ISTITUTO COMPRENSIVO STATALE

AD INDIRIZZO MUSICALE

"MATTEO RIPA"

Piazza Matteo Ripa, 1 – 84025 – **EBOLI** (SA)

Tel./Fax 0828 328155 – E-mail: saic88900p@istruzione.it – web: www.icmatteoripa.gov.it

DISTRETTO 57 – C.M. SAIC88900P- Autonomia 135 –cod. Aut. SA 3K5 – C. F. 91027510659 – Codice univoco fatt. **UFOSY7**

REGOLAMENTO PER L'UTILIZZO DEGLI STRUMENTI INFORMATICI

REV. 1.1- 10/10/2024

Titolare del trattamento dei dati	Dirigente scolastico Daniela Natalino
Indirizzo	Piazza Matteo Ripa 1
Telefono	0828 328155
E-Mail	saic88900p@istruzione.it
PEC	saic88900p@pec.it

Dati del Responsabile della Protezione dei Dati.

Nome e Cognome	Sandro Falivene
Indirizzo	via C. Maiorini,1 84096 Montecorvino Rovella (Sa)
Telefono	333/4207958
E-Mail	sandro_falivene@hotmail.com
PEC	

Sommario

CAPO I – PRINCIPI

Art. 1 – Introduzione, Definizioni e Finalità

Il presente regolamento ha l'obiettivo di definire l'ambito di applicazione, le modalità e le norme sull'utilizzo della strumentazione da parte degli utenti assegnatari (dipendenti, collaboratori ecc.) al fine di tutelare i beni dell'ente ed evitare condotte inconsapevoli 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 da adottare è ispirato ai principi di diligenza, informazione, correttezza nell'ambito dei rapporti di lavoro e inoltre finalizzato a prevenire eventuali comportamenti illeciti dei dipendenti, pur nel rispetto dei diritti a essi attribuiti dall'ordinamento giuridico italiano.

Particolare criticità viene sollevata:

- dal trattamento di dati effettuato con strumenti elettronici tramite l'utilizzo di internet e posta elettronica;
- dal trattamento dei dati personali dei lavoratori nel contesto della gestione del rapporto di lavoro.

Premesso che

In materia di uso degli strumenti elettronici, posta elettronica e internet:

- compete al Titolare del Trattamento assicurare la funzionalità ed il corretto impiego di posta elettronica e internet da parte dei lavoratori, definendone le modalità d'uso nell'organizzazione dell'attività lavorativa, tenendo conto della disciplina in tema di diritto del lavoro;
- spetta al Titolare del Trattamento adottare adeguate misure di sicurezza per assicurare la disponibilità e l'integrità di sistemi informativi e di dati, anche per prevenire utilizzi indebiti che possono essere fonte di responsabilità;
- emerge l'esigenza di tutelare gli utenti interessati, anche in relazione all'utilizzo di posta elettronica e internet ampiamente diffusi nel contesto lavorativo;
- l'utilizzo di internet da parte dei lavoratori può comportare la definizione del profilo dell'utilizzatore a seguito di raccolta di informazioni che lo riguardano da parte di sistemi informatici installati per ragioni di sicurezza;

- le informazioni così trattate contengono dati personali anche particolari riguardanti lavoratori o terzi, identificati o identificabili;
- A tale proposito si rileva che gli eventuali controlli previsti escludono finalità di monitoraggio diretto e intenzionale dell'attività lavorativa e sono disposti sulla base della vigente normativa, con particolare riferimento al Regolamento (UE) 2016/679, alla legge n. 300/1970 (Statuto dei lavoratori) e ai provvedimenti emanati dall'Autorità Garante (in particolare Provvedimento del 1° marzo 2007).

Art. 2 – Ambito di applicazione

Il presente regolamento si applica a ogni utente assegnatario di beni e risorse informatiche di proprietà dell'ente ovvero utilizzatore di servizi e risorse informative di proprietà dell'ente.

Per **utente** pertanto si intende, a titolo esemplificativo e non esaustivo, ogni dipendente, collaboratore, consulente, fornitore o altro che in modo continuativo non occasionale operi all'interno dell'ente utilizzandone beni e servizi informatici.

Per **ente** si intende, invece, la società, l'organizzazione, la scuola, la pubblica amministrazione ed in generale il titolare dei beni e delle risorse informatiche ivi disciplinate, il quale opererà per mezzo dei soggetti che ne possiedono la rappresentanza.

Per **scopo** si intendono gli scopi dettati dalla propria posizione all'interno dell'ente, a titolo esemplificativo e non esaustivo, lo scopo di un commerciale è la vendita; quindi, sono compatibili con il suo scopo l'accesso ai documenti di vendita, ma non i documenti amministrativi e contabili. Lo scopo di un assistente tecnico amministrativo scolastico assegnato alla didattica è l'accesso ai dati, anche sensibili, degli studenti, ma non l'accesso ai dati contabili e di gara dell'ente.

Art. 3 – Titolarità dei beni e delle risorse informatiche

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

Ciò considerato, il loro utilizzo è consentito solo per finalità di adempimento delle mansioni affidate a ciascun utente in base al rapporto in essere, ovvero per gli scopi professionali afferenti l'attività svolta per l'ente, e comunque per l'esclusivo perseguimento degli obiettivi dell'ente.

A tal fine si precisa sin d'ora che qualsivoglia dato o informazione trattato per mezzo dei beni e delle risorse informatiche di proprietà dell'ente sarà dallo stesso considerato come avente natura lavorativa e non 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 dell'ente.
A tal fine ogni utente, nel rispetto dei principi di diligenza sottesi al rapporto instaurato con l'ente e per quanto di propria competenza, è tenuto a tutelare il patrimonio dell'ente da utilizzi impropri o non autorizzati, danni o abusi anche derivanti da

negligenza, imprudenza o imperizia. L'obiettivo è e rimane sempre quello di preservare l'integrità e la riservatezza dei beni, delle informazioni e delle risorse dell'ente.

Ogni utente è tenuto a operare a tutela della sicurezza informatica dell'ente, in relazione al proprio ruolo e alle mansioni in concreto svolte, riportando al proprio responsabile organizzativo diretto e senza ritardo eventuali rischi di cui è a conoscenza ovvero violazioni del presente regolamento. Sono vietati comportamenti che possano creare un qualsiasi danno, anche di immagine, all'ente.

Art. 5 – Controlli

L'ente esclude la configurabilità di forme di controllo aziendali aventi direttamente a oggetto l'attività lavorativa dell'utente, in linea con quanto prescritto dall'ordinamento giuridico italiano (art. 4, Statuto dei lavoratori).

Ciò nonostante, non si esclude che si possano utilizzare sistemi informatici, impianti o apparecchiature dai quali derivi la possibilità di controllo a distanza dell'attività dei lavoratori per ragioni organizzative e produttive ovvero per esigenze dettate dalla sicurezza del lavoro. Per tali evenienze, eventualmente, sarà onere dell'ente sottoporre tali forme di controllo all'accordo con le rappresentanze sindacali. In difetto di accordo e su istanza dell'ente sarà l'ispettorato del lavoro a indicare le modalità per l'uso di tali impianti.

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.
L'ente, riservandosi 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. In attuazione di tale principio:

- I controlli saranno effettuati inizialmente solo su dati aggregati riferiti all'intera struttura ovvero a singole aree lavorative;
- Nel caso in cui si dovessero riscontrare violazioni del presente regolamento, 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 dell'ente, 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.

L'ente titolare 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.

Una lista dei sistemi utilizzati può essere trovata nell'allegato A del presente regolamento.

Capo II — MISURE ORGANIZZATIVE

Art. 6 – Amministratori di sistema

L'ente conferisce, ad uno o più, amministratori di sistema il compito di sovrintendere ai beni e alle risorse informatiche dell'ente. È compito dell'amministratore di sistema:

- Gestire l'hardware e il software di tutta la strumentazione informatica di appartenenza dell'ente;
- 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;
- 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;
- 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;
- 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; Provvedere alla sicurezza informatica dei sistemi informativi dell'ente;
- 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 a un utente in caso di prolungata assenza, non rintracciabilità o impedimento dello stesso.

Tale ultima attività, tuttavia, deve essere disposta per mezzo di un soggetto che rivesta quantomeno la posizione di soggetto autorizzato al trattamento dei dati personali (o *designato*) all'interno dell'ente e deve essere limitata altresì al tempo strettamente necessario al compimento delle attività indifferibili per cui è stato richiesto.

La lista degli amministratori di sistema può essere trovata nell'allegato B del presente regolamento.

Art. 7 – Assegnazione degli account e gestione delle password

Art 7.1 – Creazione e Gestione degli Account

Un account utente consente l'autenticazione dell'utilizzatore e di conseguenza ne disciplina l'accesso alle risorse informatiche dell'ente per singola risorsa lavorativa.

Gli account utenti vengono creati dagli amministratori di sistema e sono personali, cioè, associati univocamente alla persona assegnataria. Ogni utente è responsabile dell'utilizzo del proprio account utente.

L'accesso al proprio account avviene tramite l'utilizzo delle "credenziali di autenticazione", solitamente username e password, comunicate all'utente dall'amministratore di sistema che le genera con modalità tali da garantirne la segretezza.

Le credenziali di autenticazione costituiscono dati dell'ente da mantenere strettamente riservati e non è consentito comunicarne gli estremi a terzi, anche a 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 questo associate, è tenuto a modificare immediatamente la password e a segnalare la violazione all'amministratore del sistema nonché al responsabile privacy di riferimento.

In caso di assenza improvvisa o prolungata del lavoratore e per improrogabili necessità legate all'attività lavorativa, per le esigenze produttive dell'ente o per la sicurezza e operatività delle risorse informatiche, l'ente si riserva la facoltà di accedere a qualsiasi dotazione o apparato assegnato in uso all'utente per mezzo dell'intervento dell'amministratore di sistema.

I beni e la strumentazione informatica oggetto del presente regolamento rimangono di esclusivo dominio dell'ente, che in conseguenza dei rapporti instaurati con gli utenti ne disciplina l'assegnazione.

Art 7.2 – Gestione e Utilizzo delle Password

A seguito della prima comunicazione delle credenziali di autenticazione da parte dell'amministratore di sistema, l'utente **ha il compito** di modificare la propria password:

- Al primo utilizzo.
- Ogni qualvolta l'utente ha il sospetto o l'evidenza di una sua compromissione.
- Almeno ogni 12 mesi.
- Nel caso di trattamento di categorie particolari di dati personali (art. 9 GDPR) o relativi a condanne penali o reati (art. 10 GDPR), almeno ogni 6 mesi. Nel caso di un amministratore di sistema ogni 3 mesi.

L'utente deve rispettare le seguenti regole:

- Utilizzare almeno 10 caratteri alfanumerici. *(Non è obbligatorio inserire numeri e simboli)*
- Proteggere con la massima cura la riservatezza della password ed utilizzarla entro i limiti di autorizzazione concessi;

L'utente **non può**:

- Includere parti del nome, cognome o comunque elementi a lui agevolmente riconducibili;
- Utilizzare password comuni o prevedibili;
- Utilizzare password presenti in liste esfiltrate in passato e presenti in rete.
- Scrivere la password su post-it o altri supporti non è conforme alla normativa, questo comprometterebbe in maniera pressoché totale le misure di sicurezza previste, costituisce violazione del presente regolamento e comporta l'applicazione di sanzioni.

È fortemente consigliato l'utilizzo di un Password Manager.

Le linee di utilizzo delle password sono conformi alle linee guida NIST 800-63: https://pages.nist.gov/800-63-3/sp800-63-3.html

Art 7.3 – Cessazione Degli Account

In caso di interruzione del rapporto di lavoro con l'utente, le credenziali di autenticazione verranno:

- Sospese entro le 24 ore lavorative.
- Eliminate definitivamente da tutti i sistemi entro i 7 giorni lavorativi.

Resta in capo all'utente la possibilità di richiedere l'eliminazione immediata delle credenziali di accesso.

Art. 8 – Postazioni di lavoro

Per postazione di lavoro si intende il complesso unitario di personal computer (di seguito pc), notebook, tablet, smartphone, accessori, periferiche e ogni altro dispositivo (*device*) concesso in utilizzo all'utente. L'assegnatario di tali beni e strumenti informatici dell'ente 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 seguenti regole tecniche:

- Ogni pc, notebook (accessori e periferiche incluse), tablet, smartphone o altro dispositivo (*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 all'attività svolta.
- È 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 dall'ente. Per utilizzare software o applicativi non presenti nella dotazione standard fornita è necessario presentare espressa richiesta scritta al proprio responsabile di riferimento o all'amministratore di sistema, il quale ne valuterà i requisiti tecnici, l'aderenza alle policy interne e al ruolo ricoperto nell'ente.
- 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 di sistema o al proprio responsabile di riferimento eventuali guasti e problematiche tecniche rilevati o il cattivo funzionamento delle apparecchiature.
- È fatto divieto di cedere in uso, anche temporaneo, le attrezzature e i beni informatici dell'ente a soggetti terzi.
- L'ente si riserva la facoltà di rimuovere d'ufficio e senza alcun preavviso qualsiasi elemento hardware o software la cui installazione non sia stata appositamente e preventivamente prevista o autorizzata.

Gli apparecchi di proprietà personale dell'utente quali computer portatili, telefoni cellulari, smartphone, agende palmari, hard disk esterni, penne USB, lettori musicali o di altro tipo, fotocamere digitali e qualsiasi altro dispositivo non potranno essere collegati ai computer o alle reti informatiche dell'ente salvo preventiva autorizzazione scritta dell'ente.

CAPO III – CRITERI DI UTILIZZO DEGLI STRUMENTI INFORMATICI

Art. 9 – Dispositivi (*devices*): Desktop, Laptop, Tablet, Smartphone, etc.

Per l'espletamento delle proprie mansioni gli utenti utilizzano dispositivi (*devices*) di proprietà dell'ente e sono tenuti al rispetto delle seguenti regole:

- Non è consentito modificare la configurazione hardware e software del proprio dispositivo (*device*), se non previa esplicita autorizzazione dell'ente (per le modalità operative fare riferimento a quanto riportato all'art. 19 – Comunicazioni) 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, applicativi e ogni altro software non autorizzato espressamente dall'ente;
- È onere dell'utente, in relazione alle sue competenze lavorative, 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;
- È onere dell'utente spegnere il proprio PC al termine del lavoro. Per quanto concerne la gestione dei computer e degli altri dispositivi portatili, l'utente ha l'obbligo di custodirli con diligenza e in luogo protetto durante gli spostamenti, rimuovendo gli eventuali files elaborati prima della loro riconsegna;
- Non è consentito all'utente caricare o inserire all'interno del computer o di altri dispositivi portatili qualsiasi dato personale non attinente con l'attività lavorativa svolta.

In ogni caso, al fine di evitare o almeno ridurre al minimo la possibile circolazione di dati personali sul medesimo apparecchio, gli utenti devono cancellare tutti quelli eventualmente presenti prima di consegnare il dispositivo agli uffici competenti per la restituzione o la riparazione.

In caso siano riscontrati abusi reiterati da parte degli Utenti, verranno inoltrati preventivi avvisi collettivi con possibilità di controlli su singoli dispositivi o postazioni.

Fatto salvo il caso di non funzionalità del sistema, rispetto ai controlli di cui sopra, gli interessati, compatibilmente con la gravità del rischio e la relativa tempistica di intervento, vengono preventivamente informati dall'Amministratore di Sistema che effettua l'intervento relativamente alle modalità, alle finalità del controllo, oltre che ai trattamenti di dati che possono riguardarli.

L'Azienda informa che il personale che opera con profili di Amministratore di Sistema è autorizzato a compiere interventi su tutto il sistema informatico al fine di garantirne la sicurezza e la salvaguardia, nonché per motivi tecnici e/o manutentivi (ad es. aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, ecc.).

Gli amministratori di sistema, o gli operatori di sistema, possono collegarsi in remoto

CAPO III – CRITERI DI UTILIZZO DEGLI STRUMENTI INFORMATICI

Art. 9 – Dispositivi (*devices*): Desktop, Laptop, Tablet, Smartphone, etc.

Per l'espletamento delle proprie mansioni gli utenti utilizzano dispositivi (*devices*) di proprietà dell'ente e sono tenuti al rispetto delle seguenti regole:

- Non è consentito modificare la configurazione hardware e software del proprio dispositivo (*device*), se non previa esplicita autorizzazione dell'ente (per le modalità operative fare riferimento a quanto riportato all'art. 19 – Comunicazioni) 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, applicativi e ogni altro software non autorizzato espressamente dall'ente;
- È onere dell'utente, in relazione alle sue competenze lavorative, 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;
- È onere dell'utente spegnere il proprio PC al termine del lavoro. Per quanto concerne la gestione dei computer e degli altri dispositivi portatili, l'utente ha l'obbligo di custodirli con diligenza e in luogo protetto durante gli spostamenti, rimuovendo gli eventuali files elaborati prima della loro riconsegna;
- Non è consentito all'utente caricare o inserire all'interno del computer o di altri dispositivi portatili qualsiasi dato personale non attinente con l'attività lavorativa svolta.

In ogni caso, al fine di evitare o almeno ridurre al minimo la possibile circolazione di dati personali sul medesimo apparecchio, gli utenti devono cancellare tutti quelli eventualmente presenti prima di consegnare il dispositivo agli uffici competenti per la restituzione o la riparazione.

In caso siano riscontrati abusi reiterati da parte degli Utenti, verranno inoltrati preventivi avvisi collettivi con possibilità di controlli su singoli dispositivi o postazioni.

Fatto salvo il caso di non funzionalità del sistema, rispetto ai controlli di cui sopra, gli interessati, compatibilmente con la gravità del rischio e la relativa tempistica di intervento, vengono preventivamente informati dall'Amministratore di Sistema che effettua l'intervento relativamente alle modalità, alle finalità del controllo, oltre che ai trattamenti di dati che possono riguardarli.

L'Azienda informa che il personale che opera con profili di Amministratore di Sistema è autorizzato a compiere interventi su tutto il sistema informatico al fine di garantirne la sicurezza e la salvaguardia, nonché per motivi tecnici e/o manutentivi (ad es. aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, ecc.).

Gli amministratori di sistema, o gli operatori di sistema, possono collegarsi in remoto ai singoli PC al fine di garantire l'assistenza tecnica e la normale attività operativa. ai singoli PC al fine di garantire l'assistenza tecnica e la normale attività operativa.
L'utente dovrà attenersi ai suddetti limiti; in caso contrario potrà essere richiesto il rimborso dei costi sostenuti per il loro superamento.

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: cd-rom, dvd, pen-drive USB, riproduttori musicali mp3, fotocamere digitali, dischi rigidi esterni, ecc.

L’utilizzo di tali supporti risponde alle direttive di seguito riportate:

- non è consentito utilizzare supporti rimovibili personali, se non preventivamente autorizzati per iscritto dall’ente (per le modalità operative fare riferimento a quanto riportato all’art. 19 – Comunicazioni);
- è onere dell’utente custodire i supporti contenenti categorie particolari di dati (art. 9 GDPR) o dati relativi a condanne penali e a reati (art. 10 GDPR) in armadi chiusi a chiave, onde evitare che il loro contenuto possa essere trafugato o alterato o distrutto;

Se autorizzati in base alle procedure previste, una volta connessi all’infrastruttura informatica dell’ente, i dispositivi saranno soggetti (ove ciò sia compatibile) al presente regolamento.

Art. 13 – Stampanti, fotocopiatrici e fax

L’utilizzo di tali 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.

Quando si inviano documenti contenenti dati personali o informazioni riservate su una stampante condivisa è richiesta una particolare attenzione; ciò al fine di evitare che persone non autorizzate possano venire a conoscenza del contenuto della stampa. Bisogna evitare quindi di lasciare le stampe incustodite e ritirare immediatamente le copie appena stampate.

L’utilizzo di fax per l’invio di documenti che hanno natura strettamente confidenziale è generalmente da evitare. In caso ciò sia necessario si deve preventivamente avvisare il destinatario in modo da ridurre il rischio che persone non autorizzate possano venire a conoscenza del contenuto della comunicazione e successivamente chiedere la conferma telefonica di avvenuta ricezione.

Gli strumenti dotati di memoria, connessi o meno in rete, sono gestiti dall’Amministratore di Sistema che provvede alla cancellazione periodica del loro contenuto e a tutte le operazioni ritenute necessarie per garantirne la sicurezza.

Art. 14 – Strumenti di fonia mobile o di connettività in mobilità

A seconda del ruolo o della funzione del singolo utente, l’ente rende disponibili impianti di telefonia fissa e mobile e inoltre dispositivi quali smartphone e tablet che consentono di usufruire sia della navigazione in Internet tramite rete dati che del servizio di telefonia tramite rete mobile.

Le specifiche relative ai limiti entro cui l’utente potrà utilizzare tali strumenti sono riportate nella scheda tecnica consegnata unitamente al dispositivo. L’utente dovrà attenersi ai suddetti limiti e in caso contrario potrà essere richiesto il rimborso dei costi sostenuti per il loro superamento.

Come per qualsiasi altra dotazione dell’ente, il dispositivo mobile rappresenta un bene dell’ente concesso in uso per scopi esclusivamente lavorativi. È tuttavia permesso un utilizzo personale sporadico e moderato dei telefoni dell’ente utilizzando la “diligenza del buon padre di famiglia” prevista dalla normativa e comunque tale da non ledere il rapporto fiduciario instaurato con il proprio datore di lavoro.

Al fine di controllo del corretto utilizzo dei servizi di fonia dell'ente, l'ente può esercitare i diritti di cui all'art. 124 D.Lgs. 196/2003 (fatturazione dettagliata) richiedendo ai provider di telefonia i dettagli necessari agli accertamenti sull'uso e relativo costo del traffico effettuato nel tempo.

I controlli saranno eseguiti secondo criteri e modalità descritte all'art. 5 del presente regolamento. Qualora dall'esame del traffico di una singola utenza si rilevi uno scostamento significativo rispetto alla media del consumo sarà richiesto il tabulato analitico delle chiamate effettuate dalla SIM in incarico all'utente per il periodo interessato.
L'utilizzo dei dispositivi mobili risponde alle seguenti regole:

- Ciascun 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, per esempio codice PIN del dispositivo, che ne impedisca l'utilizzo da parte di altri soggetti. A tal fine si precisa che:
- il codice PIN dovrà essere composto da quattro o cinque cifre numeriche, altri codici di accesso dovranno garantire analoga protezione; il codice PIN o altri codici di accesso dovranno essere modificati 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 all'ente.
- In caso di furto, danneggiamento o smarrimento del dispositivo mobile l'utente assegnatario dovrà darne immediato avviso all'ente; se tali eventi siano riconducibili a un comportamento negligente o imprudente dell'utente stesso o comunque a sua colpa nella custodia del bene, lo stesso sarà ritenuto unico responsabile dei danni derivanti;
- In caso di furto o smarrimento l'ente si riserva la facoltà di attuare la procedura di cancellazione da remoto di tutti i dati sul dispositivo, rendendo il dispositivo stesso inutilizzabile e i dati in esso contenuti del tutto 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 o almeno ridurre la circolazione di dati personali sull'apparecchio, è obbligatorio cancellare tutti i dati eventualmente presenti prima di consegnare il dispositivo 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 a meno che non siano strettamente connesse con gli scopi ricoperti dal proprio ruolo e siano preventivamente autorizzate dall'ente;
- L'installazione di applicazioni, gratuite o a pagamento, su smartphone e tablet deve essere espressamente autorizzata, rimanendo in caso contrario a carico dell'utente le responsabilità derivanti dall'installazione non autorizzata che costituisce violazione del presente regolamento;
- Salvo diversi specifici accordi derivanti da esigenze di servizio, al momento della consegna di 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'ente potrebbe venire a conoscenza, seppur incidentalmente, dei dati relativi alla posizione del dispositivo stesso e del suo assegnatario.

Art. 15 – Archiviazione di dati, file e cartelle

L'Utente è responsabile del dispositivo lavorativo assegnatogli. Tutte le attività svolte mediante l'ausilio di detto strumento devono sempre garantire la custodia e la tutela dei dati dell'ente adottando tutti i provvedimenti che le circostanze rendono necessari per evitare danni o sottrazioni di dati, informazioni o documenti di proprietà del Titolare del Trattamento.

L'utilizzo del dispositivo dell'ente è strettamente legato all'attività lavorativa e deve avvenire sempre nel pieno rispetto dei principi etici, di buon costume e dell'ordine pubblico.

A ciascun Utente viene assegnata una cartella personale di rete (ad uso esclusivo), una cartella sul sistema Cloud dell'ente (ad uso esclusivo) e viene concesso l'accesso alle cartelle di rete ed alle cartelle del Cloud di cui ha bisogno per svolgere le sue mansioni all'interno dell'ente.

Nel momento in cui fosse necessario abilitare l'Utente all'accesso a specifiche ulteriori cartelle di rete, il Direttore Amministrativo provvede con formale richiesta all'amministratore di Sistema.

Le finalità di utilizzo di tali cartelle sono inerenti alle mansioni lavorative e di conseguenza non ne è permesso l'utilizzo per la conservazione di propri file e dati personali.

Utente deve procedere ad effettuare il salvataggio di dati e file sulle cartelle di rete o in Cloud in base alla catalogazione effettuata dal proprio ufficio di competenza.

Non è consentito l'utilizzo delle cartelle locali per il salvataggio e la conservazione dei dati (ad esempio Desktop, Downlod, Documents, etc.). Poiché, questi dati sono considerati temporanei (cartella Download) o personali non inerenti all'attività lavorativa (cartelle Documents, Desktop etc.) non saranno soggetti alle attività di backup centralizzato con il conseguente rischio di non poter recuperare gli stessi in caso di evento disastroso ed esponendo l'ente al rischio di un Data Breach in caso di furto o smarrimento del pc.
Le unità di rete ed i dispositivi aziendali sono aree di condivisione di informazioni strettamente lavorative e non possono in alcun modo essere utilizzate per scopi diversi. Costituisce buona regola la periodica pulizia degli archivi, con cancellazione dei file obsoleti o inutili.
Particolare attenzione deve essere prestata alla duplicazione dei dati, è, infatti, assolutamente da evitare un'archiviazione ridondante che non consenta in modo chiaro ed inequivocabile, l'identificazione dello stato di revisione di un documento.

L'Utente non deve testare o tentare di compromettere il sistema informatico o le misure di sicurezza implementate attraverso attività di hacking o altri simili tentativi.

L'Utente può fare richiesta, all'amministratore di sistema, di avere un backup automatico all'interno delle cartelle di rete, oppure nel Cloud dell'ente, i contenuti delle cartelle Desktop e Documenti. Dato che questa pratica può portare l'organizzazione a

raccogliere involontariamente dati personali dell'Utente, l'Utente deve consegnare il modulo di consenso, allegato C del presente regolamento.

Art. 16 - Smart Working

Gli Utenti che svolgono la prestazione lavorativa in modalità "Smart Working" sono tenuti al rispetto delle seguenti istruzioni:

- ogni trattamento deve essere effettuato obbligatoriamente per mezzo degli strumenti elettronici forniti dal Titolare del Trattamento;
- è fatto divieto di effettuare trattamenti mediante dispositivi privati (ad esempio connettendosi alla rete aziendale mediante VPN con dispositivi diversi da quelli forniti dal Titolare del Trattamento, fatto salvo i casi di assoluta necessità, previa acquisizione dell'autorizzazione da parte del responsabile e previa adeguata predisposizione di misure idonee a rendere sicuri i mezzi utilizzati;
- è fatto divieto di salvare o trasmettere copie dei dati personali trattati, o dei files nei quali essi sono contenuti, sui mezzi informatici privati o messi a disposizione da terzi, anche a scopi operativi, nonché di effettuare stampe o comunicazioni e-mail contenenti (nel testo o negli allegati) dati personali per mezzo di strumenti informatici privati o messi a disposizione da terzi;
- l'accesso agli strumenti deve avvenire mediante autenticazione con credenziali concesse dall'ente;
- L'utilizzo degli strumenti elettronici di lavoro deve essere effettuato in modo da non rivelare dati personali del lavoratore o di terzi, soprattutto se dati particolari ai sensi dell'art. 9, par. 1 del Reg. UE 2016/679 (es. non effettuare videochiamate in presenza di terzi nelle vicinanze);
- Il lavoratore, adeguatamente formato ed istruito, deve attenersi in modo stringente alle istruzioni impartite e, in caso di malfunzionamenti, errori umani o altre cause di conclamata o sospetta violazione delle presenti misure di sicurezza, della policy e delle istruzioni ricevute, deve darne immediata comunicazione al proprio Amministratore di Sistema e, nel rispetto degli orari di lavoro concordati, rendersi immediatamente disponibile per ogni azione riparatoria necessaria;

Il lavoratore deve avere cura che nessun soggetto non autorizzato entri in contatto con i dati trattati a fini lavorativi adottando misure precauzionali quali:

- scegliere postazioni di lavoro separate da spazi comuni o eseguire la prestazione in locali il cui accesso può essere limitato e controllato (es. stanza con porta chiusa);
- non lasciare gli strumenti elettronici accesi e con l'accesso all'account effettuato se non si è presenti e non consentire a terzi l'uso degli stessi per nessun motivo;
- assicurarsi che soggetti a qualsiasi titolo presenti nella propria abitazione o in locali pubblici non possano visionare dati personali, anche impedendo loro temporaneamente l'accesso al locale in cui la prestazione lavorativa è svolta o, se possibile, disconnettendo gli strumenti informatici utilizzati per il trattamento;
- se la prestazione è espletata in spazi pubblici (es. spazi di Co-Working, bar), evitare di lasciare incustoditi gli strumenti elettronici aziendali e evitare di affidarli a terzi non autorizzati;
- impostare un tempo breve per l'oscuramento del desktop, spegnendo o disconnettendosi dalla sessione lavorativa in caso di interruzioni o pause;
- evitare di stampare documenti contenenti dati personali mediante stampanti private o messe a disposizione da terzi, di conservare stampe cartacee contenenti

dati lavorativi nella propria abitazione o in luoghi pubblici (es. esercizi commerciali o spazi di Co-Working), di inviare stampe a dispositivi che non possono essere immediatamente raggiunti con il rischio, quindi, di consentirne la visione o la sottrazione a terzi non autorizzati;

- evitare di scattare fotografie, riprendere video o audio in luoghi privati o in luoghi pubblici nei quali, stante la conformazione degli stessi, non sia possibile impedire trattamenti accidentali (es. effettuare una conference call in un locale commerciale affollato);
- il lavoratore deve accertarsi che, nel luogo in cui espleta la propria prestazione lavorativa, non siano messe in atto tecniche o implementate strumentazioni atte ad aggirare le eventuali misure di sicurezza o limitative degli accessi o del traffico internet predisposte dalla committente al fine di effettuare, per mezzo degli strumenti tecnologici forniti dal Titolare del Trattamento, connessioni o operazioni ritenute inappropriate;
- al fine di consentire al Titolare del Trattamento di effettuare, sugli strumenti elettronici di lavoro, controlli volti alla garanzia della sicurezza dei trattamenti di dati personali che non risultino sproporzionati e ingiustamente pervasivi della sfera personale del lavoratore, quest'ultimo deve predisporre ogni ragionevole accorgimento al fine di consentire un accesso agli account e agli strumenti che non comporti fisiologicamente l'accesso a dati personali suoi o di terzi;

Il Titolare del Trattamento limiterà la conservazione di dati relativi agli accessi e alla rete internet degli utenti ed al traffico telematico ai dati relativi l'esecuzione della prestazione lavorativa; il lavoratore deve porre in essere ogni utile accorgimento per separare l'attività privata da quella lavorativa, come ad esempio rispettare gli orari di lavoro e le pause, non conservare dati personali propri o di terzi sugli strumenti informatici ad uso lavorativo e limitare il traffico su internet per finalità diverse dall'esecuzione della prestazione lavorativa ad orari non di lavoro e, se possibile, a devices privati.

Capo IV — GESTIONE DELLE COMUNICAZIONI TELEMATICHE

Art. 17 – Gestione utilizzo della rete internet

Ciascun utente potrà essere abilitato alla navigazione Internet mediante l'utilizzo delle credenziali personali su postazioni PC già connesse alla rete, reti wireless e reti ethernet e pertanto si richiamano tutti gli utenti a una particolare attenzione al suo utilizzo consapevole così come dei servizi collegati, in quanto ogni operazione posta in essere è associata all'"Indirizzo Internet Pubblico" assegnato all'ente.

La connessione a Internet, in quanto strumento a disposizione degli utenti per uso professionale, deve essere utilizzata in maniera appropriata, tenendo presente che ogni sito web può essere governato da leggi diverse da quelle vigenti in Italia; ciò deve essere tenuto in considerazione in modo da prendere ogni precauzione conseguente.

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

- L'utilizzo è consentito esclusivamente per scopi preposti 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 o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale o politica;
- È consentito l'utilizzo di soluzioni di Instant Messanger o chat esclusivamente per scopi professionali e attraverso strumenti e software messi a disposizione dall'ente;
- Non è consentito l'utilizzo di sistemi di social networking all'interno della rete dell'ente a meno che non abbia uno specifico scopo lavorativo o didattico con l'autorizzazione dell'Amministratore di Sistema;
- Non è consentito lo scambio o la condivisione di materiale audiovisivo, cinematografico, fotografico, informatico o altro anche se non protetto da copyright utilizzando sistemi Peer-to- Peer, a qualsiasi titolo e anche se non a scopo di lucro.

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 preventivamente ed espressamente approvata.

È altresì proibito rigorosamente qualsiasi uso del Web che non trasmetta un'immagine positiva o che possa essere in qualunque modo essere nocivo all'immagine dell'ente.

Per mezzo dell'Amministratore di Sistema e al fine di facilitare il rispetto delle predette regole l'ente si riserva la facoltà di configurare specifici filtri che inibiscono l'accesso ai contenuti non consentiti, con esclusione dei siti istituzionali, e che prevengono operazioni non correlate all'attività lavorativa: a titolo esemplificativo e non esaustivo upload, restrizione nella navigazione, download di file o software.
Una lista dei sistemi utilizzati e dei filtri è disponibile nell'allegato A del presente regolamento

Art. 18 – Gestione e utilizzo della posta elettronica su dominio dell'ente

Art 18.1– Principi Guida

Per ciascun 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: 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 vengono assegnate più caselle di posta elettronica collettive (gruppi o caselle condivise), che possono anche essere condivise con altri utenti dello stesso gruppo/ufficio/dipartimento.

L’utente deve utilizzare le caselle collettive per tutte le attività lavorative (in ingresso ed in uscita) verso un dominio esterno a quello dell’ente ed utilizzare l’account personale (in ingresso ed in uscita) esclusivamente per le comunicazioni interne al dominio dell’ente.

L’ente valuterà caso per caso, previa richiesta dell’utente, la possibilità di attribuire allo stesso un diverso indirizzo destinato ad uso privato.
Attraverso le caselle e-mail su dominio 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 positivamente l’immagine dell’ente.

Gli utenti sono responsabili del corretto utilizzo delle caselle di posta elettronica su dominio dell’ente conformemente alle presenti regole. Gli stessi **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 (agenti di alterazione, ad esempio 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 alle e-mail pervenute solo da emittenti conosciuti e cancellare preventivamente le altre;
- collegarsi a siti internet contenuti all’interno di messaggi solo per motivate ragioni e quando vi sia comprovata sicurezza sul contenuto degli stessi.

Inoltre, **non è consentito** agli utenti:

- diffondere il proprio indirizzo e-mail su dominio dell’ente attraverso la rete internet;
- utilizzare la casella di posta elettronica su dominio dell’ente per inviare, ricevere o scaricare allegati contenenti video, brani musicali, ecc., salvo che questo non sia funzionale all’attività prestata in favore dell'ente, per esempio presentazioni o materiali video dell’ente.
- Non è consentito l’inoltro automatico della posta elettronica ad indirizzi esterni al dominio dell’ente.

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”.

Qualora si dovessero inviare informazioni “riservate” o “strettamente confidenziali” è obbligatorio l’utilizzo della “Modalità riservata” con scadenza e Passcode SMS.

Ogni messaggio inviato da un qualunque indirizzo del dominio dell’ente verrà sempre accompagnato dal disclaimer:

"Si segnala che il presente messaggio e le risposte allo stesso potranno essere conosciute dall'organizzazione di appartenenza del mittente secondo le modalità previste dal regolamento dell'organizzazione adottato in materia. Se per un disguido avete ricevuto questa e-mail senza esserne i destinatari vogliate cortesemente distruggerla e darne informazione all'indirizzo mittente"

Nei casi in cui l'ente si doti di posta elettronica certificata per i singoli utenti o generiche si applicheranno, ove compatibili, le presenti disposizioni.

Art 18.2 - Cessazione dell'indirizzo di Posta Elettronica Individuale su dominio dell'ente

In caso di interruzione del rapporto di lavoro con l'utente, si procederà come segue:

- La casella individuale verrà disabilitata in massimo 24 ore lavorative.
- Qualora alla casella di posta individuale era concessa la possibilità di scrivere all'esterno del dominio e conduceva personalmente delle conversazioni con clienti/fornitori:
  - vengono informati gli uffici competenti ed RPD/DPO
  - l'utente insieme all'amministratore di sistema effettueranno una fase di "preeliminazione" accedendo insieme alla casella di posta individuale per salvare o inoltrare alla propria casella di posta personale la posta personale ed inoltrare al proprio dipartimento tutte le e-mail non personali.
  - "pre-eliminazione" sarà effettuata per il tramite di idoneo "fiduciario", da intendersi quale lavoratore previamente nominato e/o incaricato per iscritto dall'utente assente.
  - La casella individuale verrà eliminata definitivamente entro 7 (sette) giorni lavorativi dalla fase di "pre-eliminazione".
- Qualora alla casella di posta individuale non era concessa la possibilità di scrivere all'esterno del dominio.
  - Verrà eliminata la casella di posta individuale entro 7 (sette) giorni lavorativi.
  - L'utente può richiedere l'eliminazione immediata della casella di posta individuale.

Il sistema genererà, alla disabilitazione, un messaggio automatico al mittente informando che la casella di posta elettronica è stata disattivata con i riferimenti del suo sostituto, ma non verrà inoltrata, né verrà salvata dal sistema.
In caso di cessazione del rapporto lavorativo le caselle di posta elettronica collettive (gruppi o caselle condivise) non verranno alterate e le comunicazioni lavorative inviate o ricevute nelle caselle collettive rimarranno invariate ed immutabili in quanto chiare comunicazioni per conto dell'ente inviate tramite casella di posta collettiva.

Art 18.3 – Prolungata assenza dell'utente

Saranno messe a disposizione di ciascun utente, con modalità di agevole esecuzione, apposite funzionalità del sistema di posta elettronica che in caso di assenze programmate consentano l'inoltro ad un altro utente, oppure di inviare automaticamente messaggi di risposta contenenti 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 assenze non programmate, ad esempio per malattia, qualora il lavoratore non possa attivare la procedura descritta anche avvalendosi di servizi webmail da

remoto e perdurando l'assenza oltre il limite temporale di 7 (sette) giorni l'ente disporrà, lecitamente e mediante personale appositamente incaricato (l'Amministratore di Sistema oppure un suo incaricato), l'attivazione di un analogo accorgimento (risposta automatica o re-indirizzamento), avvertendo l'assente.

Art. 19 – Accesso agli strumenti elettronici in caso di assenza dell'Utente (dispositivi, email etc.)

Nei casi di prolungata assenza o impedimento del Lavoratore, che renda indispensabile e indifferibile intervenire per esclusive finalità di operatività e di sicurezza del sistema, potrebbe rendersi necessario accedere agli strumenti ed ai dati dell'utente.

In previsione del verificarsi di tali condizioni l'Utente può nominare un Fiduciario (si veda Allegato D), che abbia gli stessi profili di autorizzazione, a presenziare all'accesso al proprio computer, che avverrà secondo la procedura sotto riportata:

- Il Direttore Amministrativo/Responsabile di dipartimento invierà la richiesta all'Amministratore di Sistema ed al Responsabile per la Protezione dei Dati (RPD/DPO);
- L'amministratore di Sistema, ricevuta l'autorizzazione dall' RDP/DPO, provvederà a resettare e sostituire le credenziali di autenticazione per l'accesso al PC e/o alla casella di posta elettronica su dominio dell'ente dell'Utente assente;
- il Responsabile di Dipartimento o il Direttore Amministrativo, alla presenza dell'eventuale fiduciario nominato, procederà nella ricerca dei file e/o delle e-mail utili ai fini delle necessità lavorative di cui sopra;
- di tale attività sarà redatto apposito verbale e informato l'utente interessato alla prima occasione utile;

Al suo rientro, l'Utente dovrà cambiare la password di accesso allo strumento secondo l'Art 7.2 del presente regolamento.

Capo V — SANZIONI, FORMAZIONE, COMUNICAZIONI, APPROVAZIONE

Art. 20 – Sanzioni

La violazione di quanto previsto dal presente regolamento, rilevante anche ai sensi degli artt. 2104 e 2105 c.c., potrà comportare l'applicazione di sanzioni disciplinari in base a quanto previsto dall'art. 7 (sanzioni disciplinari) della Legge 20 maggio 1970 n.300 (Statuto dei Lavoratori).

Nel caso venga commesso un reato o la cui commissione sia ritenuta probabile o solo sospettata l'ente avrà cura di informare senza ritardo, e senza necessità di preventive contestazioni o addebiti formali, le autorità competenti dell'utilizzo illecito o non conforme dei beni e degli strumenti informatici dell'ente.

In caso di violazione accertata delle regole e degli obblighi esposti in questo regolamento da parte degli utenti 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 o la funzionalità dei propri beni e strumenti informatici e inoltre per impedire il reitero di tale violazione.

Art. 21 – Formazione

il Titolare del Trattamento predispone regolari sessioni formative ed informative per garantire a tutti gli incaricati il massimo aggiornamento in merito ai rischi, alle

procedure operative, alla prevenzione dei danni e, più in generale, alle problematiche relative alla sicurezza in materia di trattamento dei dati. Il Lavoratore potrà comunque rivolgersi al Titolare del Trattamento per ogni chiarimento in merito.

Art. 22 – Informativa agli utenti ex art. 13 Regolamento (UE) 2016/679

Il presente regolamento, nella parte in cui contiene le regole per l'utilizzo dei beni e degli strumenti informatici dell'ente e relativamente al trattamento di dati personali svolti dall'ente finalizzato all'effettuazione di controlli leciti, così come definiti nell'art. 5, vale quale informativa ex art. 13 del Regolamento (UE) 2016/679.

Art. 23 – Comunicazioni

Contestualmente all'assegnazione di un account il presente regolamento è messo a disposizione degli utenti per la consultazione. La versione più aggiornata dello stesso è pubblicata sia in formato immateriale digitale che in formato fisico cartaceo allo scopo di facilitarne la diffusione a tutti gli interessati.

Per ogni aggiornamento del presente regolamento sarà data comunicazione sulle bacheche dell'ente e tramite l'invio di specifico messaggio e-mail e tutti gli utenti sono tenuti a conformarsi alla versione più aggiornata.

Le richieste di autorizzazione o concessione previste dal presente regolamento possono essere inoltrate all'ente per mezzo di qualsiasi strumento che ne garantisca la tracciabilità, ad esempio tramite e-mail, a cui è riconosciuto il valore di forma scritta in modo del tutto analogo rispetto a quella cartacea.

Art. 24 – Norme di riferimento e provvedimenti

a. la Legge 20.5.1970, n. 300, recante "Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro e norme sul collocamento"; in particolare l'art. 4, comma 1, della Legge 300/1970, secondo cui la regolamentazione dell'uso degli strumenti informatici non è finalizzata all'esercizio di un controllo a distanza dei lavoratori da parte del datore di lavoro ma solo a permettere a quest'ultimo di utilizzare sistemi informativi per fare fronte ad esigenze produttive od organizzative e di sicurezza nel trattamento dei dati personali;
b. il Regolamento Europeo 679/16 "General Data Protection Regulation"; in particolare viene garantito al singolo lavoratore il controllo sui propri dati personali secondo quanto previsto dagli articoli 15-16-17-18-20-21-77 del Reg. 2016/679;
c. le "Linee guida del Garante per posta elettronica e internet" in Gazzetta Ufficiale n. 58 del 10 marzo 2007;
d. l'articolo 23 del D.lgs. n. 151/2015 (c.d. Jobs Act) che modifica e rimodula la fattispecie integrante il divieto dei controlli a distanza, nella consapevolezza di dover tener conto, nell'attuale contesto produttivo, oltre agli impianti audiovisivi, anche degli altri strumenti «dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori» e di quelli «utilizzati dal lavoratore per rendere la prestazione lavorativa»;
e. Linea guida del Garante per posta elettronica e internet, deliberazione n°13 del 1° marzo 2007 – G.U. n° 58 del 10 marzo 2007;
f. Linea guida del Garante per il trattamento di dati dei dipendenti privati, deliberazione del 23 novembre 2006 - G.U. 7 dicembre 2006, n. 285;

g. D.Lgs 151/2015 e D.Lgs 101/2018;
h. Registro dei provvedimenti n. 370 del 4 ottobre 2011 Garante Privacy: Sistemi di localizzazione dei veicoli nell'ambito del rapporto di lavoro - 4 ottobre 2011;
i. Legge 22 Maggio 2017, n. 81 Capo II Lavoro Agile.

Art. 25 – Modifiche del regolamento

Il Titolare del Trattamento potrà in ogni momento effettuare modifiche al presente Regolamento. Le modifiche potranno essere notificate via posta elettronica e/o mediante comunicazione scritta. Le modifiche, che saranno comunque rese note ai dipendenti, si daranno per operanti, indipendentemente dalla loro sottoscrizione da parte di ciascun destinatario, dal momento della loro comunicazione.

Art. 26 – Approvazione del Regolamento

Il presente regolamento è stato approvato dal Legale Rappresentante dell'ente.

CAPO VI – ALLEGATI

A. Strumenti dai quali deriva la possibilità di controllo a distanza dell'attività.

B. Contatti e compiti di Amministratori di Sistema, Operatori di Sistema.

C. Consenso al backup delle cartelle personali.

D. Nomina di un fiduciario per l'accesso agli strumenti elettronici.

E. Informativa sulla Privacy per i Dipendenti.

F. Misure tecnico-organizzative per la sicurezza dei dati.

G. Politica di Conservazione dei Dati, Backup e Disaster Recovery.

H. Elenco soggetti esterni autorizzati al trattamento dei dati personali.

I. Registro delle attività di trattamento dei dati.

J. Revisioni del regolamento. K. Regolamento per l'utilizzo delle piattaforme di produttività (Microsoft 365, Google

Workspace etc).

LUOGO E DATA

Il Titolare del Trattamento