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

Tabella di revisione

Rev. n.	Data emissione	Descrizione delle modifiche	Approvazione
00	31 dicembre 2024	Prima adozione	Delibera n° 28 del 31 dicembre 2024
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).

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 solo per finalità di adempimento delle mansioni lavorative 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 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).
Tuttavia 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 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.

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 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, in collaborazione con il Responsabile Trattamento necessario per la gestione, l'aggiornamento, l'assistenza e la manutenzione dei sistemi informatici, 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 – Accesso ai dati

Tramite autorizzazione del Titolare del Trattamento, in persona dell'Amministratore Unico del Csl La Cremeria srl, l'Amministratore di Sistema ha la facoltà di accedere in qualunque momento ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica, al solo fine di garantire l'operatività, la sicurezza del sistema ed il normale svolgimento dell'attività aziendale nei casi in cui si renda indispensabile ed indifferibile l'intervento (ad esempio, in caso di improvvisa e/o prolungata assenza o impedimento dell'incaricato), informando tempestivamente l'incaricato dell'intervento di accesso realizzato.

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.

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, **l'ente si riserva la facoltà di accedere a qualsiasi dotazione o apparato assegnato in uso all'utente per mezzo dell'intervento di personale appositamente incaricato** (Responsabile Trattamento necessario per la gestione, l'aggiornamento, l'assistenza e la manutenzione dei sistemi oppure Amministratore di sistema).

8.2 – 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 al primo utilizzo la propria password procedendo allo stesso modo ogni **90 giorni**. La richiesta di cambio password viene segnalata dal Sistema. Ciascun utente dovrà procedere ad effettuare la variazione della password come da richiesta del sistema. In caso di impossibilità ad accedere al proprio account l'utente chiede all'Amministratore di Sistema l'azzeramento e la contestuale creazione di nuove credenziali di autenticazione dell'utente interessato, con avviso che al primo accesso alla risorsa, lo stesso dovrà inserire nuove credenziali.

comunicare al Responsabile Trattamento necessario per la gestione, l'aggiornamento, l'assistenza e la manutenzione dei sistemi informatici le nuove credenziali di autenticazione, secondo le indicazioni di cui all'art. 7 del presente Regolamento.

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

- La password deve essere composta da un minimo di **12 caratteri** e deve contenere almeno un carattere maiuscolo, un carattere minuscolo, un numero o un carattere non alfanumerico tipo "!@#$£$%...";
- 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 – Accesso all'Account del lavoratore assente

Nel caso in cui l'ente abbia la necessità di accedere ai dati o alle applicazioni presenti su una risorsa informatica assegnata ad un utente resosi assente per cause improvvise, non rintracciabilità o impedimento dello stesso, si procederà come segue:

- L'accesso alla risorsa informatica sarà effettuato per il tramite di **idoneo "fiduciario"**, da intendersi quale lavoratore previamente nominato e/o incaricato per iscritto dall'utente assente (Responsabile Trattamento necessario per la gestione, l'aggiornamento, l'assistenza e la manutenzione dei sistemi, oppure collega autorizzato al trattamento dei dati personali).

OPPURE

- Nel caso di mancata nomina di idoneo "fiduciario" o di assenza dello stesso, l'accesso sarà effettuato dall'**Amministratore di sistema** con credenziali di Amministratore oppure tramite l'azzeramento e la contestuale creazione di nuove credenziali di autenticazione dell'utente interessato, con avviso che al primo accesso alla risorsa, lo stesso dovrà inserire nuove credenziali.

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.

8.4 – 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 30 (trenta) giorni da quella data; entro 90 (novanta) giorni, invece, si disporrà la definitiva e totale cancellazione dell'account utente.

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 l'attività svolta. È dovere di ogni utente usare i computer e gli altri dispositivi a lui affidati responsabilmente e professionalmente;
- 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 all'Amministratore di sistema tramite **Ticket** 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;
- I dispositivi mobili utilizzati all'esterno (convegni, fiere, visite, ecc.), in caso di allontanamento, devono essere custoditi in un luogo protetto. In caso di allontanamento dell'utente, si prevede comunque una modalità di blocco dei dispositivi in caso di stand-by, dopo 1 minuto di inattività e l'abilitazione di sistemi di accesso ai dispositivi come password, impronte digitali, riconoscimento facciale, ecc… È buona norma, in ogni caso, procedere all'attivazione manuale del salvaschermo digitando, i tasti "Crtl+ Alt + Canc" e selezionando l'opzione "blocca computer". I dispositivi, comunque, non devono mai essere lasciati incustoditi nell'autovettura neppure nel bagagliaio. 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;

- Le postazioni di lavoro 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, con avvio del **salvaschermo protetto da password**. È buona norma, in ogni caso, procedere all'attivazione manuale del salvaschermo digitando, i tasti "Crtl+ Alt + Canc" e selezionando l'opzione "blocca computer";
- 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 aziendali, senza aver ottenuto esplicita autorizzazione da parte dell'ente.

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, nell'ipotesi di ricevimento di visitatori o terzi non autorizzati, i documenti eventualmente in utilizzo dovranno essere riposti in **armadi o cassetti chiusi** e non devono 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.

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.

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.

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;
- 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;
- 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;
- 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 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;
- Non è consentito l'utilizzo di sistemi di social networking sul luogo di lavoro o durante l'orario lavorativo, se non per motivi professionali;
- È altresì proibito rigorosamente qualsiasi uso del Web che non trasmetta un'immagine positiva o che possa essere in qualunque modo 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.

Nel caso in cui, per ragioni di servizio, si necessiti di una navigazione libera dai filtri, è necessario richiedere lo sblocco mediante una mail indirizzata all'Amministratore di Sistema, ed in copia alla Direzione, nella quale siano indicati chiaramente: motivo della richiesta, utente e postazione da cui effettuare la navigazione libera, intervallo di tempo richiesto per completare l'attività. Al termine dell'attività l'Amministratore di Sistema ripristinerà i filtri alla situazione iniziale.

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 e allo scopo prevede le seguenti misure:

1. In caso di ricezione, sulla e-mail aziendale (sia essa individuale o condivisa), di posta personale, cancellare immediatamente ogni messaggio al fine di evitare ogni eventuale e possibile back up dei dati.
2. Avvisare l'organizzazione quando sulla e-mail aziendale (sia essa individuale o condivisa), arrivino messaggi di posta personale con allegati file eseguibili e/o di natura incomprensibile o non conosciuta.

Attraverso le caselle e-mail aziendali 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 aziendale.

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;
- Utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario;
- 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 l'Amministratore di Sistema per una valutazione dei singoli casi;
- Nel caso fosse necessario inviare allegati "pesanti" (fino a 10MB), ricorrere prima alla compressione dei file originali in un archivio di formato .zip o equivalenti. Nel caso di allegati ancora più voluminosi rivolgersi all'Amministratore di Sistema;
- Nel caso di invio massivo di messaggi, mettere i destinatari in copia nascosta (Ccn).

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

Occorre 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: *Avvertenze e Informativa ai sensi dell'art. 13 del Regolamento (UE) 2016/679. Le informazioni contenute in questo messaggio di posta elettronica e/o files allegati, sono da considerarsi strettamente riservati. Il loro utilizzo è consentito esclusivamente al destinatario del messaggio o a persone dallo stesso autorizzate per le finalità indicate. Vi informiamo inoltre che questo messaggio è di carattere non personale, pertanto, sia lo stesso, che le eventuali risposte, potranno essere lette anche da altro personale all'interno dell'organizzazione aziendale mittente. Qualora riceveste questo messaggio senza esserne il destinatario Vi preghiamo cortesemente di darcene notizia via e-mail e di procedere alla distruzione del messaggio stesso, cancellandolo dal Vostro sistema. Gli interessati possono esercitare in qualunque momento il diritto di accesso, cancellazione, comunicazione, aggiornamento, rettificazione, opposizione al trattamento, integrazione, limitazione, portabilità e il diritto di porre reclamo all'autorità pubblica. Qualora desideraste ottenere copia dell'Informativa completa siete pregati di richiederla in risposta a questo messaggio oppure di consultarla sul sito www.csl-cremeria.it Grazie.*

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 segue:

- La verifica del contenuto dei messaggi sarà effettuato per il tramite di **idoneo "fiduciario"**, da intendersi quale lavoratore previamente nominato e/o incaricato per iscritto dall'utente assente (Amministratore di sistema oppure Responsabile Trattamento necessario per la gestione, l'aggiornamento, l'assistenza e la manutenzione dei sistemi oppure collega autorizzato al trattamento dei dati personali).

OPPURE

- Nel caso di mancata nomina di idoneo "fiduciario" o di assenza dello stesso, l'accesso sarà effettuato dall'**Amministratore di sistema** con credenziali di Amministratore oppure tramite l'azzeramento e la contestuale creazione di nuove credenziali di autenticazione dell'utente interessato, con avviso che al primo accesso alla posta elettronica, lo stesso dovrà inserire nuove credenziali.

In ogni caso, la verifica del contenuto dei messaggi avviene nel rispetto del **principio di necessità e non eccedenza** rispetto alle attività indifferibili per il quale è stata richiesta.

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 entro un periodo massimo di 30 (trenta) giorni da quella data ed entro 90 (novanta) giorni si disporrà la definitiva e totale cancellazione dello stesso. In ogni caso, l'ente si riserva il diritto di conservare i messaggi di posta elettronica ritenuti rilevanti per le proprie attività e al fine di tutelare un interesse legittimo del titolare del trattamento.

Durante tale periodo, verrà attivato il seguente servizio di risposta automatica: "*A breve questo indirizzo e-mail non sarà più attivo. Siete pregati di scrivere a ……..@csl-cremeria.it e di aggiornare le Vostre rubriche. Cordiali saluti".*

CAPO IV – SANZIONI, COMUNICAZIONI, APPROVAZIONE

Art. 13 – 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 dall'art. 56 del CCNL per la Formazione Professionale.

Art. 14 – 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 aziendali 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. 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. La versione più aggiornata dello stesso è pubblicata nella sezione Società trasparente del sito web istituzionale.

Per ogni aggiornamento del presente regolamento sarà data comunicazione 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 alla Direzione tramite e-mail, a cui è riconosciuto il valore di forma scritta in modo del tutto analogo rispetto a quella cartacea.

Art. 16 – Disposizioni finali

Il presente Regolamento entra in vigore con decorrenza dal 6 novembre 2024, a seguito di idonea formazione da parte del Responsabile della Protezione dei Dati (RPD).

ALLEGATI

- **ALLEGATO 01 - MODULO COMUNICAZIONE PASSWORD**
- **ALLEGATO 02 - MODULO CONSEGNA ASSET AZIENDALI**