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

**INDICE**



## Capo I – I Principi

### Art.1

### Introduzione, definizioni e finalità

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, ecc.), al fine di tutelare i beni materiali e immateriali aziendali ed evitare condotte inconsapevoli e/o scorrette che potrebbero esporre l'Ente a

problematiche di sicurezza, di immagine e patrimoniali per eventuali danni cagionati anche a terzi.
L'insieme delle norme comportamentali ivi presenti, pertanto, è volto a conformare l'Ente a 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 n. 2016/679, alla Legge n. 300/1970 (c.d. Statuto dei Lavoratori) ed ai provvedimenti appositamente emanati dall'Autorità Garante (si veda in particolare Provv. 1° marzo 2007).

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

**Art. 3**

**Titolarità dei beni e delle risorse informatiche**

I beni e le risorse informatiche, i servizi ITC e le reti informative costituiscono beni aziendali rientranti nel patrimonio sociale e sono da considerarsi di esclusiva proprietà dell'Ente.
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 l'Ente), 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 riservata.

**Art.4**

**Responsabilità personale dell'Utente**

Ogni utente è personalmente responsabile dell'utilizzo dei beni e delle risorse informatiche affidatigli dall'Ente, nonché dei relativi dati trattati per finalità aziendali.
A tal fine ogni Utente, nel rispetto dei principi di diligenza sottesi al rapporto instaurato con l'Ente, 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 relazione 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, all'Ente.

**Art. 5**

**I controlli**

**I principi**

L'ente, in linea con quanto prescritto dall'ordinamento giuridico italiano (art. 4 Statuto del Lavoratori), esclude la configurabilità di forme di controllo aziendali aventi direttamente ad oggetto l'attività lavorativa dell'Utente.
Ciò nonostante, non si esclude che, per ragioni organizzative e produttive, ovvero per esigenze dettate dalla sicurezza del lavoro, si utilizzino sistemi informatici, impianti o apparecchiature dai quali derivi la possibilità di controllo a distanza dell'attività dei lavoratori. In tali casi, infatti, sarà onere dell'Ente sottoporre tali forme di controllo all'accordo con le rappresentanze sindacali aziendali, ovvero, in assenza di queste, con la commissione interna. In difetto di accordo, su istanza dell'Ente, provvede l'Ispettorato del lavoro, dettando, ove occorra, le modalità per l'uso di tali impianti.
I controlli posti in essere, pertanto, saranno sempre tali da evitare ingiustificate interferenze con i diritti e le libertà fondamentali dei lavoratori e non saranno costanti, prolungati e indiscriminati.
L'Ente, nel riservarsi il diritto di procedere a tali controlli sull'effettivo adempimento della prestazione lavorativa, nonché sull'utilizzo da parte degli utenti dei beni e dei servizi informatici aziendali (artt. 2086, 2087 e 2104 c.c.), agirà in base al principio della "gradualità".
Secondo questo principio:

- I controlli saranno effettuati inizialmente solo su dati aggregati riferiti all'intera struttura aziendale, ovvero a singole aree lavorative.
- 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 l'Ente non può utilizzare sistemi da cui derivino forme di controllo a distanza dell'attività lavorativa che permettano di ricostruire l'attività del lavoratore.
Per tali si 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 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 dei dispositivi per l'accesso alla rete internet.

## Capo II – Misure Organizzative

### Art. 6

### Amministratori del sistema

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

1. gestire l'hardware e il software di tutta la strumentazione informatica di appartenenza dell'Ente;
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 assegnati agli utenti, purché rientranti nelle normali attività di manutenzione, gestione della sicurezza della protezione dei dati;
6. provvedere alla sicurezza informatica dei sistemi informativi aziendali, nel rispetto di quanto prescritto dal d.lgs. 196/2003 (artt. 31 e 33);
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.

Di seguito si riporta il nominativo dell'amministratore di sistema dell'Ente:

- interno: ……..
- esterno: ……..

### 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 prestazione lavorativa.

- Gli account utenti vengono creati dagli amministratori di sistema e sono personali, ovvero associati univocamente alla persona assegnataria.
- L'accesso all'account avviene tramite l'utilizzo delle "credenziali di autenticazione" (es. "Username" e "Password"), comunicate dall'Utente all'amministratore di sistema oppure dal referente privacy, che le genera,

attraverso modalità che ne garantiscono la segretezza (es. busta chiusa e sigillata).

- Le credenziali di autenticazione costituiscono dati aziendali da mantenere strettamente riservati e non è consentito comunicarne gli estremi a terzi (seppure soggetti in posizione apicale all'interno dell'Ente).
- 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 queste 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.
- 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.
- Si ricorda, infine, che i beni e la strumentazione informatica oggetto del presente disciplinare interno rimane esclusivo dominio dell'Ente, 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 o dal Referente Privacy, 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 (#, %, ecc.), 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 delle 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.

**Cessione degli Account**

In caso di interruzione del rapporto di lavoro con l'Utente, le credenziali di autenticazione (password) di cui sopra verranno modificate entro un periodo massimo di 30 giorni da quella data.

**Art. 8**

**Postazione di lavoro**

Per postazione di lavoro si intende il complesso unitario di Personal Computer (di seguito PC), notebook, accessori, periferiche e ogni altro device concesso dall'Ente 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, l'Ente ha adottato le regole tecniche, che di seguito si riportano:

- ogni Pc, notebook (accessori e periferiche incluse), e altro device, sia esso acquistato, noleggiato, o affidato in locazione, rimane di esclusiva proprietà dell'Ente ed è concesso all'Utente per lo svolgimento delle proprie mansioni lavorative e comunque per finalità strettamente attinenti l'attività svolta.
- È dovere di ogni Utente usare i Pc 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 dall'Ente. 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 struttura.
- 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 della 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.
- È fatto divieto di cedere in uso, anche temporaneo, le attrezzature e i beni informatici aziendali a soggetti terzi.
- L'Ente 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 degli Utenti 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 dell'Ente.

## Capo III – Criteri di utilizzo degli strumenti informatici

### Art. 9
### Personale computer e computer portatili

Gli Utenti utilizzano per l'espletamento delle proprie mansioni dispositivi di proprietà dell'Ente; 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 dell'Ente che la esegue per mezzo dell'amministratore di 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 dall'Ente;

- è onere dell'Utente, in relazione alle sue competenze, eseguire richieste di aggiornamento sulla propria postazione di lavoro derivanti da software antivirus o altri malfunzionamenti, segnalando prontamente l'accaduto all'amministratore del sistema;
- è onere dell'Utente spegnere il proprio Pc o computer portatile al termine del lavoro.

Per quanto concerne, invece, la gestione eventuale dei computer portatili, l'Utente ha l'obbligo di custodirli con diligenza e in un 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 dei 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 dall'Ente per installare o comunque utilizzare qualsiasi programma o software dotato di licenza non proprietaria ("freeware" o "shareware").
L'Ente 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:

- l'Ente 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 download né l'upload tramite internet di software non autorizzato.
- L'Ente, sulla scorta di quanto disposto dalle normative a tutela della proprietà intellettuale e del diritto di autore, ricorda che le persone coinvolte nella riproduzione illegale del software sono responsabili sia civilmente che penalmente.
- L'Ente 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 dall'Ente 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 l'Ente 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, ecc.
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 dall'Ente;
- è onere dell'Utente custodire i supporti magnetici contenenti dati 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 dell'Ente, i dispositivi saranno soggetti (ove compatibili) al presente disciplinare interno.

**Art. 13**

**Stampanti e fotocopiatrici**

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 dell'Ente.
È richiesta una particolare attenzione quando si inviano su una stampante condivisa documenti aventi ad oggetti 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.

**Art. 14**

**Strumenti di fonia mobile e/o di connettività in mobilità**

L'Ente potrebbe mettere 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 telefonia tramite rete cellulare.
Specifiche relative ai limiti entro cui l'Utente potrà utilizzare tali strumenti saranno riportate nella scheda tecnica consegnata all'Utente, unitamente ai dispositivi di cui sopra.
L'utente dovrà attenersi ai suddetti limiti, potendo in caso contrario l'Ente 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. 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 (la società).

A tal fine, si informano gli utilizzatori dei servizi di fonia aziendale che l’Ente eserciterà i diritti di cui all'art. 124 d.lgs. 196/2003 (c.d. Fatturazione dettagliata), richiedendo ai provider di telefonia i dettagli necessari ad effettuare controlli sull'utilizzo ed i relativi costi di traffico effettuato nel tempo.

## Capo IV – Gestione delle Comunicazioni Telematiche

### Art. 15

### Gestione utilizzo della rete internet

Ogni Utente potrà essere abilitato dall’Ente alla navigazione Internet. Con il 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 all'Ente stesso.

Internet è uno strumento messo a disposizione degli utenti per uso professionale. Ciascun lavoratore, pertanto, deve 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:

- l'utilizzo è consentito esclusivamente per scopi aziendali e, pertanto, non è consentito navigare in siti non attinenti allo svolgimento delle proprie mansioni lavorative;
- 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 dall’Ente;
- è vietata ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa;
- 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);
- 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;
- è 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 dell’Ente;
- non è consentito l'utilizzo di sistemi di social networking sul luogo di lavoro o durante l'orario lavorativo;
- 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 scopi di lucro, di materiale audiovisivo, cinematografico, fotografico, informatico, ecc., protetto da copyright;
- non è consentito sfruttare i marchi registrati, i segni distintivi e ogni altro bene immateriale di proprietà dell’Ente in una qualsiasi pagina web o pubblicandoli su Internet, a meno che tale azione non sia stata approvata espressamente.

Per facilitare il rispetto delle predette regole, l’Ente si riserva, per mezzo dell'amministratore di sistema, la facoltà di configurare specifici filtri che inibiscano l'accesso ai contenuti ivi non consentiti.

**Art.16**

**Gestione e utilizzo della posta elettronica aziendale**

**Principi guida**

Ad ogni Utente titolare di un account, l'Ente 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 dell'Ente ed è conferito in uso per l'esclusivo svolgimento delle mansioni lavorative affidate.

Ad uno stesso utente potrebbero essere assegnate più caselle di posta elettronica che possono essere condivise con altri utenti. Tali caselle devono essere utilizzate prevalentemente per la ricezione dei messaggi; quando utilizzate per le risposte o gli invii dovranno sempre contenere il fondo al messaggio la firma completa del mittente.

L'Ente 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 l'Ente 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 mittenti 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, ecc., salvo che questo non sia funzionale all'attività prestata in favore dell'Ente (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”.

**Accesso alla casella di posta elettronica del lavoratore assente**

In caso di assenza prolungata di un lavoratore i messaggi di posta potranno essere letti e presi in carico dal Referente privacy/responsabile interno.

**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.

## Art.17

## Gestione salvataggio dei dati e backup

Per i dati ed i documenti che risiedono sui server gestiti centralmente, il servizio informatico esegue i salvataggi con frequenza …….attraverso la seguente procedura ……..

Per i dati ed i documenti che risiedono esclusivamente sul pc di ciascun Utente, il salvataggio/backup dei dati avviene ad opera di ……..con frequenza ……..

Questo allo scopo di garantire la disponibilità ed il ripristino dei dati nel caso di una generica compromissione delle risorse (cancellazione accidentale, guasti, furti, ecc. ecc.).

A tal fine si raccomanda, ancora una volta, ciascun Utente a non salvare sugli strumenti informatici aziendali file/cartelle personali.

## Art. 18

## Sanzioni

L'eventuale violazione di quanto previsto dal presente disciplinare interno, rilevante anche ai sensi dell'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.

L’Ente 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, l’Ente 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 n. 2016/679**

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 dall'Ente e finalizzati alla effettuazione di controlli leciti, così come definiti nell'art. 5, vale quale informativa ex art. 13 del Regolamento UE n.2016/679.

Si precisa che una sintesi delle predette regole è stata inserita anche nelle lettere di designazione consegnate a ciascun incaricato.

**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.

Ad ogni aggiornamento del presente documento, ne sarà data comunicazione sulla bacheca aziendale 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 richiesti 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).

Luogo e data _____ L'Ente _____