REGOLAMENTO
PER L'UTILIZZO DELLA STRUMENTAZIONE INFORMATICA AZIENDALE E DELLA RETE INTERNET

Identificativo del Documento	TGN-L-4-01	REGOLAMENTO PER L'UTILIZZO DELLA STRUMENTAZIONE INFORMATICA AZIENDALE E DELLA RETE INTERNET
Revisione	2	Prima revisione
Redatto da	DPO	Alessandro Circassia;
Verificato	QHSE; HR; IT; GM	Riccardo Masetti; Grazia Ramponi; Fabrizio Schiavo; Melania Fabbri
Emesso	AD	Andrea Tozzi
Data emissione	2/10/2022	

Rev.	Par.	Descrizione della Revisione/*Revision description*
1		**Prima emissione**/ *First issue*
2	17	**Prima revisione**/ *First review* – Revisione della politica di cessazione della mail aziendale.

N° Hold	Par.	Descrizione dell'Hold/*Description of Hold*

REGOLAMENTO PER L'UTILIZZO DELLA STRUMENTAZIONE INFORMATICA AZIENDALE E DELLA RETE INTERNET

****

INDICE

CAPO I – I PRINCIPI

1. SCOPO

Lo scopo del presente disciplinare interno è di definire l'ambito di applicazione, le modalità e le norme sull'utilizzo della strumentazione informatica da parte degli utenti assegnatari (dipendenti, collaboratori etc.), al fine di tutelare i beni aziendali ed evitare condotte inconsapevoli e/o scorrette che potrebbero esporre la Società a problematiche di sicurezza, di immagine e patrimoniali per eventuali danni cagionati anche a terzi.

L'insieme delle norme comportamentali ivi incluse, pertanto, è volto a conformare la Società ai principi di diligenza, informazione e correttezza nell'ambito dei rapporti di lavoro, con l'ulteriore finalità di prevenire eventuali comportamenti illeciti dei dipendenti, pur nel rispetto dei diritti ad essi attribuiti dall'ordinamento giuridico italiano.

A tal fine, pertanto, si rileva che gli eventuali controlli ivi previsti escludono finalità di monitoraggio diretto ed intenzionale dell'attività lavorativa e sono disposti sulla base della vigente normativa, con particolare riferimento a quelle privacy, alla Legge n. 300/1970 (c.d. Statuto dei Lavoratori) alla luce delle modifiche intervenute ad opera del D.lgs. 14 settembre 2015, n. 151 e ai provvedimenti appositamente emanati dall'Autorità Garante (si veda in particolare Provvedimento 1 marzo 2007).

2. APPLICABILITÀ

La presente procedura si applica a tutti i lavoratori degli stabilimenti dell'azienda che siano assegnatari di beni e risorse informatiche aziendali ovvero utilizzatori di servizi e risorse informatiche di pertinenza della Società.

3. TERMINI E DEFINIZIONI

- **Chat**: servizio offerto da Internet, che mediante apposito software permette a più interlocutori di conversare scambiandosi messaggi scritti che appaiono in tempo reale sul monitor di ciascuno;
- **Client**: personal computer collegato in rete a un altro computer (server), sul quale risiedono i dati che il primo utilizza;
- **Computer portatile**: elaboratore elettronico aziendale trasportabile con facilità;
- **E-mail**: messaggio inviato tramite posta elettronica;
- **Società**: l'organizzazione e/o comunque il Titolare dei beni e delle risorse informatiche ivi disciplinate, il quale opererà per mezzo dei soggetti che ne possiedono la rappresentanza.
- **Estensione**: set di tre lettere che segue il nome di un file di un computer e ne identifica il genere;
- **Log**: registrazione ufficiale di eventi;
- **Password**: parola o sigla di riconoscimento fornita dall'utente al computer per poter accedere a un sistema operativo a un programma o a un file;
- **Peer to peer**: sistema di computer collegati gli uni agli altri senza la connessione ad un server;
- **Personal Computer**: elaboratore Elettronico destinato all'uso aziendale;
- **Phishing**: l'attività criminale di mandare e-mail o costituire un sito web al fine di ingannare qualcuno e carpire informazioni (es. numeri di carta di credito o password).
- **Rete Aziendale**: sistema di trasmissione delle informazioni costituito da linee di collegamento e da stazioni che possono essere costituite da elaboratori, terminali o unità di memoria;
- **Server**: computer collegato in rete ad altri computer (client), sul quale risiedono i dati che questi utilizzano;
- **Smartphone**: apparecchio elettronico che combina le funzioni di un telefono cellulare e di un computer palmare.

- **Spamming**: mandare messaggi a diverse persone tramite e-mail o internet generalmente a fini commerciali;
- **Tablet**: elaboratore elettronico aziendale compatto con interfaccia touch;
- **Utente**: colui che si serve di un'attrezzatura di lavoro di pertinenza della Società;

4. TITOLARITÁ DEI BENI E DELLE RISORSE INFORMATICHE

I beni e le risorse informatiche, i servizi ICT e le reti informative costituiscono beni aziendali rientranti nel patrimonio sociale e sono da considerarsi di esclusiva proprietà della Società.

Il loro utilizzo, pertanto, è consentito solo per finalità di adempimento delle mansioni lavorative affidate ad ogni Utente in base al rapporto in essere (ovvero per scopi professionali afferenti all'attività svolta per la Società), e comunque per l'esclusivo perseguimento degli obiettivi aziendali.

A tal fine si precisa sin d'ora che qualsivoglia dato e/o informazione trattato per mezzo dei beni e delle risorse informatiche di proprietà della Società, sarà dalla stessa considerata come avente natura aziendale e non riservata.

5. RESPONSABILITÀ PERSONALE DELL'UTENTE

Ogni Utente è personalmente responsabile dell'utilizzo dei beni e delle risorse informatiche affidatigli dalla Società nonché dei relativi dati trattati per finalità aziendali.

A tal fine ogni Utente, nel rispetto dei principi di diligenza sottesi al rapporto instaurato con la Società, è tenuto a tutelare (per quanto di propria competenza) il patrimonio aziendale da utilizzi impropri e non autorizzati, danni o abusi anche derivanti da negligenza, imprudenza o imperizia. L'obiettivo è quello di preservare l'integrità e la riservatezza dei beni, delle informazioni e delle risorse aziendali.

Ogni Utente, pertanto, è tenuto, in relazioni al proprio ruolo e alle mansioni in concreto svolte, ad operare a tutela della sicurezza informatica aziendale, riportando al proprio responsabile e senza ritardo eventuali rischi di cui è a conoscenza ovvero violazioni del presente disciplinare interno.

Sono severamente vietati comportamenti che possano creare un danno, anche di immagine, alla Società.

6. AGGIORNAMENTO

L'aggiornamento del presente regolamento è competenza delle seguenti aree:

- **IT**;
- **Human Resources** (HR);
- **Legal Affairs** (L).

CAPO II – MISURE ORGANIZZATIVE

7. AMMINISTRATORI DEL SISTEMA

La Società conferisce all'amministratore di sistema il compito di sovrintendere i beni e le risorse informatiche aziendali. I principali compiti, a titolo meramente esemplificativo e non esaustivo sono:

1) gestire l'hardware e il software di tutta la strumentazione informatica di appartenenza della Società;

2) gestire la creazione, l'attivazione, la disattivazione, e tutte le relative attività amministrative degli account di rete e dei relativi privilegi di accesso alle risorse, previamente assegnati agli utenti;

3) monitorare il corretto utilizzo delle risorse di rete, dei computer e degli applicativi affidati agli utenti, purché attività rientranti nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati;

4) creare, modificare, rimuovere o utilizzare qualunque account o privilegio purché attività rientranti nelle normali attività di manutenzione, gestione della sicurezza, e della protezione dei dati;

5) rimuovere software e/o componenti hardware dalle risorse informatiche assegnate agli utenti, purché attività rientranti nelle normali attività di manutenzione, gestione della sicurezza, e della protezione dei dati;

6) provvedere alla sicurezza informatica dei sistemi informativi aziendali, nel rispetto di quanto prescritto dalla normativa privacy;

7) utilizzare le credenziali di accesso di amministratore del sistema per accedere, anche da remoto, ai dati o alle applicazioni presenti su una risorsa informatica assegnata ad un Utente in caso di prolungata assenza, irreperibilità o impedimento dello stesso. Tale ultima attività, tuttavia, deve essere disposta per mezzo di un soggetto che rivesta quantomeno la posizione di Responsabile Privacy all'interno della Società e deve essere limitata altresì al tempo strettamente necessario al compimento delle attività indifferibili per cui è stato richiesto.

I nominativi degli amministratori di sistema della Società sono disponibili su richiesta ai Servizi Informatici.

8. ASSEGNAZIONE DEGLI ACCOUNT E GESTIONE DELLE PASSWORD

Creazione e gestione degli Account

Un account Utente consente l'autenticazione dell'utilizzatore e di conseguenza ne disciplina l'accesso alle risorse informatiche aziendali, per singola postazione lavorativa.

La gestione di tali account segue quanto sotto espressamente previsto:

- l'accesso al proprio account avviene tramite l'utilizzo delle "credenziali di autenticazione" (es. "Username" e "Password"), comunicate all'Utente dall'amministratore di sistema, che le genera, attraverso modalità che ne garantiscano la segretezza. Si chiarisce che la Società potrà prevedere modalità di accesso a multi-fattore (c.d. strong authentication), sia di tipo hardware che software, i quali rientrano nelle logiche specificate nel presente documento;
- le credenziali di autenticazione costituiscono dati aziendali da mantenere strettamente riservati e non è consentito comunicarne gli estremi a terzi;
- se l'Utente ha il sospetto che le proprie credenziali di autenticazione siano state identificate da qualcuno, o il sospetto di un utilizzo non autorizzato del proprio account e delle risorse a questo associate, lo stesso è tenuto a modificare immediatamente la password e/o a segnalare la violazione all'amministratore del sistema nonché al Responsabile privacy di riferimento;
- ogni Utente è responsabile dell'utilizzo del proprio account Utente;
- in base a quanto previsto dal punto n. 10 del Disciplinare Tecnico – Allegato B al Codice della privacy si ricorda che in caso di assenza improvvisa e/o prolungata del lavoratore e per improrogabili necessità legate all'attività lavorativa, per le esigenze produttive aziendali o per la sicurezza ed operatività delle risorse informatiche della Società, questa si riserva la facoltà di accedere a qualsiasi dotazione e/o apparato assegnato in uso all'Utente per mezzo dell'intervento dell'amministratore di sistema.

Gestione e utilizzo delle password

Dopo la prima comunicazione delle credenziali di autenticazione da parte dell'amministratore di sistema, l'Utente ha il compito di modificare, al suo primo utilizzo, la propria password, procedendo allo stesso modo ogni 90 giorni.

L'Utente, nel definire il valore della password, deve rispettare le seguenti regole:

- utilizzare almeno 8 caratteri alfanumerici;
- evitare di includere parti del nome, cognome e/o comunque elementi a lui agevolmente riconducibili;
- evitare l'utilizzo di password comuni e/o prevedibili;
- evitare l'utilizzo di password uguali o simili ad altre utilizzate in precedenza;

- cercare di utilizzare password differenti per ciascun servizio;
- proteggere con la massima cura la riservatezza della password ed utilizzarla entro i limiti di autorizzazione concessi.

Si ricorda che scrivere la password su post-it o altri supporti (ivi compresa la sua memorizzazione sul telefono/smartphone aziendale) non è conforme alla normativa e costituisce violazione del presente disciplinare interno. Fanno eccezione a tale regola i software di gestione delle password preventivamente autorizzati e messi a disposizione dalla Società.

Cessazione degli Account

In caso di cessazione del rapporto di lavoro con l'Utente, le credenziali di autenticazione di cui sopra verranno disabilitate entro un periodo massimo di 48 ore da quella data; entro un mese, invece, si disporrà la definitiva e totale disabilitazione dell'account Utente.

Qualora vi sia richiesta di reset password di un utente a qualsiasi titolo, perché, per esempio, sussiste il dubbio che terzi ne siano venuti a conoscenza o perché dimenticata, l'IT procederà a riassegnare una nuova password temporanea al fine di consentire all'Utente l'accesso ai sistemi presso cui è accreditato, con l'impegno di modificarla subito dopo nei termini sopra individuati.

9. POSTAZIONI DI LAVORO

Per Postazione di Lavoro si intende il complesso unitario di Personal Computer (di seguito, PC), notebook, accessori (telefono fisso, telefono mobile, stampante), periferiche e ogni altro *device* concesso, dalla Società, in utilizzo all'Utente. L'assegnatario di tali beni e strumenti informatici aziendali, pertanto, ha il compito di farne un uso compatibile con i principi di diligenza sanciti nel codice civile.

Al fine di disciplinare un corretto utilizzo di tali beni, la Società ha adottato le regole tecniche, che di seguito si riportano:

- la Postazione di Lavoro, comprenda essa risorse acquistate, noleggiate, o affidate in locazione, rimane di esclusiva proprietà della Società, ed è concesso temporaneamente all'Utente per finalità strettamente attinenti all'attività svolta;
- è dovere di ogni Utente usare la Postazione di Lavoro a lui affidata responsabilmente e professionalmente;
- la Postazione di Lavoro deve essere utilizzata con hardware autorizzato espressamente dalla Società;
- non è consentito modificare la configurazione hardware della Postazione di Lavoro, se non previa autorizzazione scritta della Società;
- non è consentito rimuovere, danneggiare o asportare componenti hardware dalla Postazione di Lavoro;
- non è consentito installare autonomamente sulla Postazione di Lavoro programmi informatici, software ed ogni altro applicativo non autorizzato preventivamente e per scritto dalla Società;
- non è consentito modificare la configurazione software della Postazione di Lavoro, se non previa autorizzazione scritta della Società;
- la Postazione di Lavoro non deve essere lasciata incustodita con le sessioni utenti attive; conseguentemente quando un Utente si allontana dalla propria postazione di lavoro, deve bloccare tastiera e schermo con un programma salvaschermo (screensaver) protetto da password assegnata dalla Società o effettuare il log-out dalla sessione;
- non aprire, specialmente se si lavora in rete, file sospetti e/o di dubbia provenienza;
- controllare che il programma antivirus installato sia aggiornato periodicamente e sia attivo;

- verificare con l'ausilio del programma antivirus in dotazione ogni memoria di massa esterna contenente dati (supporti ottici CD/DVD, memorie SD/USB, ecc.), prima dell'esecuzione dei file in esso contenuti;
- porre la necessaria attenzione sui risultati delle elaborazioni effettuate e sulle eventuali segnalazioni anomale inviate dal personal computer (es. eventuali rallentamenti o crash improvvisi del sistema);
- l'Utente deve segnalare con la massima tempestività alla Società eventuali guasti tecnici, problematiche tecniche o il cattivo funzionamento delle apparecchiature;
- è onere dell'Utente spegnere la Postazione di Lavoro una volta terminata la sessione di lavoro;
- i dispositivi assegnati in particolar modo i dispositivi mobili assegnati, al termine della giornata lavorativa o alla fine del turno, devono essere conservati in un luogo sicuro;
- è fatto divieto di cedere in uso, anche temporaneo, le attrezzature e i beni informatici aziendali a soggetti terzi non autorizzati;
- non è consentito all'Utente caricare o inserire all'interno della Postazione di Lavoro dati personali non attinenti all'attività lavorativa svolta;
- la Società si riserva la facoltà di rimuovere qualsiasi elemento hardware la cui installazione non sia stata dal medesimo appositamente e preventivamente prevista o autorizzata;
- gli apparecchi di proprietà personale dell'Utente quali computer portatili, telefoni cellulari, agende palmari (PDA), hard disk esterni, penne USB, lettori musicali o di altro tipo, fotocamere digitali, ecc. potranno essere collegati alla Postazione di Lavoro esclusivamente per motivi professionali e nel rispetto di quanto previsto nel Capo III articolo 13 del presente documento.

In caso di furto o smarrimento del dispositivo assegnato deve essere immediatamente informati per iscritto gli uffici IT, L e HR.

CAPO III – CRITERI DI UTILIZZO DEGLI STRUMENTI INFORMATICI

10. PERSONAL COMPUTER, COMPUTER PORTATILI

Il personal computer, il computer portatile presente sul proprio posto di lavoro o assegnato sono considerati quali strumenti di lavoro di proprietà della Società, e devono essere utilizzati per compiere mansioni lavorative.

Per quanto concerne la gestione dei computer portatili, l'Utente ha l'obbligo di custodirli con diligenza e in luogo protetto durante gli spostamenti, rimuovendo gli eventuali *file* elaborati prima della sua riconsegna.

Non è consentito all'Utente caricare o inserire all'interno del portatile qualsiasi dato personale non attinente all'attività lavorativa svolta. In ogni caso, al fine di evitare e/o ridurre al minimo la possibile circolazione di dati personali sull'apparecchio, si ricorda agli utenti di cancellare tutti i dati eventualmente presenti prima di consegnare il portatile agli uffici competenti per la restituzione o la riparazione.

Sul server centrale la Società può creare uno spazio riservato all'Utente per la conservazione dei dati, al fine di permettere all'utente di conservare file di lavoro. Il lavoratore è tenuto ad utilizzare detto spazio per conservare esclusivamente dati di natura aziendale in quanto i file in esso contenuti possono essere aperti, spostati e ulteriormente sottoposti a lettura e/o modifica.

Per assicurare la riservatezza e la disponibilità dei dati aziendali, l'Utente è tenuto a conservare i documenti aziendali sugli storage messi a disposizione dalla Società, evitando di conservarli in locale.

Nel caso in cui l'Utente vi conservi, contrariamente alle direttive impartitegli, dati di natura personale, la Società in nessun caso potrà essere ritenuto responsabile della salvaguardia o della perdita di tali dati.

Il personale IT ha la facoltà di collegarsi e visualizzare in remoto il desktop delle singole postazioni PC al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza contro virus, spyware, malware, etc. L'intervento viene effettuato esclusivamente su chiamata dell'utente e in sua presenza o comunque previa sua specifica autorizzazione.

11. SOFTWARE

Premesso che l'installazione di software privi di regolare licenza non è consentita in nessun caso, gli utenti dovranno ottenere espressa autorizzazione della Società (cfr. art. 21) per installare o comunque utilizzare qualsiasi programma o software dotato di licenza non proprietaria ("freeware" o "shareware").

La Società richiama l'attenzione del proprio personale su alcuni aspetti fondamentali che l'Utente è tenuto ad osservare per un corretto utilizzo del software in azienda:

- la Società acquista le licenze d'uso dei software da vari fornitori esterni. L'Utente, pertanto, è soggetto a limitazioni nell'utilizzo di tali programmi e della relativa documentazione e non ha il diritto di riprodurlo in deroga ai diritti concessi. Tutti gli utenti sono quindi tenuti a utilizzare il software entro i limiti specificati nei contratti di licenza;
- non è consentito fare né il download né l'upload tramite internet di software non autorizzato;
- la Società, sulla scorta di quanto disposto dalle normative a tutela della proprietà intellettuale e del diritto d'autore, ricorda che le persone coinvolte nella riproduzione illegale del software sono responsabili sia civilmente che penalmente e quindi possono essere condannate al pagamento dei danni e anche alla reclusione;
- la Società non tollererà la duplicazione illegale del software.

12. DISPOSITIVI MOBILI DI CONNESSIONE (INTERNET KEY)

Agli assegnatari di computer portatili, può essere data in dotazione anche una chiavetta per la connessione alla rete aziendale, volta a facilitare lo svolgimento delle mansioni lavorative anche da remoto.

I suddetti dispositivi devono essere utilizzati esclusivamente sui computer forniti in dotazione dalla Società e non è consentito concederne l'utilizzo a soggetti terzi, né utilizzarli su computer privati.

Specifiche relative ai limiti entro cui l'Utente potrà utilizzare il servizio offerto tramite la chiavetta, sono riportate nella scheda tecnica consegnata all'Utente unitamente al dispositivo di cui sopra.

L'Utente dovrà attenersi ai suddetti limiti, potendo in caso contrario la Società richiedere il rimborso dei costi sostenuti per il superamento degli stessi.

13. DISPOSITIVI DI MEMORIA PORTATILI

Per dispositivi di memoria portatili si intendono tutti quei dispositivi che consentono di copiare o archiviare dati, file o documenti esternamente al computer. Sono considerati tali CD-ROM, DVD, penne o chiavi di memoria USB, fotocamere digitali, dischi rigidi esterni, etc.

L'utilizzo di tali supporti risponde alle direttive che di seguito si riportano:

- gli apparecchi di proprietà personale dell'Utente, quali computer portatili, telefoni cellulari, agende palmari (PDA), hard disk esterni, penne USB, lettori musicali o di altro tipo, fotocamere digitali etc., potranno essere collegati alla Postazione di Lavoro esclusivamente per finalità strettamente legate all'attività lavorativa svolta e solo in casi eccezionali di necessità e urgenza, e comunque nel rispetto delle disposizioni definite nel presente documento per i corrispondenti dispositivi aziendali;

- una volta connessi all'infrastruttura informatica della Società, i dispositivi saranno soggetti (ove compatibili) al presente disciplinare interno;

- i dati caricati sui dispositivi di memoria portatili non possono in alcun modo essere divulgati all'esterno;

- è onere dell'Utente custodire i dispositivi di memoria portatili contenenti dati particolari (ex dati sensibili) e giudiziari utilizzando particolari accortezze (utilizzando per esempio armadi provvisti di una chiusura a chiave) onde evitare che il loro contenuto possa essere trafugato e/o alterato e/o distrutto.

14. STAMPANTI, FOTOCOPIATRICI E FAX

L'utilizzo dei suddetti strumenti deve avvenire sempre per scopi professionali. Non è consentito un utilizzo per fini diversi o privati, salvo una specifica autorizzazione da parte della Società.

L'utilizzo delle stampanti è subordinato all'inserimento da parte dell'utente delle proprie credenziali tramite autenticazione con badge personale aziendale.

È richiesta una particolare attenzione quando si invia su una stampante condivisa documenti aventi ad oggetto dati personali o informazioni riservate; ciò al fine di evitare che persone non autorizzate possano venirne a conoscenza. Si richiede quindi di evitare di lasciare le stampe incustodite e ritirarne immediatamente le copie non appena uscite dalla stampa.

L'utilizzo dei fax per l'invio di documenti che hanno natura strettamente confidenziale, è generalmente da evitare. Nei casi in cui questo sia necessario, si deve preventivamente avvisare il destinatario, in modo da ridurre il rischio che persone non autorizzate possano venirne a conoscenza, e successivamente chiedere la conferma telefonica di avvenuta ricezione.

15. STRUMENTI DI FONIA MOBILE E/O DI CONNETTIVITÁ IN MOBILITÁ

L'azienda mette a disposizione, a seconda del ruolo o della funzione del singolo Utente, impianti di telefonia fissa e mobile, nonché dispositivi - quali smartphone e tablet - che consentono di usufruire della navigazione in internet tramite rete dati e/o del servizio di telefonica tramite rete cellulare.

Specifiche relative ai limiti entro cui l'Utente potrà utilizzare tali strumenti sono riportate nella scheda tecnica consegnata all'Utente unitamente ai dispositivi di cui sopra.

L'Utente dovrà attenersi ai suddetti limiti, potendo in caso contrario la Società richiedere il rimborso dei costi sostenuti per il superamento degli stessi.

Come per qualsiasi altra dotazione aziendale, il dispositivo mobile rappresenta un bene aziendale che è dato in uso per scopi lavorativi. È tuttavia concesso un utilizzo personale sporadico e moderato dei telefoni aziendali utilizzando la c.d. "*diligenza del buon padre di famiglia*" e comunque tale da non ledere il rapporto fiduciario instaurato con il proprio datore di lavoro (Società).

A tal fine si informano gli utilizzatori dei servizi di fonia aziendale, che la Società eserciterà i diritti, richiedendo ai provider di telefonia i dettagli necessari ad effettuare controlli sull'utilizzo ed i relativi costi di traffico effettuato nel tempo.

I controlli saranno eseguiti secondo le modalità descritte all'art. 18 del presente disciplinare interno.

La Società si riserva la facoltà, qualora dall'esame del traffico di una singola utenza rilevi uno scostamento significativo rispetto alla media del consumo, di richiedere un tabulato analitico delle chiamate effettuate dalla SIM in incarico all'Utente per il periodo interessato.

La Società precisa che tutte le utenze utilizzate per la fonia aziendale, alla cessazione del rapporto, resteranno in dotazione alla società.

L'utilizzo dei dispositivi ivi disciplinati risponde alle regole che di seguito si riportano:

- ogni Utente assegnatario del dispositivo è responsabile dell'uso appropriato dello stesso, e, conseguentemente, anche della sua diligente conservazione.

I dispositivi devono essere dotati di strumenti di autenticazione che ne impedisca l'utilizzo da parte di soggetti non autorizzati. A tal fine si precisa che:

• il CODICE PIN dovrà essere composto di almeno n. 4 cifre numeriche o altro sistema disponibile sul device;

• il CODICE PIN dovrà essere modificato dall'assegnatario con cadenza al massimo semestrale;

• ogni Utente deve adottare le necessarie e dovute cautele per assicurare la segretezza della password e, qualora ritenga che un soggetto non autorizzato possa esserne venuto a conoscenza, dovrà provvedere immediatamente a cambiarla dando comunque comunicazione del fatto alla Società;

- in caso di danneggiamento l'Utente assegnatario dovrà darne immediato avviso alla Società, in caso di furto o smarrimento del dispositivo mobile in oggetto, l'Utente assegnatario dovrà denunciare il fatto alle competenti autorità pubbliche e darne successivo avviso alla Società; ove detti eventi siano riconducibili ad un comportamento negligente, imprudente dell'Utente e/o comunque a sua colpa nella custodia del bene, lo stesso sarà ritenuto unico responsabile dei danni derivanti;

- in caso di furto o smarrimento la Società si riserva la facoltà di attuare la procedura di remote-wipe (cancellazione da remoto di tutti i dati sul dispositivo), rendendo il dispositivo inutilizzabile e i dati in esso contenuti irrecuperabili;

- non è consentito all'Utente caricare o inserire all'interno del dispositivo o SIM qualsiasi dato personale non attinente con l'attività lavorativa svolta. In ogni caso, al fine di evitare e/o ridurre al minimo la possibile circolazione di dati personali sull'apparecchio, si ricorda agli assegnatari di cancellare tutti i dati eventualmente presenti prima di consegnare il cellulare agli uffici competenti per la restituzione o la riparazione;

- non è in generale consentito all'Utente effettuare riprese, fotografie, registrazioni di suoni con qualsiasi tipologia di apparecchiatura elettronica adatta a tali scopi che esulino dall'attività lavorativa; le attività appena elencate possono tuttavia essere attuate dall'Utente sporadicamente e con le dovute cautele del caso;

- non è consentito all'Utente effettuare procedure di jailbreak, modifiche del firmware o procedure di sblocco a vario titolo, tali da permettere l'illegittima installazione di software e/o applicazioni coperte da copyright;

- è onere dell'Utente mantenere installato software antivirus sullo smartphone aziendale; in caso di problemi l'Utente potrà rivolgersi al Personale IT competente;

- l'eventuale installazione di applicazioni, sia gratuite che a pagamento, sugli smartphone e tablet deve essere espressamente autorizzata, rimanendo, diversamente, a carico dell'Utente le spese che la Società dovrà sostenere, nonché le responsabilità derivanti dall'installazione non autorizzata;

- salvo diversi specifici accordi, al momento della consegna del tablet o smartphone l'Utente è tenuto a verificare la disattivazione del sistema di geolocalizzazione potenzialmente attivabile sugli smartphone e tablet, consapevole che, in caso contrario, l'Azienda potrebbe venire a conoscenza, seppur incidentalmente, dei dati relativi alla posizione del dispositivo stesso e del suo assegnatario;

- per motivi di sicurezza sul lavoro i dipendenti devono limitare l'uso dei telefoni privati a casi eccezionali e devono sempre subordinare l'uso di suddette apparecchiature alla sicurezza personale e alla sicurezza e produttività degli impianti, ponendosi in posizione sicura per sé e per gli altri. In particolare, per chi opera sulle linee di produzione o su mezzi aziendali, quali auto o mezzi d'opera, l'uso di telefoni mobili privati così come aziendali è invece tassativamente vietato.

CAPO IV – GESTIONE DELLE COMUNICAZIONI TELEMATICHE

16. GESTIONE UTILIZZO DELLA RETE INTERNET

Ogni Utente potrà essere abilitato, dalla Società, alla navigazione Internet. Col presente disciplinare interno si richiamano gli utenti ad una particolare attenzione nell'utilizzo di Internet e dei servizi relativi, in quanto ogni operazione posta in essere è associata all'"Indirizzo Internet Pubblico" assegnato alla Società stessa.

Internet è uno strumento messo a disposizione degli utenti per uso professionale. Ciascun lavoratore, pertanto, deve quindi usare la rete Internet in maniera appropriata, tenendo presente che ogni sito web può essere governato da leggi diverse da quelle vigenti in Italia; l'Utente deve quindi prendere ogni precauzione a tale riguardo.

Le norme di comportamento da osservare nell'utilizzo delle connessioni ad Internet sono le seguenti:

a. l'utilizzo è consentito per scopi aziendali e, pertanto, non è consentito navigare in siti non attinenti allo svolgimento delle proprie mansioni lavorative;

b. durante l'orario di lavoro non è consentita l'effettuazione di ogni genere di transazione finanziaria, ivi comprese le operazioni di remote banking, acquisti on-line e simili, ad esclusione delle operazioni / casi espressamente autorizzati dalla Società o rientranti nell'attività lavorativa dell'Utente;

c. durante l'orario di lavoro è vietata ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa;

d. non sono permesse, se non per motivi professionali, la partecipazione a forum, l'utilizzo di chat-line o di bacheche elettroniche e le registrazioni in *guest-book*, anche utilizzando pseudonimi (o nicknames);

e. è severamente vietata la navigazione in siti e la memorizzazione di documenti informatici di natura oltraggiosa, pornografica, pedopornografica e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;

f. è consentito l'utilizzo di soluzioni di Instant Messenger e/o chat esclusivamente per scopi professionali ed attraverso gli strumenti ed i software messi a disposizione dalla Società;

g. è consentito l'utilizzo di sistemi di social networking (es. LinkedIn, YouTube) sul luogo di lavoro o durante l'orario lavorativo purché siano strettamente pertinenti con l'attività professionale del singolo Utente;

h. non è consentito lo scambio e/o la condivisione (es. i c.d. sistemi di Peer-to-Peer) a qualsiasi titolo, anche se non a scopo di lucro, di materiale audiovisivo, cinematografico, fotografico, informatico, etc., protetto da copyright;

i. non è consentito sfruttare i marchi registrati, i segni distintivi e ogni altro bene immateriale di proprietà della Società in una qualsiasi pagina web o pubblicandoli su Internet, a meno che tale azione non sia stata approvata espressamente.

È altresì proibito qualsiasi uso del Web che possa essere nocivo all'immagine della Società.

Per facilitare il rispetto delle predette regole, la Società si riserva, per mezzo dell'amministratore di sistema, la facoltà di configurare specifici filtri che inibiscano l'accesso ai contenuti ivi non consentiti (con esclusione dei siti istituzionali) e che prevengano operazioni non correlate all'attività lavorativa (es. upload, restrizione nella navigazione, download di *file* o software).

L'Utente che ritenga necessario navigare su siti che risultano inibiti potrà avanzare specifica richiesta scritta alla Direzione IT, indicando i contenuti che ha necessità di navigare ed altresì le specifiche ragioni.
L'eventuale conservazione di dati è effettuata per il tempo strettamente limitato al perseguimento di finalità organizzative, produttive e di sicurezza. I sistemi software sono programmati e configurati in modo da cancellare periodicamente ed automaticamente (attraverso procedure di sovra registrazione come, ad esempio, la cd. rotazione dei log file) i dati personali relativi agli accessi ad Internet e al traffico telematico, la cui conservazione non sia necessaria.

17. GESTIONE E UTILIZZO DELLA POSTA ELETTRONICA AZIENDALE

Principi guida

Ad ogni Utente titolare di un account, la Società provvede ad assegnare una casella di posta elettronica individuale.

I servizi di posta elettronica devono essere utilizzati a scopo professionale: si ricorda a tutti gli utenti che l'account e-mail è uno strumento di proprietà della Società ed è conferito in uso per l'esclusivo svolgimento delle mansioni lavorative affidate.

Ad uno stesso Utente possono essere assegnate più caselle di posta elettronica che possono essere condivise con altri utenti dello stesso gruppo/dipartimento. Tali caselle devono essere utilizzate per la ricezione dei messaggi, mentre per le risposte o gli invii, è consigliabile utilizzare la casella di posta individuale assegnata.

La Società valuterà caso per caso e previa richiesta dell'Utente, la possibilità di attribuire allo stesso un diverso indirizzo destinato ad uso privato.

Attraverso l'e-mail aziendale, gli utenti rappresentano pubblicamente la Società e per questo motivo viene richiesto di utilizzare tale sistema in modo lecito, professionale e comunque tale da riflettere l'immagine aziendale.

Gli utenti sono responsabili del corretto utilizzo delle caselle di posta elettronica aziendale e sono tenuti ad utilizzarla in modo conforme alle presenti regole. Gli stessi, pertanto, devono:

- conservare la password nella massima riservatezza e con la massima diligenza;
- mantenere la casella in ordine, cancellando documenti inutili e allegati ingombranti;

- memorizzare gli allegati dei messaggi di posta negli appositi spazi messi a disposizione dalla Società, al fine di permettere la storicizzazione delle informazioni funzionali alle attività aziendali;
- prestare attenzione alla dimensione degli allegati per la trasmissione di file all'interno della struttura nonché alla posta ricevuta. Gli allegati provenienti da mittenti sconosciuti non devono essere aperti in quanto possono essere utilizzati come veicolo per introdurre programmi dannosi (es. virus);
- accertarsi dell'identità del mittente e controllare a mezzo di software antivirus i file attachment di posta elettronica prima del loro utilizzo;
- rispondere ad e-mail pervenute solo da emittenti conosciuti e cancellare preventivamente le altre;
- collegarsi a siti internet contenuti all'interno di messaggi solo quando vi sia comprovata sicurezza sul contenuto degli stessi.

Si ricorda che il sistema di posta aziendale non deve essere deputato alla trasmissione o alla condivisione di allegati di grandi dimensioni (ad esempio superiori a 25 MG). Rispetto a questi, tali attività devono essere svolte attraverso gli strumenti messi a disposizione dalla Società (es. Google Drive).

L'utente che riceve una e-mail a carattere, violento, razzista o pornografico, o che rappresenti forme di spamming o phishing ha il dovere di avvertire rapidamente la Società affinché siano prese le misure necessarie per fermare il ricevimento di questi messaggi non sollecitati. È in generale vietato trasmettere e-mail di tipo professionale al proprio indirizzo privato, fatta salva l'autorizzazione ricevuta dalla proprietà o dal proprio diretto superiore.

Non è consentito agli utenti di:

- diffondere intenzionalmente e senza autorizzazione il proprio indirizzo e-mail aziendale attraverso la rete internet;

- utilizzare la casella di posta elettronica aziendale per inviare, ricevere o scaricare allegati contenenti video, brani musicali, etc., salvo che questo non sia funzionale all'attività prestata in favore della Società (es: presentazioni o materiali video aziendali, formazione specifica).

Si ricorda che, salvo l'utilizzo di appositi strumenti di cifratura, i sistemi di posta elettronica non possono garantire la riservatezza delle informazioni trasmesse. Pertanto, si richiede agli utenti di valutare con attenzione l'invio di informazioni classificabili quali *"riservate"* o aventi comunque carattere *"strettamente confidenziale"*.

Occorre inoltre che i messaggi di posta elettronica contengano un avvertimento ai destinatari, nel quale sia dichiarata l'eventuale natura non personale dei messaggi stessi e precisato che le risposte potranno essere conosciute nell'organizzazione di appartenenza del mittente.

NB: Nei casi in cui la Società si doti di posta elettronica certificata si applicheranno, ove compatibili, le presenti disposizioni.

Accesso alla casella di posta elettronica del lavoratore assente

Saranno messe a disposizione di ciascun Utente, con modalità di agevole esecuzione, apposite funzionalità del sistema di posta elettronica che consentano di inviare automaticamente, in caso di assenze programmate, messaggi di risposta che contengano le coordinate di altro soggetto cui trasmettere le comunicazioni e-mail di contenuto lavorativo o altre utili modalità di contatto in caso di assenza del lavoratore.

In caso di eventuali assenze non programmate (ad es., per malattia), qualora il lavoratore non possa attivare la procedura descritta (anche avvalendosi di servizi *webmail*), la Società, perdurando l'assenza oltre un determinato limite temporale pari a 60 giorni, disporrà lecitamente, sempre che sia necessario e mediante personale appositamente incaricato (ad es., l'amministratore di sistema oppure, se presente, un incaricato aziendale per la protezione dei dati RSPD), l'attivazione di un analogo accorgimento (risposta automatica o re-indirizzamento), avvertendo l'assente.

Nel caso, invece, la Società necessiti conoscere il contenuto dei messaggi di posta elettronica dell'Utente resosi assente per cause improvvise o per improrogabili necessità legate all'attività lavorativa, si procederà come segue:

- la verifica del contenuto dei messaggi sarà effettuata per il tramite di idoneo "fiduciario", da intendersi quale lavoratore previamente nominato e/o incaricato (per iscritto) dall'Utente assente;
- di tale attività sarà redatto apposito verbale e informato l'Utente interessato alla prima occasione utile.
- sarà preventivamente richiesto all'utente di farlo lui stesso, se possibile, tramite web mail.

Cessazione dell'indirizzo di posta elettronica aziendale

In caso di cessazione del rapporto di lavoro con l'Utente, le credenziali dell'Utente verranno disabilitate entro 48 ore dalla suddetta cessazione previa comunicazione da parte dell'ufficio del personale. Per un periodo di 90 (novanta) giorni i messaggi di posta inviati all'indirizzo dismesso potranno essere automaticamente inoltrati al responsabile gerarchico, dando atto di tale re-inoltro al mittente. Oltre a questo termine di 90 giorni non sarà più attivo.

In caso di cessazione del rapporto di lavoro, le email del dipendente dimissionario verranno conservate per un periodo di 90 (novanta) giorni dopodiché verranno definitivamente eliminate.

La Società si riserva tuttavia il diritto di conservare quei messaggi di posta elettronica che possono risultare significativi per la risoluzione di controversie e nei casi previsti dalla legge.

Tale registrazione è conservata in osservanza delle norme civilistiche e fiscali ex art. 2220 cod. civ. e dell'art. 22 del D.P.R. n. 600 del 29/9/73 e comunque fino al termine di eventuali accertamenti fiscali o di accertamenti comunque disposti dall'autorità giudiziaria.

18. I CONTROLLI

I principi

La Società, in linea con quanto prescritto dall'ordinamento giuridico italiano (art. 4, Statuto dei Lavoratori), esclude la configurabilità di forme di controllo aziendali aventi direttamente ad oggetto l'attività lavorativa dell'Utente.
Ciononostante, non si esclude che, per ragioni organizzative e produttive, di tutela del patrimonio aziendale ovvero per esigenze dettate dalla sicurezza del lavoro, si utilizzino sistemi informatici, impianti, apparecchiature o dispositivi dai quali derivi la possibilità di controllo a distanza dell'attività dei lavoratori. In tal caso tali strumenti verranno valutati e subordinati rispetto alla normativa di settore, ed i dati acquisiti con lo strumento verranno trattati secondo l'informativa privacy allegata al presente disciplinare.

Fermo restando il diritto della Società di effettuare controlli sull'effettivo adempimento della prestazione lavorativa nonché sul corretto utilizzo dei beni e servizi informatici aziendali (artt. 2086, 2087 e 2104 c.c.), i controlli posti in essere, saranno sempre tali da evitare ingiustificate interferenze con i diritti e le libertà fondamentali dei lavoratori e non saranno costanti, prolungati e indiscriminati, nel rispetto del principio di pertinenza e non eccedenza.

La Società, nel riservarsi il diritto di procedere a tali controlli, informa che le modalità di effettuazione degli stessi sono ispirate al principio della "gradualità" così come di seguito più precisamente specificato.

Modalità di effettuazione dei controlli

I controlli consentono alla Società di intervenire con verifiche qualora si riscontrino anomalie d'area o di unità, senza arrivare al dettaglio del soggetto singolo, almeno in una prima fase.

Secondo il principio della gradualità:
- I controlli saranno effettuati inizialmente solo su dati aggregati riferiti all'intera struttura aziendale ovvero a singole aree lavorative, aventi caratteristiche tali da precludere l'immediata identificazione dell'utente.
- Nel caso in cui si dovessero riscontrare violazioni del presente disciplinare interno, indizi di commissione di gravi abusi o illeciti o attività contrarie ai doveri di fedeltà e diligenza, verrà diffuso un avviso generalizzato,

o circoscritto all'area o struttura lavorativa interessata, relativo all'uso anomalo degli strumenti informatici aziendali, con conseguente invito ad attenersi scrupolosamente alle istruzioni ivi impartite.
- In caso siano rilevate ulteriori violazioni, si potrà procedere con verifiche più specifiche e puntuali, anche su base individuale.

I controlli non autorizzati
In ogni caso la Società non può in alcun caso utilizzare sistemi da cui derivino forme di controllo a distanza dell'attività lavorativa che permettano di ricostruire l'attività del lavoratore.

Per tali s'intendono, a titolo meramente esemplificativo e non esaustivo:
- la lettura e la registrazione sistematica dei messaggi di posta elettronica, al di là di quanto necessario per fornire e gestire il servizio di posta elettronica stesso;
- la riproduzione e la memorizzazione sistematica delle pagine internet visualizzate da ciascun Utente, dei contenuti ivi presenti, e del tempo di permanenza sulle stesse;
- la lettura e la registrazione dei caratteri inseriti dal lavoratore tramite tastiera o dispositivi analoghi;
- l'analisi occulta di computer portatili affidati in uso.

19. SANZIONI

L'eventuale violazione di quanto previsto dal presente disciplinare interno – rilevante anche ai sensi degli art. 2104 e 2105 c.c. – potrà comportare l'applicazione di sanzioni disciplinari in base a quanto previsto dall'art. 7 dello Statuto dei Lavoratori.

La Società avrà cura di informare senza ritardo (e senza necessità di preventive contestazioni e/o addebiti formali) le autorità competenti, nel caso venga commesso un reato, o la cui commissione sia ritenuta probabile o solo sospettata, tramite l'utilizzo illecito o non conforme dei beni e degli strumenti informatici aziendali.

Si precisa, infine, che in caso di violazione accertata da parte degli utenti delle regole e degli obblighi esposti in questo disciplinare, la Società si riserva la facoltà di sospendere, bloccare o limitare gli accessi di un account, quando appare ragionevolmente necessario per proteggere l'integrità, la sicurezza e/o la funzionalità dei propri beni e strumenti informatici.

20. INFORMATIVA AGLI UTENTI

Il presente disciplinare interno, nella parte in cui contiene le regole per l'utilizzo dei beni e degli strumenti informatici aziendali, e relativamente ai trattamenti di dati personali svolti dalla Società e finalizzati alla effettuazione di controlli leciti.
Si rimanda all'informativa "DIPENDENTI" completa per conoscere nel dettaglio la tipologia di trattamento posto in essere con riferimento agli strumenti adottati dalla Società nel rispetto delle normative di settore.

21. COMUNICAZIONI

Il presente disciplinare interno sarà distribuito agli utenti tramite e-mail al momento della sua prima redazione. All'interno della intranet aziendale verrà inoltre pubblicata la versione del presente documento con gli eventuali successivi aggiornamenti che dovessero intervenire allo scopo di facilitarne la conoscibilità a tutti gli interessati.

Ad ogni aggiornamento del presente documento, ne sarà data comunque comunicazione sulle bacheche aziendali e potrà esserne disposto l'invio tramite di apposito messaggio e-mail. Tutti gli utenti sono tenuti a conformarsi alla versione più aggiornata del presente disciplinare.

Le autorizzazioni e/o concessioni richieste dal presente disciplinare ovvero poste nella facoltà degli utenti potranno essere comunicate alla Società per mezzo di qualsiasi strumento che ne garantisca la tracciabilità (es: e-mail).

22. APPROVAZIONE DEL DISCIPLINARE

Il presente disciplinare interno è stato approvato dal Legale Rappresentante della Società in data 07/11/2018

Ravenna, lì 04/10/2022

Il Legale Rappresentante

Andrea Tozzi