REGOLAMENTO
PER L'UTILIZZO DEI DISPOSITIVI INFORMATICI, DELLA RETE INTERNET E IL TRATTAMENTO DEGLI ARCHIVI CARTACEI

Tabella di revisione

Rev. n.	Data approvazione	Descrizione delle modifiche	Approvazione
00	29.08.2024	Prima emissione	Verbale CDA n.219
01			
02			
03			
04			
05			

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 aziendali 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.

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 in gazzetta Ufficiale n. 58 del 10 marzo 2007) ed in adempimento al decreto del Presidente della Repubblica del 16 aprile 2013, n. 62, recante: «Codice di comportamento dei dipendenti pubblici, a norma dell'articolo 54 del decreto legislativo 30 marzo 2001, n. 165», oltre che in ottemperanza del DPR n. 81/2023.

Art. 2 – Ambito di applicazione

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

Per utente pertanto si intende, a titolo esemplificativo e non esaustivo, ogni dipendente, collaboratore, tirocinante, consulente o altro che operi all'interno della struttura aziendale utilizzandone beni e servizi informatici e che sia in possesso di specifiche credenziali di autenticazione. Tale figura potrà venire indicata anche come "incaricato/autorizzato del trattamento".

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

Si definisce anche la figura della società che per conto del Titolare del trattamento, ovvero l'ente, si occupa della gestione dei sistemi informatici e tratta i dati per conto dell'ente, sulla base di sue specifiche istruzioni. Questa società verrà individuata come responsabile esterno del trattamento ai sensi dell'art. 28 del GDPR e all'interno della stessa verrà individuata la figura dell'amministratore di sistema, che è un tecnico informatico specializzato che viene incaricato con apposita nomina ad hoc conferita dall'ente e i cui compiti sono illustrati al seguente art. 6.

Art. 3 – Titolarità 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 dell'ente.

Ciò considerato, il loro utilizzo è consentito prevalentemente per finalità di adempimento delle mansioni lavorative affidate a ciascun utente in base al rapporto in essere, ovvero per gli 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 o informazione trattato per mezzo dei beni e delle risorse informatiche di proprietà dell'ente sarà dallo stesso considerato come avente natura aziendale e non riservata.

Art. 4 – Responsabilità personale dell'utente

Ogni utente è personalmente responsabile dell'utilizzo dei beni e delle risorse informatiche affidategli 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 e per quanto di propria competenza, è tenuto a tutelare il patrimonio aziendale 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 aziendali.

Ogni utente è tenuto ad operare a tutela della sicurezza informatica aziendale, 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.

Ogni utente viene nominato incaricato/autorizzato al trattamento dei dati con specifiche istruzioni e appositamente formato.

Art. 5 – Controlli

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

Forma Futuro, attraverso i propri responsabili di struttura, ha facoltà di svolgere gli accertamenti necessari e adottare ogni misura atta a garantire la sicurezza e la protezione dei sistemi informatici, delle informazioni e dei dati. Le modalità di svolgimento di tali accertamenti, anche se saranno verificate le future linee guida adottate dall'Agenzia per l'Italia Digitale e Garante Privacy, al momento risultano le seguenti:

- Accesso ai sistemi con profilazione personale
- Memorizzazione dei log dei sistemi e negli applicativi, dove previsto. Tali log sono memorizzati ed utilizzati/visionati solamente in caso di necessità.

- Possibilità di filtraggio del traffico internet per determinate categorie di siti (armi, pedopornografia, etc..)
- Sistemi di filtraggio della posta elettronica al fine di prevenire SPAM ed attacchi ai dipendenti di Forma Futuro.

Tuttavia, non si esclude che in futuro possano essere implementati 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 aziendali. In difetto di accordo e su istanza dell'ente sarà l'ispettorato del lavoro a indicare le modalità per l'uso di tali impianti.

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 aziendale 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 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;
- Qualora il rischio di compromissione del sistema informativo sia imminente e grave a tal punto da non permettere l'attesa dei tempi necessari per i passaggi sopra descritti, la società tecnico/informatica ovvero il Responsabile del Trattamento, per il tramite dell'Amministratore di sistema e/o suo delegato, potrà intervenire senza indugio sullo strumento da cui proviene la potenziale minaccia attuando tutte le misure tecnicamente necessarie alla soluzione del problema.

CAPO II – MISURE ORGANIZZATIVE

Art. 6 – Amministratori di sistema

L'ente conferisce all'Amministratore di sistema, il compito di sovrintendere ai beni e alle risorse informatiche aziendali. 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 aziendali;
- Utilizzare le credenziali di accesso di Amministratore di 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, non rintracciabilità o impedimento dello stesso. Tale ultima attività deve essere limitata al tempo strettamente necessario al compimento delle attività indifferibili per cui è stata richiesta.

Deve essere redatto un elenco completo degli Amministratori di sistema, contenente tutti i dati rilevanti, aggiornato ogni volta che si rilevino modifiche.

Art. 7 – Gestione delle credenziali in assenza del personale

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 e operatività delle risorse informatiche, il Titolare del Trattamento o suoi delegati possono rivolgersi all'amministratore di sistema per il reset delle credenziali (es: Dominio interno, Posta elettronica, etc..).

È fatto obbligo di comunicazione all'interessato di aver proceduto al reset delle sue credenziali e deve essere comunicato il nome del dipendente a cui sono state assegnate.

In ogni caso, l'accesso avviene nel rispetto del **principio di necessità e non eccedenza** rispetto alle attività indifferibili per il quale è stato richiesto

Al ritorno del dipendente/collaboratore a cui sono state resettate le credenziali sarà effettuato un ulteriore cambio della password in modo che l'interessato torni in pieno possesso delle proprie informazioni.

Art. 8 – Assegnazione degli account e gestione delle password

8.1 – 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, 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. La password è personale e riservata e dovrà essere conservata e custodita dall'incaricato con la massima diligenza senza divulgarla.

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 di sistema nonché al responsabile privacy di riferimento.

8.2 – Gestione e Utilizzo delle Password

A seguito della prima comunicazione delle credenziali di autenticazione da parte dell'Amministratore di sistema per poter accedere al proprio PC ed alla rete aziendale, l'utente ha il compito di modificare al primo utilizzo la propria password procedendo allo stesso modo ogni **90 giorni**. La richiesta di cambio password viene segnalata dal Sistema.

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

- La password deve essere composta da un minimo di **8 caratteri** e deve contenere almeno un carattere maiuscolo, un carattere minuscolo, un numero o un carattere non alfanumerico tipo "!@#$£$%...";
- Il sistema memorizza le ultime 5 password e ne impedisce che l'utente possa riutilizzarle;
- Evitare di includere parti del nome, cognome o comunque elementi a lui agevolmente riconducibili;
- Proteggere con la massima cura la riservatezza della password ed utilizzarla entro i limiti di autorizzazione concessi.

8.3 – Cessazione degli Account

In caso di interruzione del rapporto di lavoro con l'utente, le credenziali di autenticazione verranno disabilitate entro un periodo massimo di 7 (sette) giorni da quella data.

Art. 9 – 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 aziendali 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;
- Al fine di recepire il Decreto n°81 del 2023 all'utente è consentito l'utilizzo degli strumenti informatici forniti dall'amministrazione per poter assolvere alle incombenze personali senza doversi allontanare dalla sede di servizio, purché l'attività sia contenuta in tempi ristretti e senza alcun pregiudizio per i compiti istituzionali;
- È fatto divieto di cedere in uso, anche temporaneo, le attrezzature e i beni informatici aziendali a soggetti terzi;

- L'utente deve segnalare con la massima tempestività ai referenti interni eventuali **guasti** e problematiche tecniche rilevati o il cattivo funzionamento delle apparecchiature;
- Il pc e gli altri dispositivi di cui sopra devono essere utilizzati con **hardware e software autorizzati** dall'ente. Non è consentito installare autonomamente programmi informatici, applicativi e ogni altro software non autorizzato espressamente dall'ente;
- 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;
- Al termine del rapporto di lavoro con l'ente, sarà obbligo dell'utente restituire la disponibilità dello strumento utilizzato con la medesima dotazione presente al momento della consegna. Qualsiasi dato, file, programma estraneo all'attività lavorativa che dovesse risultare installato o comunque presente sul PC, in violazione delle direttive di cui alla presente procedura, sarà immediatamente cancellato dall'Amministratore di sistema;
- Le postazioni di lavoro fisse e mobili non devono essere lasciate incustodite con le sessioni utenti attive. Quando un utente si allontana dalla propria postazione di lavoro e, comunque, in caso di non utilizzo del PC per oltre 10 minuti, si attiva la funzione automatica di blocco del computer. È buona norma, in ogni caso, procedere all'attivazione manuale del blocco della macchina digitando, i tasti "Crtl+ Alt + Canc" e selezionando l'opzione "Blocca";
- I dispositivi mobili utilizzati all'esterno e all'interno delle strutture dell'ente non devono mai essere lasciati incustoditi. In caso di furto o smarrimento è obbligatorio comunicare tempestivamente l'accaduto alla Direzione, effettuare denuncia presso l'ufficio di pubblica sicurezza locale e consegnare copia della stessa in Azienda;

Art. 10 – Trattamento dei dati in formato cartaceo

I documenti contenenti dati personali – soprattutto se particolari e/o giudiziari – non devono rimanere incustoditi su scrivanie o tavoli di lavoro.

Devono essere custoditi dai soggetti autorizzati in modo che non vi accedano persone prive di autorizzazione; in particolare, dovranno essere riposti in **armadi o cassetti chiusi** e non dovranno essere condivisi, comunicati o inviati a persone che non ne necessitano per lo svolgimento delle proprie mansioni lavorative.

I documenti contenenti dati personali che vengono prelevati dagli archivi per l'attività quotidiana devono esservi riposti a fine giornata.

Le copie dei documenti contenenti dati personali che risultino inutilizzate o mal riuscite, non devono essere utilizzate come carta da appunti o da riciclo e devono essere distrutte. Qualora sia necessario distruggere i documenti contenenti dati personali, questi devono essere eliminati utilizzando gli appositi apparecchi "**distruggi documenti**" o, in assenza, devono essere sminuzzati, in modo da non essere più ricomponibili.

Le misure di sicurezza applicate alle copie o alle riproduzioni dei documenti contenenti dati personali devono essere identiche a quelle applicate agli originali.

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.

Quando si scansionano documenti contenenti dati personali o informazioni riservate, è richiesta una particolare attenzione; ciò al fine di evitare che persone non autorizzate possano venire a conoscenza del contenuto della scansione. Occorre pertanto provvedere tempestivamente, al termine dell'utilizzo, alla cancellazione dei file esito delle **scansioni** dalle cartelle condivise.

CAPO III – GESTIONE DELLE COMUNICAZIONI TELEMATICHE

Art. 11 – Gestione utilizzo della rete internet

Le regole di seguito specificate sono adottate anche ai sensi delle "Linee guida del Garante per posta elettronica e internet" pubblicate in Gazzetta Ufficiale n. 58 del 10 marzo 2007 e relativi aggiornamenti.

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, va evitata la navigazione in siti non attinenti allo svolgimento delle proprie mansioni lavorative;
- È consentito l'utilizzo di soluzioni di chat esclusivamente per scopi professionali e attraverso strumenti e software messi a disposizione dall'ente, in particolare per dipendenti/collaboratori dotati di strumenti aziendali;
- L'utilizzo di strumenti e dispositivi personali da utilizzarsi per scopi professionali o per l'attività dell'Ente dovrebbe essere evitato e comunque, dove necessario, comunicato al referente privacy o alla Direzione;
- È vietato compiere azioni che siano potenzialmente in grado di arrecare danno alla società, ad esempio, il download o l'upload di file audio e/o video, l'uso di servizi di rete con finalità ludiche o, comunque, estranee all'attività lavorativa;
- È vietata ogni forma di registrazione a siti/APP i cui contenuti non siano legati all'attività lavorativa utilizzando le credenziali aziendali;
- 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;
- Va evitato, se non previsto dalla mansione, l'utilizzo di sistemi di social networking durante l'orario lavorativo, se non per motivi professionali mediante i dispositivi aziendali.

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.

Art. 12 – Gestione e utilizzo della posta elettronica aziendale

12.1 – Principi Guida

Per ciascun utente titolare di un account, l'ente provvede ad assegnare una casella di posta elettronica individuale. Ad uno stesso utente possono essere assegnate più caselle di posta elettronica, che possono anche essere condivise con altri utenti dello stesso gruppo/ufficio/dipartimento, questo per evitare che degli utenti singoli mantengano l'esclusività su dati.

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 lo svolgimento delle mansioni lavorative affidate.

L'organizzazione è consapevole della possibilità di un **limitato utilizzo personale** della posta elettronica da parte degli Incaricati.

Al fine di garantire una adeguata sicurezza dei sistemi informativi interni all'ente, qualora arrivino messaggi di posta con allegati file eseguibili e/o di natura incomprensibile o non conosciuta, è richiesto che il ricevente comunichi con il referente Sistemi Informativi per decidere in merito alle modalità di gestione e cancellazione.

Gli utenti sono responsabili del corretto utilizzo delle caselle di posta elettronica aziendale 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;
- Controllare i file allegati di posta elettronica prima del loro utilizzo. In particolare, si deve evitare, secondo le regole di buona diligenza, l'apertura e la lettura di messaggi di posta elettronica in arrivo provenienti da mittenti di cui non si conosce con certezza l'identità o che contengano allegati del tipo .exe, .com, .vbs, .htm, .scr, .bat, .js, .pif. È necessario porre molta attenzione, inoltre, alla credibilità del messaggio e del mittente per evitare casi di phishing o frodi informatiche. In qualunque situazione di incertezza contattare il referente Sistemi Informativi per una valutazione dei singoli casi;
- Nel caso di invio massivo di messaggi, mettere i destinatari in copia nascosta (Ccn);
- Come da decreto n°81 del 2023, non è consentito inviare o memorizzare messaggi (interni ed esterni) di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica, o che costituiscano comunque condotta illecita o che siano in qualunque modo fonte di responsabilità dell'ente;
- Come da decreto n°81 del 2023, l'utilizzo di account istituzionali è consentito per i soli fini connessi all'attività lavorativa o ad essa riconducibili e non può in alcun modo compromettere la sicurezza o la reputazione dell'ente. L'utilizzo di caselle di posta elettroniche personali è di norma evitato per attività o comunicazioni afferenti al servizio, salvi i casi di forza maggiore dovuti a circostanze in cui l'utente, per qualsiasi ragione, non possa accedere all'account istituzionale;
- L'utente è responsabile del contenuto dei messaggi inviati. I dipendenti/collaboratori si uniformano alle modalità di firma dei messaggi di posta elettronica di servizio individuate dall'ente di appartenenza. Ciascun messaggio in uscita deve consentire l'identificazione del dipendente/collaboratore mittente e deve indicare un recapito istituzionale al quale il medesimo è reperibile.

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 limitare l'invio per e-mail di informazioni personali.

A scopo di esempio può essere necessario inviare un nome e cognome di uno stagista all'azienda di riferimento ma non è corretto inviare per e-mail file Excel contenenti liste di studenti, contenuti massivi di dati personali o dati particolari/sensibili dove non espressamente autorizzati (es: le liste corsisti per le finalità di ricerca di lavoro sono già state preventivamente autorizzate dagli interessati all'atto dell'iscrizione).

Dove per finalità lavorative sia necessario inviare informazioni personali in liste, massive o dati particolari/sensibili, è consigliabile l'invio per e-mail tramite protezione dell'allegato con una password/pin comunicato al destinatario su altro canale (es: SMS, WhatsApp).

Occorre infine 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 da altri nell'organizzazione di appartenenza del mittente. Esempio:

NOME e COGNOME
FUNZIONE AZIENDALE
Riferimenti per contatti

Le informazioni contenute in questo messaggio di posta elettronica sono riservate e sono indirizzate esclusivamente al destinatario; non ne sono consentiti trattamenti diversi.
Qualora tale messaggio sia stato ricevuto per errore, si prega di avvisare il mittente e cancellare il messaggio dal proprio computer. Tutti i messaggi provenienti dal dominio formafuturo.it hanno natura esclusivamente aziendale con finalità lavorative e professionali e possono essere letti anche da persone diverse dal mittente/destinatario.
Relativamente al trattamento dei dati personali, qualora previsti, si informa che il titolare al trattamento dei dati della presente comunicazione è Forma Futuro nella figura del direttore. Informativa completa al trattamento dei dati personali è disponibile al seguente link: https://www.formafuturo.it/content/2-privacy

12.2 – Accesso alla casella di posta elettronica del lavoratore assente

Al fine di garantire la funzionalità del servizio di posta elettronica aziendale e di ridurre al minimo l'accesso ai dati, nel rispetto del principio di necessità e di proporzionalità, l'utente - **in caso di assenze programmate** (ad es. per ferie o attività di lavoro fuori sede) – dovrà impostare il **messaggio di risposta automatica "Fuori ufficio"**, indicando le coordinate di altro soggetto cui trasmettere le comunicazioni e-mail di contenuto lavorativo o altre utili modalità di contatto della struttura.

In caso di assenze non programmate, qualora l'ente necessiti di 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 sopra descritto all' Art.7.

12.3 – 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 in accordo con il punto precedentemente trattato Art. 8.3.

Dove sia necessario garantire un tempo più lungo rispetto a quanto indicato nel punto 8.3 del presente regolamento, è opportuno procedere nel seguente modo:

- Alla cessazione del dipendente/collaboratore si provvede ad eseguire il reset delle credenziali in

collaborazione con il referente Sistemi Informativi;

- Il referente Sistemi Informativi provvede ad attivare il **messaggio di risposta automatica che avvisa che il dipendente ha cessato l'attività ed i riferimenti del nuovo incaricato in sua sostituzione,** per il tempo che l'ente ritiene necessario;
- Il referente Sistemi Informativi provvede ad attivare **l'inoltro automatico della nuova posta** al referente incaricato in sua sostituzione, per il tempo che l'ente ritiene necessario;
- Terminato il tempo stabilito dall'Ente il referente Sistemi Informativi disporrà la definitiva e totale cancellazione della casella e-mail eventualmente effettuando un salvataggio o backup dei contenuti della casella e-mail.

Art. 13 – Gestione dei Social Media (Decreto n°81 nel 2023)

Nell'utilizzo dei propri account di social media, il dipendente/collaboratore utilizza ogni cautela affinché le proprie opinioni o i propri giudizi su eventi, cose o persone, non siano in alcun modo attribuibili direttamente all' amministrazione di appartenenza.

In ogni caso il dipendente/collaboratore è tenuto ad astenersi da qualsiasi intervento o commento che possa nuocere al prestigio, al decoro o all'immagine dell'amministrazione di appartenenza o della pubblica amministrazione in generale.

Al fine di garantirne i necessari profili di riservatezza, le comunicazioni afferenti direttamente o indirettamente il servizio non si svolgono, di norma, attraverso conversazioni pubbliche mediante l'utilizzo di piattaforme digitali o social media. Sono escluse da tale limitazione le attività o le comunicazioni per le quali l'utilizzo dei social media risponde ad una esigenza di carattere istituzionale.

Al momento Forma Futuro non ha definito una "social media policy" ma si riserva la possibilità di realizzarla in futuro.

Fermi restando i casi di divieto previsti dalla legge, i dipendenti/collaboratori non possono divulgare o diffondere per ragioni estranee al loro rapporto di lavoro con l'amministrazione e in difformità alle disposizioni di cui al decreto legislativo 13 marzo 2013, n. 33, e alla legge 7 agosto 1990, n. 241, documenti, anche istruttori, e informazioni di cui essi abbiano la disponibilità.

CAPO IV – SANZIONI, COMUNICAZIONI, APPROVAZIONE

Art. 14 – Sanzioni

La violazione di quanto previsto dal presente regolamento, rilevante anche ai sensi degli artt. 2104 e 2105 del Codice Civile, potrà comportare l'applicazione di sanzioni disciplinari in base a quanto previsto dal CCNL per la Formazione Professionale.

Art. 15 – Comunicazioni

Il presente regolamento è messo a disposizione degli utenti per la consultazione e viene consegnato a tutto il personale dell'ente con adeguata formazione ed informazione sull'intera procedura. Una volta approvata una nuova versione la stessa viene diffusa al personale interessato per e-mail.

Le richieste di autorizzazione o concessione previste dal presente regolamento possono essere inoltrate alla Direzione o al referente sistemi informativi tramite e-mail, a cui è riconosciuto il valore di forma scritta in modo del tutto analogo rispetto a quella cartacea.

ALLEGATI

- **ALLEGATO 01 - MODULO CONSEGNA ASSET AZIENDALI**