Regolamento Gestione Sistema Informatico

Informativa Accesso

Febbraio 2025

1. PRINCIPI GENERALI

Il presente documento ha l'obiettivo di regolamentare l'utilizzo di internet e posta elettronica per gli utenti di tali servizi nell'ambito della struttura aziendale della SAN LIDANO COOPERATIVA.

Le presenti regole di sicurezza hanno valenza per l'Azienda si pongono l'obiettivo di fornire agli utenti idonee misure di sicurezza e linee di comportamento adeguate per utilizzare in modo conforme e non rischioso la posta elettronica aziendale e la navigazione in internet.

Il Regolamento è adottato in conformità al Provvedimento del Garante per la tutela dei dati personali del 1° marzo 2007.

A tal proposito, allo scopo di rappresentare agli utenti il quadro normativo di riferimento si specifica che le principali fonti normative in materia sono le seguenti:

- Decreto Legislativo n.196 del 30/06/2003 c.d. Codice della Privacy (di seguito "Codice") come novellato dal D.lgs. 101/2018;
- REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI Regolamento UE (GDPR) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 (di seguito " Regolamento ");
- Provvedimento del "Garante della Privacy" n. 13 del 01/03/2007 – Linee Guida del Garante per posta elettronica e internet;
- Provvedimento del Garante della Privacy nr. 364 del 6 giugno 2024 – Documento di indirizzo. Programmi e servizi informatici di gestione della posta elettronica nel contesto lavorativo e trattamento dei metadati;

Copia del presente Regolamento viene pubblicata sul sito internet aziendale nella sezione "Privacy Policy" e consegnata a ciascun dipendente. L'inosservanza delle norme sulla privacy può comportare sanzioni di natura civile e penale per l'Autorizzato e per l'Azienda per cui si raccomanda di prestare la massima attenzione nella lettura delle disposizioni di seguito riportate.

2. CAMPO DI APPLICAZIONE

Le presenti Istruzioni si applicano:

• a tutti i Lavoratori dipendenti e a tutti i Collaboratori di SAN LIDANO COOPERATIVA a prescindere dal rapporto contrattuale con la stessa intrattenuto (lavoratori somministrati, collaboratori a progetto, agenti, stagisti, consulenti, ecc.) che si trovano ad operare sui dati personali di cui SAN LIDANO COOPERATIVA stessa è Titolare (di seguito "**Utenti**");

• a tutte le attività o comportamenti comunque connessi all'utilizzo della rete Internet e della posta elettronica, mediante strumentazione aziendale o di terze parti autorizzate all'uso dell'infrastruttura aziendale.

3. RIFERIMENTI NORMATIVI E DEFINIZIONI

Gli Autorizzati sono le persone fisiche autorizzate a compiere le operazioni di trattamento dal Titolare o dal Responsabile. In particolare, le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del Titolare o del Responsabile, attenendosi alle istruzioni impartite.

La designazione è effettuata per iscritto e individua puntualmente l'ambito del trattamento consentito.

Si evidenzia preliminarmente che, ai fini del presente Regolamento:

• con il termine "**Trattamento**" ci si riferisce ad una qualunque operazione effettuata sui dati, svolta con o senza l'ausilio di mezzi automatizzati, che abbia come oggetto la raccolta, la registrazione, la consultazione, l'elaborazione, la modifica, la diffusione, l'estrazione, la distruzione di dati, anche se non registrati in una banca dati; il trattamento comprende l'intera vita del dato personale, dal momento della raccolta a quello della distruzione, abbracciando operazioni di utilizzo interno (organizzazione, conservazione, raffronto, ecc.) ed esterno (comunicazione, diffusione, interconnessione ad altre banche dati), e prescindendo sia dall'eventuale uso di strumenti informatici, sia dalla circostanza che il dato venga divulgato o elaborato nel senso stretto del termine; di conseguenza, si parla di trattamento sia nel caso in cui vengano utilizzati mezzi elettronici o comunque automatizzati, sia altri mezzi che richiedono l'esclusivo apporto umano;

• con il termine "**Dato Personale**" si fa riferimento a qualunque informazione relativa a persona fisica e giuridica, ente o associazione, siano esse informazioni nominative (come le generalità di una persona), o una qualunque altra informazione che possa rendere identificabile l'interessato, anche indirettamente (ad esempio codice fiscale, numero di matricola del Dipendente);

• con il termine "**Dato Particolare (anche indicato come Sensibile)**" si fa riferimento ai dati idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale nonché i dati personali idonei a rivelare lo stato di salute dell'interessato;

• con il termine "**Dato Giudiziario**" si fa riferimento ai dati idonei a rivelare i provvedimenti in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reati e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli artt. 60 e 61 del Codice di procedura penale.

4. LINEE GUIDA

Di seguito vengono descritte le norme a cui gli Incaricati devono attenersi nell'esecuzione dei compiti che implicano un trattamento di dati personali riferiti sia a persone fisiche che giuridiche.

Preliminarmente va evidenziato che, al fine di evitare che soggetti estranei possano venire a conoscenza dei dati personali oggetto del trattamento, l'Autorizzato **deve** osservare le seguenti regole di ordinaria diligenza, nonché tutte le altre ulteriori misure ritenute necessarie per garantire il rispetto di quanto disposto dalla normativa in ambito privacy:

• tutte le operazioni di trattamento devono essere effettuate in modo tale da garantire il rispetto delle misure di sicurezza, la massima riservatezza delle informazioni di cui si viene in possesso considerando tutti i dati confidenziali e, di norma, soggetti al segreto d'ufficio;

• le singole fasi di lavoro e la condotta da osservare devono consentire di evitare che i dati siano soggetti a rischi di perdita o distruzione, che vi possano accedere persone non autorizzate, che vengano svolte operazioni di trattamento non consentite o non conformi ai fini per i quali i dati stessi sono stati raccolti;

• in caso di allontanamento, anche temporaneo, dalla propria postazione di lavoro si devono porre in essere tutte le misure necessarie (es. blocco del pc) affinché soggetti terzi, anche se dipendenti, non possano accedere ai dati personali per i quali era in corso un qualunque tipo di trattamento, sia esso cartaceo che automatizzato;

• non devono essere eseguite operazioni di trattamento per fini non previsti tra i compiti assegnati dal diretto responsabile;

• devono essere svolte le sole operazioni di trattamento necessarie per il raggiungimento dei fini per i quali i dati sono stati raccolti;

• deve essere costantemente verificata l'esattezza dei dati trattati e la pertinenza rispetto alle finalità perseguite nei singoli casi. Quanto descritto impone, quindi, di operare con la massima attenzione in tutte le fasi di trattamento, dalla esatta acquisizione dei dati, al loro aggiornamento, alla conservazione ed eventuale distruzione. Nei successivi paragrafi si riportano le norme che gli Autorizzati devono adottare sia che trattino dati in formato elettronico che cartaceo.

4.1 Accesso ai dati dalla postazione di lavoro

La postazione di lavoro **deve** essere:

i) utilizzata solo per scopi legati alla propria attività lavorativa;

ii) utilizzata in modo esclusivo da un solo utente;

iii) protetta, evitando che terzi possano accedere ai dati che si sta trattando. Occorre, inoltre, precisare che è dovere dell'Autorizzato:

iv) non utilizzare in Azienda risorse informatiche private (PC, periferiche, token, hard disk, ecc.);

v) non installare alcun software;

vi) non utilizzare i device aziendali (siano essi fissi o portatili) su reti esterne o su wi-fi non espressamente autorizzati o verificati dalla SAN LIDANO COOPERATIVA;

vii) non lasciare sulla scrivania informazioni riservate su qualunque supporto esse siano archiviate (carta, CD, dischetti, ecc.);

viii) richiamare le funzioni di sicurezza del sistema operativo (con la sequenza dei tasti CTRL+ALT+CANC) ed assicurarsi della attivazione della funzione Lock Workstation in caso di abbandono momentaneo del proprio PC o, in alternativa, impostare lo screen saver con password in modo che si attivi dopo max.5 minuti di inattività;

ix) non lasciare il computer portatile incustodito sul posto di lavoro (al termine dell'orario lavorativo, durante le pause di lavoro, o durante riunioni lontane dalla propria postazione);

x) non lasciare incustoditi cellulari e palmari;

xi) non utilizzare telefono od altri strumenti informatici per trasmettere informazioni riservate e personali se non si è assolutamente certi dell'identità dell'interlocutore o del destinatario e se esso non è legittimato a riceverle.

4.2 Gestione delle password

Per una corretta gestione delle password, ciascun Autorizzato **deve** aver cura di:

• modificare, alla prima connessione, quella che l'IT ha attribuito di default;

• cambiarla almeno ogni 90 giorni, o immediatamente nei casi in cui sia compromessa o venga richiesto dall'IT;

• comporla utilizzando almeno 8 caratteri o, nel caso in cui lo strumento elettronico non lo consenta, con un numero di caratteri pari al massimo consentito;

• usare sia lettere che numeri e almeno un carattere maiuscolo;

• non basare la scelta su informazioni facilmente deducibili quali, ad esempio, il proprio nome, il nome dei propri familiari, le date di nascita, i codici fiscali, ecc.,

• mantenerla riservata e non divulgarla a terzi;

• non permettere ad altri utenti (es. colleghi) di operare con il proprio identificativo utente;

• non trascriverla su supporti (es. fogli, post-it) facilmente accessibili a terzi;

• non comunicarla mai per telefono salvo gravi necessità.

4.3 Antivirus

I Personal Computer (PC) in dotazione agli utenti, pur protetti contro gli attacchi dei virus informatici mediante appositi programmi, rimangono potenzialmente esposti ad aggressioni di virus non conosciuti. Per ridurre le probabilità del verificarsi di tali attacchi è necessario che **vengano osservate** le seguenti regole:

• controllare che il programma antivirus installato sia aggiornato periodicamente e sia attivo;

• chiudere correttamente i programmi in uso;

• non aprire, se si lavora in rete, files sospetti e di dubbia provenienza;

• non scaricare o installare applicazioni/software che non siano state preventivamente approvate e autorizzate;

• verificare con l'ausilio del programma antivirus in dotazione ogni supporto magnetico contenente dati, prima dell'esecuzione dei file in esso contenuti;

• non utilizzare altri supporti elettronici di provenienza incerta e comunque non di proprietà aziendale;

• porre la necessaria attenzione sui risultati delle elaborazioni effettuate e sulle eventuali segnalazioni anomale inviate dal PC;

• usare correttamente e solo per esigenze di lavoro i servizi di posta elettronica e di Internet;

• non modificare le configurazioni impostate sul proprio PC;

• spegnere il PC al termine della giornata di lavoro.

Alla verifica di un malfunzionamento del PC, che può far sospettare la presenza di virus, o di altre applicazioni nocive l'Autorizzato **deve**: a. sospendere ogni operazione sul PC evitando di lavorare con il sistema infetto;

b. contattare immediatamente l'Area IT;

c. chiudere il sistema e le relative applicazioni.

4.4 Salvataggio dei dati

Tutti i dati al termine della giornata lavorativa vanno salvati sul server aziendale.

A tale riguardo, qualora vi sia la necessità, l'Autorizzato può richiedere all'Area IT la creazione sul server di una cartella a lui intestata o, in alternativa, di una cartella condivisa dal gruppo di lavoro cui fa riferimento l'Autorizzato stesso.

4.5 Protezione dei PC portatili

Un computer portatile presenta maggiori vulnerabilità rispetto ad una postazione di lavoro fissa. Fatte salve tutte le disposizioni dei paragrafi precedenti, di seguito vengono illustrate le ulteriori precauzioni **da adottare** nell'uso dei dispositivi portatili:

• conservare lo strumento in un luogo sicuro alla fine della giornata lavorativa;

• non lasciare mai incustodito l'elaboratore in caso di utilizzo in ambito esterno all'azienda;

• avvertire tempestivamente l'Area IT ed il proprio Referente interno per la gestione della Privacy, che darà le opportune indicazioni, in caso di furto di un PC portatile;

• essere sempre ben consapevole delle informazioni archiviate sul portatile il quale è maggiormente soggetto a furto e smarrimento rispetto alla postazione fissa;

• operare sempre nella massima riservatezza quando si utilizza il PC portatile in pubblico: i dati, ed in particolare le password, potrebbero essere intercettati da osservatori indiscreti.

4.6 Internet e posta elettronica

Gli strumenti di comunicazione telematica (Internet e Posta elettronica) **devono** essere utilizzati solo ed esclusivamente per finalità lavorative. Sono **vietati**

comportamenti che possano arrecare danno all'Azienda. In particolare, l'**Utente dovrà osservare** le seguenti regole:

• è consentita la navigazione internet solo in siti attinenti e necessari per lo svolgimento delle mansioni assegnate;

• non è consentito scaricare software gratuiti (freeware o shareware) prelevati da siti Internet;

• non è consentita la registrazione a siti internet o partecipare a Forum di discussione se questo non è strettamente necessario per lo svolgimento della propria attività lavorativa;

• non è consentito l'utilizzo funzioni di instant messaging a meno che autorizzate dall'Area IT;

• è vietato aprire e-mail e file allegati di origine sconosciuta o che presentino degli aspetti anomali (quali ad esempio, un soggetto non chiaro);

• non è consentito rispondere a messaggi provenienti da un mittente sconosciuto o di dubbio contenuto in quanto tale atto assicura al mittente l'esistenza del destinatario;

• è vietato l'utilizzo della posta elettronica per comunicare informazioni riservate, dati personali o dati critici, senza garantirne l'opportuna protezione. Le mail personali aziendali possono essere utilizzate per soli fini aziendali e sono vietati utilizzi a fini privati;

• occorre sempre accertarsi che i destinatari della corrispondenza per posta elettronica siano autorizzati ad entrare in possesso dei dati che ci si appresta ad inviare;

• occorre sempre essere consapevoli che posta elettronica e navigazione internet sono veicoli per l'introduzione sulla propria macchina (e quindi in azienda) di virus e altri elementi potenzialmente dannosi;

• è consentito solo l'utilizzo dei programmi ufficialmente installati dall'Area IT;

• è vietato installare autonomamente programmi, sussistendo infatti il grave pericolo di introdurre virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti, di violare la legge sul diritto d'autore non disponendo delle apposite licenze d'uso acquistate dalla SAN LIDANO COOPERATIVA;

• è vietato modificare le caratteristiche impostate sulle dotazioni o installare dispositive di memorizzazione, comunicazione o altro (ad esempio masterizzatori, modem, wi-fi o connect card), collegare alla rete aziendale qualsiasi apparecchiatura (ad es. switch, hub, apparati di memorizzazione di rete, ecc), effettuare collegamenti verso l'esterno di qualsiasi tipo (ad es. tramite modem o connect card ecc.) utilizzando un pc che sia contemporaneamente collegato alla rete aziendale (creando così un collegamento tra la rete aziendale interna e la rete esterna);

• al fine di ottimizzare le risorse a disposizione della posta elettronica aziendale e migliorare le prestazioni del sistema si evidenzia che la casella di posta deve essere "tenuta in ordine" cancellando periodicamente o comunque se sono superati i limiti di spazio concessi, documenti inutili o allegati ingombranti;

• è vietato l'utilizzo dei supporti di origine esterna (per es. chiavi USB, dischi esterni, ecc.), avvertendo immediatamente l'Amministratore di sistema nel caso in cui siano rilevati virus.

L'**Utente**, in caso di assenza programmata (ad esempio per ferie o attività di lavoro fuori sede) - di almeno 5 giornate lavorative - deve attivare l'apposita funzionalità di sistema (cd. "*Fuori Sede*") che consente di inviare automaticamente ai mittenti un messaggio di risposta contenente le "coordinate" (anche elettroniche o telefoniche) di un altro utente o altre modalità utili di contatto della struttura.

SAN LIDANO COOPERATIVA, in caso di assenza improvvisa o prolungata dell'**Utente** o comunque non programmata e per improrogabili necessità di sicurezza o di operatività del sistema, si riserva, per mezzo dell'Amministratore di Sistema e Responsabile sistemi ICT, di accedere alla casella di posta elettronica dell'utente assente: per i dettagli si rimanda al paragrafo 5 "*Accesso ai dati dell'Utente*".

4.6.1 Particolari cautele nella predisposizione dei messaggi di posta elettronica

Nell'utilizzo della posta elettronica ciascun **Utente** deve tenere in debito conto che i soggetti esterni possono attribuire carattere istituzionale alla corrispondenza ricevuta da dipendenti aziendali. Pertanto si deve prestare particolare attenzione agli eventuali impegni contrattuali e precontrattuali contenuti nei messaggi.

La formulazione dei messaggi **deve** pertanto far uso di un linguaggio appropriato, corretto e rispettoso che tuteli la dignità delle persone, l'immagine e la reputazione di SAN LIDANO COOPERATIVA.

SAN LIDANO COOPERATIVA determina e pone, inoltre, le seguenti regole di comportamento a cui gli **Utenti devono** attenersi:

a) conservare le comunicazioni inviate o ricevute, in particolare quelle dalle quali si possano desumere impegni e/o indicazioni operative provenienti dalla Committenza pubblica;

b) prestare attenzione ai messaggi di posta elettronica ed ai file, programmi e oggetti allegati, ricevuti da mittenti sconosciuti, con testo del messaggio non comprensibile o comunque avulso dal proprio contesto lavorativo.

In tali casi gli **Utenti devono** in particolare:

• visualizzare preventivamente il contenuto tramite utilizzo della funzione "*Riquadro di lettura*" (o preview) e, nel caso si riscontri un contenuto sospetto, non aprire il messaggio,

• una volta aperto il messaggio, evitare di aprire gli allegati o cliccare sui "*link*" eventualmente presenti,

• cancellare il messaggio e svuotare il "*cestino*" della posta,

• segnalare l'accaduto all'Amministratore di Sistema ed **evitare** di cliccare sui collegamenti ipertestuali dubbi presenti nei messaggi di posta: in caso di necessità, accedere ai siti segnalati digitando il nome del sito da visitare direttamente nella barra degli indirizzi nei consueti strumenti di navigazione; in caso di iscrizione a servizi informativi accessibili via internet ovvero a servizi di editoria on line, veicolati attraverso lo strumento di posta elettronica:

• adoperare estrema cautela ed essere selettivi nella scelta della Società che fornisce il servizio; in particolare l'adesione dovrà avvenire in funzione dell'attinenza del servizio con la propria attività lavorativa,

• utilizzare il servizio solo per acquisire informazioni inerenti finalità aziendali, facendo attenzione alle informazioni fornite a terzi in modo da prevenire attacchi di social engineering,

• in caso di appesantimento dovuto ad un eccessivo traffico di messaggi scambiati attraverso la lista di distribuzione, revocare l'adesione alla stessa.

Si **raccomanda**, in proposito, di approfondire al momento dell'iscrizione le modalità per richiederne la revoca.

Salvo sia strettamente necessario per finalità lavorative, evitare del tutto l'inserimento di dati particolari o sensibili nell'oggetto delle comunicazioni e/o evitare di inserire dati personali nell'oggetto e nel testo delle comunicazioni elettroniche, privilegiando, ove possibile, termini neutri o generali di pari efficacia.

In caso di errore nella spedizione o ricezione, contattare rispettivamente il destinatario cui è stata trasmessa per errore la comunicazione o il mittente che, per

errore, l'ha spedita, eliminando quanto ricevuto (compresi allegati) senza effettuare copia. Ove dalla propria spedizione possa determinarsi un potenziale caso di Data Breach, cioè una perdita di confidenzialità di dati personali della SAN LIDANO COOPERATIVA in quanto contenuti o allegati alla e.mail erroneamente spedita, l'**Utente deve** immediatamente informare il proprio Referente interno per la gestione della Privacy, in modo da consentire di valutare i provvedimenti più tempestivi ed opportuni;

evitare di predisporre messaggi che contengano materiali che violino la legge sul diritto d'autore, o altri diritti di proprietà intellettuale o industriale.

4.7 Trasmissione e riproduzione dei documenti

i) Al fine di prevenire eventuali accessi ai dati aziendali da parte di soggetti terzi non autorizzati, occorre adottare delle cautele nella trasmissione e riproduzione dei documenti contenenti dati personali. Quando le informazioni devono essere trasmesse telefonicamente occorre essere assolutamente certi dell'identità dell'interlocutore e verificare che esso sia legittimato ad ottenere quanto domandato. In particolare, nel caso di richieste da parte di terzi **può essere necessario**, a seconda della natura dei dati richiesti, procedere nel seguente modo:

• chiedere il nome del chiamante e la motivazione della richiesta;

• richiedere il numero di telefono da cui l'interlocutore sta effettuando la chiamata;

• verificare che il numero dichiarato corrisponda a quello del chiamante;

• procedere immediatamente a richiamare la persona che ha richiesto l'informazione, con ciò accertandosi della identità dichiarata in precedenza.

ii) Quando il dato deve essere inviato posta elettronica, SMS, ecc. e, in particolar modo, nel caso in cui vengano inviati documenti contenenti dati sensibili **occorre**:

• prestare la massima attenzione affinché il numero telefonico o l'indirizzo e-mail immessi siano corretti.

iii) Nel caso di documenti inviati per posta elettronica accertarsi, prima di confermare l'invio, di avere allegato il file giusto.

iv) In caso di trasmissione di dati particolarmente delicati è opportuno anticipare l'invio chiamando il destinatario della comunicazione al fine di assicurare il ricevimento nelle mani del medesimo, evitando che terzi estranei o non autorizzati conoscano il contenuto della documentazione inviata.

v) Non utilizzare per la trasmissione programmi o applicazioni non espressamente autorizzati dalla SAN LIDANO COOPERATIVA o tramite account aventi carattere personale.

Tutti coloro che provvedono alla duplicazione di documenti con stampanti, macchine fotocopiatrici o altre apparecchiature, in caso di copia erronea o non leggibile correttamente, da cui potrebbero essere desunti dati personali, sono tenuti a distruggere il documento con qualunque mezzo/modalità che ne renda impossibile la ricostruzione in modo da escludere qualunque possibilità da parte di estranei di venire a conoscenza dei dati medesimi.

4.8 Archivi Cartacei

Tutto il materiale cartaceo contenente dati personali non deve essere lasciato incustodito sulle scrivanie e, a fine lavoro, deve essere riposto in un luogo sicuro.

Inoltre, occorre usare la medesima perizia nello svolgimento delle normali quotidiane operazioni di lavoro, per evitare che il materiale risulti facilmente visibile a persone terze o, comunque, ai non autorizzati al trattamento. In caso di trattamento di dati particolarmente sensibili (condizione di salute, dati giudiziari, ecc.), tutta la documentazione cartacea deve essere conservata in armadi/cassetti chiusi a chiave o stanze chiuse a chiave in caso di allontanamento, anche temporaneo, dalla postazione di lavoro.

L'accesso a tutti i locali aziendali deve essere consentito solo a personale preventivamente autorizzato da SAN LIDANO COOPERATIVA, attraverso i propri rappresentanti apicali.

5. ACCESSO AI DATI DELL'UTENTE

L'Amministratore di Sistema IT **può accedere** ai dati trattati dall'**Utente** tramite posta elettronica o navigazione in rete esclusivamente per motivi di sicurezza e protezione del sistema informatico (ad es., contrasto virus, malware, intrusioni telematiche, fenomeni quali spamming, phishing, spyware, etc.), ovvero per motivi tecnici e/o manutentivi e/o di regolare svolgimento dell'attività lavorativa (ad esempio, aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware), ovvero, infine, per motivi/esigenze disciplinari.

Fatta eccezione per gli interventi urgenti che si rendano necessari per affrontare situazioni di emergenza e massima sicurezza, il personale incaricato accederà ai dati su richiesta dell'**Utente** e/o previo avviso al medesimo. Ove sia necessario per garantire la sicurezza, l'assistenza tecnica e la normale attività operativa, il personale Autorizzato avrà anche la facoltà di collegarsi e visualizzare in remoto il desktop delle singole postazioni.

Lo stesso Amministratore di Sistema può, nei casi suindicati, procedere a tutte le operazioni di configurazione e gestione necessarie a garantire la corretta funzionalità del sistema informatico aziendale (ad es. rimozione di file o applicazioni pericolosi).

L'Amministratore di Sistema, in caso di assenza improvvisa o prolungata dell'**Utente** o comunque non programmata e per improrogabili necessità di sicurezza o di operatività del sistema è abilitato ad accedere alla posta elettronica dell'**Utente** per le necessità operative.

Di tale avvenuto accesso sarà data tempestiva comunicazione all'**Utente**.

L'Amministratore di Sistema può procedere a controlli sulla navigazione finalizzati a garantire l'operatività e la sicurezza del sistema, nonché il necessario svolgimento delle attività lavorative, es. mediante un sistema di controllo dei contenuti (Proxy server) o mediante "*file di log*" della navigazione svolta.

L'eventuale controllo sui file di log da parte dell'Amministratore di Sistema non è comunque continuativo e concerne alcune informazioni (es. Posta elettronica: l'indirizzo del mittente e del destinatario, la data e l'ora dell'invio e della ricezione e l'oggetto – Navigazione internet: il nome dell'**Utente**, l'identificativo della postazione di lavoro, indirizzo IP, la data e ora di navigazione, il sito visitato e il totale degli accessi effettuati) ed i file stessi vengono conservati per il periodo strettamente necessario per il perseguimento delle finalità organizzative, produttive e di sicurezza dell'azienda, e comunque non oltre 12 mesi, fatti salvi in ogni caso specifici obblighi di legge. Il sistema di registrazione dei log è configurato per cancellare periodicamente ed automaticamente (attraverso procedure di sovraregistrazione) i dati personali degli utenti relativi agli accessi internet e al traffico telematico.

L'Amministratore di Sistema è altresì abilitato ad accedere ai dati contenuti negli strumenti informatici restituiti dall'**Utente** a SAN LIDANO COOPERATIVA per cessazione del rapporto, sostituzione delle apparecchiature, etc. Sarà cura dell'**Utente** la cancellazione preventiva di tutti i soli eventuali dati personali eventualmente ivi contenuti.

SAN LIDANO COOPERATIVA garantisce la non effettuazione di alcun trattamento mediante sistemi hardware e software specificatamente preordinati al controllo a distanza, quali, a titolo esemplificativo:

- lettura e registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori (log) al di là di quanto tecnicamente necessario per svolgere il servizio e-mail, nel rispetto del Provvedimento;

• riproduzione ed eventuale memorizzazione sistematica delle pagine web visualizzate dal lavoratore;

• lettura e registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo.

6. CONTROLLI DA PARTE DELLA TITOLARITÀ

Con il presente capitolo si informa e si porta all'attenzione di ogni Dipendente e/o Autorizzato la possibilità/facoltà di SAN LIDANO COOPERATIVA di effettuare controlli sulle proprie apparecchiature tecnologiche al fine di preservare la sicurezza informatica dei dati personali in esse contenuti.

A tale proposito si sottolinea che la strumentazione tecnologica/informatica e quanto con essa creato è di proprietà di SAN LIDANO COOPERATIVA in quanto mezzo/strumento di lavoro ed inerente al corretto andamento della organizzazione aziendale.

E' pertanto fatto divieto di utilizzo del mezzo tecnologico/informatico e delle trasmissioni interne ed esterne con esso effettuate per fini ed interessi non coincidenti con quelli di cui SAN LIDANO COOPERATIVA è titolare e/o anche solo portatrice. Nel rispetto dei principi di pertinenza e non eccedenza, le verifiche sugli strumenti informatici saranno posti in essere da SAN LIDANO COOPERATIVA nel pieno rispetto dei diritti e delle libertà fondamentali degli **Utenti** e del presente Regolamento.

In caso di anomalie, SAN LIDANO COOPERATIVA per quanto possibile, privilegerà preliminari controlli anonimi e quindi riferiti a dati aggregati nell'ambito di intere strutture lavorative o di sue aree nelle quali si è verificata l'anomalia.

In tali casi, il controllo si concluderà con un avviso al Responsabile della struttura dell'Area aziendale interessata in cui è stato rilevato l'utilizzo anomalo degli strumenti aziendali affinché lo stesso inviti le strutture da lui dipendenti ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite.

In caso di successive, perduranti anomalie, ovvero ravvisandone comunque la necessità, SAN LIDANO COOPERATIVA si riserva di effettuare verifiche anche su base individuale, comunque finalizzate esclusivamente alla individuazione di eventuali condotte illecite.

In nessun caso verranno realizzate verifiche prolungate, costanti o indiscriminate, fatte salve le verifiche atte a tutelare gli interessi aziendali.

Fermo restando quanto sopra previsto in materia di utilizzo della Rete internet aziendale, durante lo svolgimento della prestazione lavorativa, non è consentito in alcun modo l'accesso e l'uso di social network, app, giochi o altre attività " virtuali " di intrattenimento, anche mediante dispositivi personali.

7. RESPONSABILITÀ E SANZIONI

L'**Utente**, al fine di non esporre sé stesso e SAN LIDANO COOPERATIVA a rischi sanzionatori, è tenuto ad adottare comportamenti puntualmente conformi alla normativa vigente ed alla regolamentazione aziendale.

L'**Utente** **è responsabile** del corretto utilizzo dei servizi di Internet e Posta Elettronica. Pertanto sarà responsabile per i danni cagionati al patrimonio, alla reputazione e alla Committenza. Tutti gli **Utenti** sono pertanto **tenuti ad osservare e a far osservare** le disposizioni contenute nel presente Regolamento il cui mancato rispetto o la cui violazione, costituendo inadempimento contrattuale potrà comportare:

• per il personale Dipendente oltre che l'adozione di provvedimenti di natura disciplinare previsti dal Contratto Collettivo Nazionale di Lavoro tempo per tempo vigente, le azioni civili e penali stabilite dalle leggi tempo per tempo vigenti;

• per i Collaboratori esterni oltre che la risoluzione del contratto le azioni civili e penali stabilite dalle leggi tempo per tempo vigenti.

Il presente Documento è stato predisposto dal Responsabile per il Trattamento dei dati ed approvato dal Consiglio di Amministrazione di SAN LIDANO COOPERATIVA.