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

Approvato con Deliberazione del Consiglio di Amministrazione del 21 marzo 2012

Revisione con Deliberazione dell'Amministratore Unico del 11 settembre 2018

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

Data di redazione 11 settembre 2018

***

INDICE

CAPO I – I PRINCIPI

ART. 1
INTRODUZIONE, DEFINIZIONI E FINALITA'

Il presente disciplinare interno ha l'obiettivo 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 al *Regolamento UE 2016/679 e successiva regolamentazione D. Lgs. 101/2018* , alla *Legge n. 300/1970* (c.d. Statuto dei Lavoratori) alla luce delle modifiche intervenute ad opera del D. Lgv. 14 settembre 2015, n. 151 ed ai provvedimenti appositamente emanati dall'Autorità Garante (si veda in particolare *Provv. 1 marzo 2007*- Linee Guida del Garante per posta elettronica e internet).

ART. 2
AMBITO DI APPLICAZIONE

Il presente disciplinare interno si applica ad ogni *Utente* assegnatario di beni e risorse informatiche aziendali ovvero utilizzatore di servizi e risorse informative di pertinenza della Società.

Per *Utente* si intende, pertanto, a titolo esemplificativo e non esaustivo, ogni dipendente, collaboratore (interno o esterno), consulente, fornitore e/o terzo che in modo continuativo e non occasionale operi all'interno della struttura aziendale utilizzandone beni e servizi informatici.

Per *Società* si intende, invece, 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.

ART. 3
TITOLARITA' 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 l'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 dallo stesso considerato come avente natura aziendale e non riservata.

ART. 4
RESPONSABILITA' 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 vietati comportamenti che possano creare un danno, anche di immagine, alla Società.

ART. 5
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 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;

CAPO II – MISURE ORGANIZZATIVE

ART. 6 AMMINISTRATORI DEL SISTEMA

L'a Società conferisce all'amministratore di sistema il compito di sovrintendere i beni e le risorse informatiche aziendali. E' compito dell'amministratore di sistema:

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 dal *Regolamento UE 2016/679 e successiva regolamentazione D. Lgs. 101/2018*;
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, irrintracciabilità 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.

La società nomina l'Amministratore di sistema in una persona o società esterna

ART. 7
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.

- Gli account utenti vengono creati dagli amministratori di sistema e sono personali, ovvero associati univocamente alla persona assegnataria;
- 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 (Es: busta chiusa e sigillata);
- le credenziali di autenticazioni costituiscono dati aziendali da mantenere strettamente riservati e non è consentito comunicarne gli estremi a terzi (seppur soggetti in posizione apicale all'interno della Società).
- 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 protezione dati 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 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, lo stesso 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 (cfr. art. 6 n. 7).
- Si ricorda, infine, che i beni e la strumentazione informatica oggetto del presente disciplinare interno rimane di esclusivo dominio della Società, il quale, in virtù dei rapporti instaurati con gli utenti, ne disciplina l'affidamento.

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

- utilizzare almeno 8 caratteri alfanumerici, inclusi i caratteri speciali (#, %, etc.), di cui almeno uno numerico;
- la password deve contenere almeno un carattere maiuscolo, un carattere minuscolo, un numero o un carattere non alfanumerico tipo "@#§£$%...";
- evitare di includere parti del nome, cognome e/o comunque elementi a lui agevolmente riconducibili;
- evitare l'utilizzo di password comuni e/o prevedibili;

- 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 non è conforme alla normativa e costituisce violazione del presente disciplinare interno.

Cessazione degli Account

In caso di interruzione del rapporto di lavoro con l'Utente, le credenziali di autenticazione di cui sopra verranno disabilitate entro un periodo massimo di 30 giorni da quella data; entro 6 mesi, invece, si disporrà la definitiva e totale cancellazione dell'account Utente

ART. 8
POSTAZIONI DI LAVORO

Per postazione di lavoro si intende il complesso unitario di Personal Computer (di seguito, PC), notebook, accessori, periferiche e ogni altro *devices* 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:

- Ogni PC, notebook (accessori e periferiche incluse), e altro devices, sia esso acquistato, noleggiato, o affidato in locazione, rimane di esclusiva proprietà della Società, ed è concesso all'Utente per lo svolgimento delle proprie mansioni lavorative e comunque per finalità strettamente attinenti l'attività svolta;
- E' dovere di ogni Utente usare i computer e gli altri dispositivi a lui affidati responsabilmente e professionalmente;
- Il PC e gli altri dispositivi di cui sopra devono essere utilizzati con hardware e software autorizzati dalla Società. Per utilizzare software o applicativi non presenti nella dotazione standard fornita, si necessita di espressa richiesta scritta dell'utente indirizzata al proprio Responsabile privacy di riferimento, il quale ne valuterà i requisiti tecnici e l'aderenza alle policy interne ed al ruolo ricoperto in azienda;
- Le postazioni di lavoro non devono essere lasciate incustodite con le sessioni utenti attive;
- Quando un Utente si allontana dalla propria postazione di lavoro, deve bloccare tastiera e schermo con un programma salvaschermo (screensaver) protetto da password o effettuare il log-out dalla sessione;
- L'Utente deve segnalare con la massima tempestività all'amministratore del sistema ovvero al proprio Responsabile di riferimento eventuali guasti tecnici, problematiche tecniche o il cattivo funzionamento delle apparecchiature;
- E' fatto divieto di cedere in uso, anche temporaneo, le attrezzature e i beni informatici aziendali a soggetti terzi;
- La Società si riserva la facoltà di rimuovere qualsiasi elemento hardware la cui installazione non sia stata 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. non potranno essere collegati ai computer o alle reti informatiche aziendali, salvo preventiva autorizzazione scritta della Società.

CAPO III – CRITERI DI UTILIZZO DEGLI STRUMENTI INFORMATICI

ART. 9
PERSONAL COMPUTER E COMPUTER PORTATILI

Gli utenti utilizzano per l'espletamento delle proprie mansioni dispositivi di proprietà della Società; ne consegue che gli stessi sono tenuti al rispetto delle seguenti regole:

- Non è consentito modificare la configurazione hardware e software del proprio PC, se non previa esplicita autorizzazione della Società che la esegue per mezzo dell'amministratore del sistema;
- Non è consentito rimuovere, danneggiare o asportare componenti hardware;
- Non è consentito installare autonomamente programmi informatici, software ed ogni altro applicativo non autorizzato espressamente dalla Società;
- E' onere dell'Utente, in relazione alle sue competenze, eseguire richieste di aggiornamento sulla propria postazione di lavoro derivanti da software antivirus nonché sospendere ogni attività in caso di minacce *virus* o altri malfunzionamenti, segnalando prontamente l'accaduto all'amministratore del sistema;
- E' onere dell'Utente spegnere il proprio PC o computer portatile al termine del lavoro.

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

Non è consentito all'Utente caricare o inserire all'interno del portatile 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 utenti di cancellare tutti i dati eventualmente presenti prima di consegnare il portatile agli uffici competenti per la restituzione o la riparazione.

ART. 10
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 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 concessigli. 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.

ART. 11
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.

ART. 12
DISPOSITIVI DI MEMORIA PORTATILI

Per dispositivi di memoria portatili si intendono tutti quei dispositivi che consentono di copiare o archiviare dati, files, o documenti esternamente al computer. Sono considerati tali CD-ROM, DVD, penne o chiavi di memoria USB, riproduttori musicali MP3, fotocamere digitali, dischi rigidi esterni, etc.

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

- non è consentito utilizzare supporti rimovibili personali, se non preventivamente autorizzati per iscritto dalla Società; è onere dell'Utente custodire i supporti magnetici contenenti dati sensibili e giudiziari in armadi chiusi a chiave, onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto.
- Si precisa che, ove autorizzati in base a quanto sopra disposto, una volta connessi all'infrastruttura informatica della Società, i dispositivi saranno soggetti (ove compatibili) al presente disciplinare interno.

ART. 13
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.
E' 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.

ART. 14
STRUMENTI DI FONIA MOBILE E/O DI CONNETTIVITA' IN MOBILITA'

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 esclusivamente lavorativi. E' 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 .
A tal fine si informano gli utilizzatori dei servizi di fonia aziendale, che la Società eserciterà i diritti di cui all'art. 124 D.Lgs. 101/2018 (cd. *fatturazione dettagliata*), 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. 5 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.

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 password di sicurezza (cd. codice pin del dispositivo) che ne impedisca l'utilizzo da parte di soggetti non autorizzati. A tal fine si precisa che:
  - il CODICE PIN dovrà essere composto di n. 5 cifre numeriche;
  - 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 dandone comunque comunicazione alla Società.
- In caso di furto, danneggiamento o smarrimento del dispositivo mobile in oggetto, l'Utente assegnatario dovrà darne immediato 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 consentito all'Utente effettuare riprese, fotografie, registrazioni di suoni con qualsiasi tipologia di apparecchiatura elettronica adatta a tali scopi.
- 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.

CAPO IV – GESTIONE DELLE COMUNICAZIONI TELEMATICHE

ART. 15
GESTIONE UTILIZZO DELLA RETE INTRANET AZIENDALE

1. La rete interna, istituita appositamente per permettere collegamenti funzionali tra Utenti che prestano servizio all'interno della struttura lavorativa, non può esser utilizzata per scopi diversi da quelli lavorativi.
2. Qualora nella rete interna debbano circolare dati, notizie ed informazioni aziendali, deve essere premura di ciascun Utente preservare gli stessi dalla conoscibilità di terzi soggetti non espressamente autorizzati ad aver notizia di tali dati.

ART. 16
GESTIONE UTILIZZO DELLA RETE INTERNET

Ogni Utente potrà essere abilitato, dalla Società, alla navigazione Internet tramite la rete aziendale. Col presente disciplinare interno si richiama 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.
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 esclusivamente per scopi aziendali e, pertanto, non è consentito navigare in siti non attinenti allo svolgimento delle proprie mansioni lavorative.
b. Non è consentita l'effettuazione di ogni genere di transazione finanziaria, ivi comprese le operazioni di remote banking, acquisti on-line e simili, salvo casi espressamente autorizzati dalla Sociegtà.
c. 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. Non è consentita 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. E' consentito l'utilizzo di soluzioni di Instant Messanger e/o chat esclusivamente per scopi professionali ed attraverso gli strumenti ed i software messi a disposizione dalla Società.
g. Non è consentito l'utilizzo di sistemi di social networking sul luogo di lavoro o durante l'orario lavorativo.
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 rigorosamente qualsiasi uso del Web e dei social networks che non trasmetta un'immagine positiva o che possa in qualunque modo risultare nocivo all'immagine della Società.

La registrazione di informazioni relative al traffico Internet, in ogni caso, avverrà in forma anonima o tale da precludere l'immediata identificazione di utenti mediante loro opportune aggregazioni (ad es., con riguardo ai *file* di *log* riferiti al traffico *web*).

In caso di abusi singoli o reiterati – *cfr*. sul punto l' art. 5 del Disciplinare interno – verranno inoltrati preventivi avvisi collettivi di richiamo al rispetto delle regole. Qualora, nonostante i rischiami generalizzati, perduri un indebito utilizzo della rete internet la Società procederà all'invio di avvisi più circoscritti, e – solo se a seguito della gradualità dei controlli emergano fondati sospetti – verranno allora effettuati controlli nominativi o su singoli dispositivi e postazioni.

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

L'eventuale conservazione di dati è effettuata per il tempo strettamente limitato al perseguimento di finalità organizzative, produttive e di sicurezza. Ogni utente settimanalmente provvede a cancellare i dati relativi agli accessi ad Internet e al traffico telematico, la cui conservazione non sia necessaria.

ART. 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 esclusivamente per la ricezione dei messaggi, mentre per le risposte o gli invii, si deve sempre utilizzare la casella di posta 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;
- utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario;
- 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).
- inviare preferibilmente *files* in formato PDF;
- accertarsi dell'identità del mittente e controllare a mezzo di software antivirus i files 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.

Non è consentito agli utenti, al contrario:

- diffondere 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).

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.

Alla posta elettronica certificata della Società si applicano, 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 2 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), 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.

Cessazione dell'indirizzo di posta elettronica aziendale

In caso di interruzione del rapporto di lavoro con l'Utente, l'indirizzo di posta elettronica verrà disabilitato entro un periodo massimo di 30 giorni da quella data; entro 3 mesi, invece, si disporrà la definitiva e totale cancellazione dello stesso. In ogni caso, la Società si riserva il diritto di conservare i messaggi di posta elettronica che riterrà rilevanti.

ART. 18
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.

ART. 19
INFORMATIVA AGLI UTENTI EX ART. 13 REGOLAMENTO UE 2016/679 e SUCCESSIVA REGOLAMENTAZIONE D. LGS. 101/2018

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, così come definiti nell'art. 5, vale quale informativa ex. art. 13 del Regolamento UE 2016/679 e successiva regolamentazione D. Lgs. 101/2018, così come disposta dal punto 3.3 delle Linee Guida del Garante Privacy del 1 marzo 2007.

ART. 20
COMUNICAZIONI

Il presente disciplinare interno è messo a disposizione degli utenti, per la consultazione, al momento dell'assegnazione di un account Utente. Sulla intranet aziendale, ovvero presso la bacheca aziendale è pubblicata la versione più aggiornata dello stesso allo scopo di facilitarne la conoscibilità a tutti gli interessati.
Ad ogni aggiornamento del presente documento, ne sarà data comunicazione sulle bacheche aziendali e tramite l'invio 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).

ART. 21
APPROVAZIONE DEL DISCIPLINARE

Il presente disciplinare interno congiuntamente all'Allegato A, sono stati approvati dall' Amministratore unico della Società in data 11 settembre 2018

Prato, lì 11 settembre 2018.

La Società, in persona del legale rappresentante _____.