quindi inserire il nominativo e il logo della Società, né potrà

pubblicare disegni, modelli od altro connesso ai citati diritti. Ogni deroga a quanto sopra disposto potrà peraltro avvenire solo previa specifica autorizzazione della Direzione. L'utente deve garantire la tutela della riservatezza e dignità delle persone; di conseguenza, non potrà comunicare o diffondere dati personali (quali dati anagrafici, immagini, video, suoni e voci) di colleghi e in genere di collaboratori, se non con il preventivo personale consenso di questi, e comunque non potrà postare nei social media immagini, video, suoni e voci registrati all'interno dei luoghi di lavoro, se non con il preventivo consenso del Responsabile d'ufficio. Qualora l'utente intenda usare social network, blog, forum su questioni anche indirettamente professionali (es. post su prodotti, servizi, fornitori, partner, ecc.) egli esprimerà unicamente le proprie opinioni personali; pertanto, ove necessario od opportuno per la possibile connessione con la Società, in particolare in forum professionali, l'utente dovrà precisare che le opinioni espresse sono esclusivamente personali e non riconducibili alla Società.

16. Pubblicazione e messa a disposizione

Il presente Regolamento è stato redatto dall'Amministratore di Sistema che è chiamato a garantire il coordinamento degli adempimenti.

La sua pubblicazione, a cura dell'Amministratore di Sistema, avverrà nelle seguenti forme: affissione in luogo accessibile a tutti i lavoratori (art. 7, comma 1. Statuto dei Lavoratori), attraverso l'app aziendale e la sua pubblicazione nel sito internet aziendale.

Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni e modifiche al presente Regolamento tramite comunicazione all'Amministratore di Sistema.

17. Sanzioni disciplinari

È fatto obbligo a tutti i dipendenti/collaboratori/utenti di osservare le disposizioni portate a conoscenza con il presente Regolamento.

Eventuali violazioni del presente Regolamento da parte dei dipendenti nonché di altre norme previste dal CCNL applicato, a seconda della gravità della infrazione, comportano l'adozione dei seguenti provvedimenti:

- censura scritta;
- sospensione dal servizio;
- licenziamento in tronco;
- licenziamento di diritto.

Rimane comunque riservato il diritto di intraprendere azioni civili e penali nei confronti dei responsabili di qualsivoglia violazione a danno dell'Azienda.

Verona, 04/04/2025
Approvato dal Consiglio di Amministrazione
Vefim S.r.l.