Regolamento per l'utilizzo dei sistemi, strumenti informatici e archivi cartacei

Il presente regolamento è stato redatto tenendo conto delle linee guida del Garante della Privacy emanate con delibera n. 13 del 1° marzo 2007.
Lo stesso documento assolve anche agli obblighi informativi, ai sensi del D.lgs.101/2018 e Reg. EU 679/2016 (GDPR), sia, eventualmente, ai sensi dell'art. 4 - 3°comma dello Statuto dei lavoratori.

Regolamento per l'utilizzo dei sistemi, strumenti informatici e archivi cartacei della SOCIETA' COOPERATIVA SOCIALE INTERACTIVE

Indice

Premessa

La Società Cooperativa Sociale Interactive (di seguito "Titolare") ha disposto che al proprio interno venga osservata la presente Policy aziendale per l'utilizzo di sistemi e strumenti informatici ed archivi cartacei.

La progressiva diffusione delle nuove tecnologie informatiche e, in particolare, il libero accesso alla rete Internet da Personal Computer, tablet e smartphone, espone i dati personali del Titolare, dei lavoratori (soci lavoratori, dipendenti, collaboratori della stessa, etc.) e dell'utenza dei servizi svolti dal Titolare, a rischi di violazioni rilevanti rispetto alla normativa "privacy", oltre che ad eventuali responsabilità del Titolare di natura civile e/o penale.

Premesso quindi che l'utilizzo delle risorse informatiche e telematiche deve sempre ispirarsi al principio della ***diligenza e correttezza***, comportamenti che normalmente si adottano nell'ambito dei rapporti di lavoro, il Titolare ha adottato un Regolamento interno diretto ad evitare che comportamenti anche inconsapevoli possano innescare problemi o minacce alla sicurezza nel trattamento dei dati e quindi del proprio sistema informatico. Il Regolamento svolge anche la funzione di informare compiutamente gli utenti sugli specifici trattamenti dei loro dati personali che sono effettuati, e delle modalità adottate.

Le prescrizioni di seguito previste si aggiungono ed integrano le specifiche istruzioni già fornite a tutti gli addetti in attuazione del D.lgs. 30 giugno 2003 n. 196 e del D.lgs.101/2018 e Reg. EU 679/2016 (GDPR), anche in ordine alle ragioni e alle modalità dei possibili controlli o alle conseguenze di tipo disciplinare in caso di violazione delle stesse, come previsto dall'art. 4-3°comma dello Statuto dei lavoratori.

1. Entrata in vigore del Regolamento e pubblicità

Il nuovo Regolamento entrerà in vigore il 30.05.2025. Con l'entrata in vigore del presente Regolamento tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi abrogate, qualora incompatibili o difformi, poiché sostituite dalle presenti.
Copia del Regolamento, oltre ad essere affisso nelle bacheche aziendali e disponibile in una cartella informatica di ogni server delle Comunità anche per quanto prevede l'art.7 della Legge n. 300/1970, sarà reso disponibile e spiegato a ciascun lavoratore al momento dell'assunzione, anche ai fini del D.lgs. 101/2018 e Reg. EU 679/2016 (GDPR) e dell'art.4, comma 3°, dello Statuto dei lavoratori, oltre che a collaboratori, consulenti, od altri incaricati esterni, al momento della sottoscrizione del contratto, che venissero autorizzati a far uso di strumenti tecnologici del Titolare o ad accedere alla rete informatica aziendale e ad eventuali dati ed informazioni ivi conservati e trattati. Pertanto, il presente regolamento entra a far parte, per quanto occorra, del Codice disciplinare aziendale.

2. Campo di applicazione del Regolamento

2.1 Il nuovo Regolamento si applica a tutti i lavoratori, senza distinzione di ruolo e/o livello, nonché a tutti i collaboratori e consulenti dell'azienda a prescindere dal rapporto contrattuale con la stessa intrattenuto (lavoratori somministrati, collaboratori coordinati e continuativi, in stage/tirocini, agenti di commercio, prestatori d'opera intellettuale, etc.) che venissero autorizzati a far uso di strumenti tecnologici del Titolare o perfino di accedere alla rete informatica aziendale e ad eventuali dati ed informazioni ivi conservati e trattati. Pertanto, le regole di seguito previste devono intendersi a carico tanto dei primi quanto dei secondi, ferma restando la necessità che il contratto concluso con quest'ultimi rinvii al presente Regolamento.

2.2 Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche e telematiche, per "utente", da ora in poi, deve così intendersi ogni lavoratore, dipendente, collaboratore e/o consulente, il quale abbia accesso ad archivi cartacei ovvero ad archivi digitali, a cui accede, in quest'ultimo caso, tramite specifiche credenziali di autenticazione. Tale figura potrà anche venir indicata quale "responsabile esterno del trattamento", "terzo" o "persona autorizzata", in ragione delle attività e degli impegni che il soggetto assume nell'organizzazione aziendale od a favore del Titolare stesso.

3. Definizioni

3.1 Dato personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale (art. 4, punto 1).

3.2 Trattamento: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione (art. 4, punto 2).

3.3 Archivio: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico (art. 4, punto 6).

3.4 Autorità Garante: Autorità Garante per la Protezione dei Dati personali.

3.5 Titolare del trattamento (anche in breve "Titolare"): la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri (art. 4, punto 7).

3.6 Designato al trattamento: la persona fisica, espressamente designata, che opera sotto l'autorità del titolare del trattamento, con specifici compiti e funzioni connessi al trattamento dei dati personali (art. 2-quatordecies del D.lgs. 196-03).

3.7 Responsabile del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento (art. 4, punto 8).

3.8 Amministratore di Sistema: figura professionale finalizzata alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti, per conto di un Titolare del trattamento, e figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati (Provvedimento dell'Autorità Garante- Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008).

3.9 Violazione dei dati personali (anche Data breach): la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati (art. 4, punto 12).

4. Utilizzo degli archivi cartacei

4.1 L'accesso è consentito solo se previamente autorizzato dal Titolare del trattamento e deve riguardare i soli dati personali la cui conoscenza sia strettamente necessaria per adempiere i compiti assegnati.

4.2 In particolare, i documenti cartacei devono essere prelevati dagli archivi per il tempo strettamente necessario allo svolgimento delle mansioni; atti e documenti contenenti dati particolari o giudiziari devono essere custoditi in contenitori muniti di serratura e devono essere controllati in modo tale che a tali atti e documenti non possano accedere persone prive di autorizzazione; atti e documenti contenenti dati particolari o giudiziari devono essere restituiti al termine delle operazioni affidate. Tutti i documenti cartacei non devono uscire dai locali del Titolare, salvo espressa autorizzazione del Titolare o del Coordinatore di Struttura o loro delegato per specifiche fattispecie.

4.3 Con specifico riferimento alla conservazione delle cartelle cliniche dei pazienti, successivamente alla cessazione del rapporto del paziente con la relativa Struttura, la stessa è affidata alla società CSA S.p.a., debitamente nominata responsabile esterno del trattamento, ai sensi dell'art. 28 del GDPR, la quale si occupa dell'archiviazione fisica dei documenti, presso propri magazzini e, contestualmente, provvede alla digitalizzazione degli stessi.

4.4 La richiesta di rilascio di copia di cartella clinica, che avvenga successivamente alla cessazione del rapporto del paziente con la relativa Struttura, dovrà essere indirizzata al Servizio ICT o alla Segreteria Generale del Titolare, i quali, previa autorizzazione del Legale Rappresentante e/o del DPO aziendale, provvederanno a richiedere copia della stessa a CSA. Il Servizio ICT o la Segreteria Generale trasmetteranno copia digitalizzata, salvo diverso avviso del richiedente, della documentazione all'interessato, all'indirizzo e-mail dallo stesso indicato.

4.5 La richiesta di rilascio di copia di cartella clinica, che avvenga in costanza del rapporto del paziente con la relativa Struttura, dovrà essere indirizzata al Coordinatore di Struttura. Il Coordinatore di Struttura, previa autorizzazione del Legale Rappresentante e/o del DPO aziendale ed eventuale collaborazione con il Servizio ICT, provvederà a trasmettere copia digitalizzata, salvo diverso avviso del richiedente, della documentazione all'interessato, all'indirizzo e-mail dallo stesso indicato.

4.6 Il rilascio di copia della cartella clinica, di cui ai punti precedenti, avviene in conformità alle vigenti disposizioni di legge ed in particolare alla Legge 24/2017.

5. Utilizzo del Personal Computer

5.1 **Il Personal Computer affidato all'utente è uno strumento di lavoro**. Ogni utilizzo non inerente all'attività lavorativa è vietato perché può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. È inoltre vietato il salvataggio o la copia di qualsiasi documento audiovisivo protetto da diritto d'autore in violazione della normativa vigente. Il personal computer deve essere custodito con cura da parte degli assegnatari evitando ogni possibile forma di danneggiamento.

5.2 Il personal computer dato in affidamento all'utente permette l'accesso ai dati e agli applicativi del Titolare solo attraverso specifiche **credenziali di autenticazione** come meglio descritto al successivo punto 6 del presente Regolamento.

5.3 Il Titolare rende noto che il personale del servizio Information and Communication Tecnology (nel seguito per brevità "Servizio ICT"), nonché gli Amministratori di Sistema (per gli ambiti di rispettiva competenza, di seguito "A.d.S.") sono stati autorizzati a compiere interventi nel sistema informatico aziendale diretti a garantire la sicurezza e la salvaguardia del sistema stesso, nonché per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, etc.). La stessa facoltà, sempre ai fini della sicurezza del sistema e per garantire la normale operatività del Titolare, si applica anche in caso di assenza prolungata o impedimento dell'utente. Qualora lo specifico intervento dovesse comportare anche l'accesso a contenuti delle singole postazioni PC, il Servizio ICT e/o gli A.d.S. ne daranno comunicazione agli utenti interessati, preventivamente ovvero, nel caso di urgenza dell'intervento stesso, successivamente ad esso.

5.4 I suddetti soggetti hanno la facoltà di collegarsi e visualizzare in remoto i contenuti delle singole postazioni PC al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza informatica. L'intervento è effettuato esclusivamente su chiamata dell'utente o, in caso di oggettiva necessità**,** a seguito della rilevazione tecnica di problemi nel sistema informatico e telematico, previa comunicazione all'utente della necessità dell'intervento stesso, ove possibile.

5.5 **Non è consentito** l'uso di programmi diversi da quelli ufficialmente installati dal Servizio ICT e dagli A.d.S. per conto del Titolare né agli utenti di installare autonomamente programmi provenienti dall'esterno, sussistendo infatti il grave pericolo di introdurre virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti. L'inosservanza della presente disposizione espone il Titolare a gravi responsabilità civili; si evidenzia, inoltre, che le violazioni della normativa a tutela dei diritti d'autore sul software che impone la presenza nel sistema di software regolarmente licenziato, o comunque libero e quindi non protetto dal diritto d'autore, sono sanzionate penalmente e possono anche comportare il sorgere di una responsabilità amministrativa a carico del Titolare, come disposta dall'art. 25-nonies del D.lgs. 8 giugno 2001, n. 231, con applicazione di sanzioni pecuniarie ed interdittive.

5.6 Salvo preventiva espressa autorizzazione del personale del Servizio ICT e/o degli A.d.S., non è consentito all'utente modificare le caratteristiche impostate sul proprio PC né procedere ad installare

dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, …).

5.7 Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il Servizio ICT e/o gli A.d.S. nel caso in cui siano rilevati virus e adottando quanto previsto dal successivo punto 12 del presente Regolamento relativo alle procedure di protezione antivirus.

5.8 Il personal computer deve essere spento al termine dell'attività lavorativa prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio o in caso di suo inutilizzo, salva la necessità di mantenere lo stesso acceso (ma debitamente bloccato) al fine di garantire l'operatività da remoto. In caso di allontanamento per breve lasso di tempo, non lasciare accessibile il personal computer, bloccandolo manualmente. È impostato un salvaschermo (screen saver) automatico protetto da password che pulisca la videata entro alcuni minuti in caso di inutilizzo. In ogni caso, lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso.

6. Gestione e assegnazione delle credenziali di autenticazione

6.1 Soggetto preposto alla gestione delle credenziali di autenticazione è il personale incaricato del Servizio ICT.

6.2 Le credenziali di autenticazione per l'accesso alla rete sono assegnate dal Servizio ICT previa espressa indicazione del Coordinatore di struttura nell'ambito del quale sarà inserito ed andrà ad operare il nuovo utente.

6.3 Le credenziali di autenticazione consentono un livello di accesso ai dati e relativi poteri conformi alla mansione concretamente svolta dal soggetto autorizzato.

6.4 Le credenziali di autenticazione consistono in un "nome utente" formata da *nome.cognome* dell'utente stesso assegnato dal Servizio ICT, associato ad una parola chiave (password) riservata che dovrà essere **custodita dall'addetto con la massima diligenza e non divulgata**. Non è consentita l'attivazione della password di accensione (bios), senza preventiva autorizzazione da parte del Servizio ICT.

6.5 La parola chiave deve essere formata dalla combinazione di lettere maiuscole e minuscole e numeri, deve essere composta da almeno otto caratteri e non deve contenere riferimenti agevolmente riconducibili all'addetto o contenere il proprio nome e cognome o una delle precedenti password.

6.6 È necessario procedere alla modifica della parola chiave a cura dell'utente, addetto del trattamento, al primo utilizzo e, successivamente, **ogni 90 giorni**. Qualora l'utente non provveda a variare la propria password in tempo, l'accesso al personale computer e/o al sistema sarà temporaneamente bloccato.

6.7 Qualora la parola chiave dovesse venir sostituita, per decorso del termine sopra previsto e/o in quanto abbia perduto la propria riservatezza, o sia stata dimenticata dall'utente stesso, si procederà in tal senso d'intesa con il personale del Servizio ICT.

7. Utilizzo della rete della Società Cooperativa Sociale Interactive

7.1 L'utilizzo di tutte le reti internet, Wi-Fi o cablate, presenti presso i locali del Titolare è limitato agli utenti autorizzati. A tale scopo si precisa che l'utilizzo di qualsiasi rete disponibile presso i locali del Titolare e dallo stesso configurata è possibile solo a seguito di digitazione di specifiche credenziali assegnate e a seguito dell'abilitazione del dispositivo nel filtro indirizzi MAC (*o MAC Address, Media Access Control: codice esadecimale di 12 cifre assegnato in modo univoco dai produttori a livello mondiale*) gestito dal personale del reparto ICT.

7.2 Per l'accesso al dominio aziendale e agli applicativi del Titolare ciascun utente deve utilizzare la propria credenziale personale di autenticazione.

7.3 È assolutamente proibito entrare nella rete e nei programmi con un codice d'identificazione utente diverso da quello assegnato. Le parole chiave d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite.

7.4 L'accesso da remoto alla VPN è possibile agli utenti abilitati solo a seguito di utilizzo di credenziali aziendali di accesso al dominio aziendale e installazione di software che lo abilita sui dispositivi in uso.

7.5 Le macro-cartelle presenti nei server del Titolare sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto, qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità sono svolte regolari attività di manutenzione, amministrazione e back up da parte del personale del Servizio ICT e/o degli ADS. Si ricorda che tutti i dischi o altre unità di memorizzazione locali - es. disco C: interno PC - non sono soggette a salvataggio da parte del personale incaricato del Servizio ICT. La responsabilità del salvataggio dei dati ivi contenuti è pertanto a carico del singolo utente, fermo restando che qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità.
Sono presenti le cartelle "Scambio" e "Scansioni" per l'archiviazione temporanea di dati e sono soggette a cancellazione automatica dei file con data di creazione antecedente al mese precedente.

7.6 Il personale del Servizio ICT e/o gli ADS possono in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la Sicurezza sia sui PC degli addetti sia sulle unità di rete.

7.7 Risulta opportuno che, con regolare periodicità, ciascun utente provveda alla pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati, essendo infatti necessario evitare un'archiviazione ridondante.

7.8 Nella gestione dei sistemi informatici aziendali, il servizio ICT e/o gli ADS potranno acquisire informazioni generate dalle funzionalità insite negli stessi sistemi, quali, nell'eventualità dell'adozione di appositi software, ad esempio, le informazioni sugli orari di accensione e spegnimento dei personal computer, rilevati automaticamente tramite il sistema di autenticazione al dominio di rete, e i log degli accessi a specifiche risorse di rete (file o cartelle). Tali informazioni potranno essere utilizzate, ai sensi del successivo punto 16.2, per tutti i fini connessi al rapporto di lavoro, sempre nell'ambito delle finalità individuate nel precedente punto 5.3., e con espressa esclusione di qualsiasi forma di controllo sistematico e costante nei confronti degli utenti degli stessi sistemi.

7.9 L'accesso da remoto alla rete aziendale è possibile solo utilizzando i dispositivi previsti. A tale scopo sono impostate delle regole sul firewall che impediscono l'accesso di dispositivi non abilitati.

7.10 Il dipendente con contratto di lavoro agile, qualora presente, è tenuto al rispetto delle procedure elencate nel presente documento, ed in particolare alla cura e all'utilizzo responsabile della postazione di lavoro fornitagli dal Titolare, che riceve mediante comodato d'uso e dei cui danni è responsabile ai sensi dell'art. 2051 del codice civile, a meno che non provi il caso fortuito. Il lavoratore agile è, altresì, tenuto al dovere di riservatezza su tutte le informazioni delle quali venga in possesso per il lavoro assegnatogli e di quelle derivanti dall'utilizzo delle apparecchiature, dei programmi e dei dati in essi contenuti nonché all'adozione di ogni accortezza tecnica e comportamentale atta a garantire la tutela ed il corretto uso dei dati trattati.

7.11 Il dipendente o il professionista collaboratore non può utilizzare attrezzature proprie per accedere alla rete aziendale, salvo esplicita autorizzazione rilasciata dal Legale Rappresentante in casi eccezionali. In tali casi, l'accesso avverrà attraverso l'attivazione di un software di VPN e di una abilitazione dedicata predisposti dal Servizio ICT, purché i dispositivi siano compatibili dal punto di vista tecnico e di conformità alle norme di sicurezza con la prestazione da svolgere. L'autorizzazione deve essere formalizzata esplicitamente nel contratto o in suoi specifici allegati/addendum.

8. Utilizzo di altri dispositivi elettronici

8.1 Tutti i dispositivi elettronici dati in dotazione al personale del Titolare **devono considerarsi strumenti di lavoro:** ne viene concesso l'uso esclusivamente per lo svolgimento delle attività lavorative, non essendo quindi consentiti utilizzi a carattere personale o comunque non strettamente inerenti le attività lavorative.

8.2 L'utente resta responsabile della custodia ex art. 1768 c.c. del singolo dispositivo assegnato e deve custodirlo con diligenza sia durante trasferte e spostamenti sia durante l'utilizzo nel luogo di lavoro; va sempre adottata ogni cautela per evitare danni o sottrazioni. In caso di smarrimento o furto di dispositivi le cui memorie possano essere cancellate o bloccate da remoto a cura del Servizio ICT per

evitare sottrazioni o diffusioni di dati incontrollati, l'utente dovrà immediatamente avvisare il referente ICT, e comunque al massimo entro 2 ore dal fatto.

8.3 Con riferimento ai telefoni aziendali, tablet e smartphone, fermo restando quanto sopra già disposto circa il loro uso e custodia, la ricezione o l'effettuazione di telefonate personali, così come l'invio o la ricezione di SMS, MMS, messaggi WhatsApp o e-mail di natura personale o comunque non pertinenti rispetto allo svolgimento dell'attività lavorativa, è consentita solo nel caso di comprovata necessità ed urgenza.

8.4 Su ciascun telefono aziendale e smartphone viene installato da parte del Servizio ICT un sistema MDM (Mobile Device Management), che raccoglie taluni dati tecnici del device (ad es. marca, modello, seriale, ecc.) e permette l'installazione e gestione delle applicazioni aziendali necessarie per l'operatività e per la protezione e la sicurezza dei dati e del device stesso. Altre app non posso essere installate dagli utenti, al di fuori di quelle approvate dal Titolare. In caso di furto e/o smarrimento del device, dietro denuncia formale alle Autorità e previa approvazione del Legale Rappresentante, sarà possibile, da parte del Servizio ICT, tentare (con indicazione di motivazione scritta) di rintracciare il device.

8.5 Si precisa, peraltro, che le disposizioni previste nel presente Regolamento ai punti 5, 9, 10, 11, 12 e 15 dello stesso trovano applicazione anche nell'uso dei dispositivi elettronici qui considerati.

8.6 E' infine disposto il divieto di utilizzo per fini personali di fax aziendali, per spedire o per ricevere documentazione, e/o di fotocopiatrici aziendali, salva diversa esplicita autorizzazione da parte del Coordinatore di struttura.

9. Utilizzo e conservazione dei supporti rimovibili

9.1 Non è previsto l'utilizzo di supporti di archiviazione rimovibili (es. supporti pendrive USB o hard-disk portatili), salvo casi eccezionali che dovranno essere autorizzati dal legale rappresentante o dal DPO. In questi casi eccezionali, i supporti di archiviazione rimovibili contenenti dati particolari nonché informazioni costituenti know-how aziendale, devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto o, successivamente alla cancellazione, recuperato.

9.2 L'utente resta, in ogni caso responsabile della custodia dei supporti e dei dati aziendali in essi contenuti e, in particolare, è tenuto a cancellarli definitivamente dal dispositivo immediatamente dopo l'utilizzo.

9.3 È severamente vietato l'utilizzo di supporti rimovibili personali.

9.4 Al fine di assicurare la distruzione e/o inutilizzabilità di supporti di archiviazione contenenti dati sensibili all'interno di dispositivi che devono essere dismessi, ciascun utente dovrà contattare il personale del Servizio ICT e seguire le istruzioni da questo impartite. Nel caso di dispositivi elettronici, con riferimento in particolare a computer portatili, tablet ed altri dispositivi sui quali possano venir salvati documenti, dati ed altro materiale, dovrà farsi particolare attenzione al salvataggio su server del materiale aziendale e alla rimozione effettiva degli eventuali documenti personali prima della riconsegna del dispositivo, concordata comunque ogni opportuna azione al riguardo con il personale del Servizio ICT.

10. Uso della posta elettronica

10.1 **La casella di posta elettronica assegnata all'utente è uno strumento di lavoro.** Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.
È fatto divieto di utilizzare le caselle di posta elettronica aziendali oppure il sistema di indirizzi di posta elettronica delle strutture tra più utenti per motivi diversi da quelli strettamente legati all'attività lavorativa. In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare la posta elettronica per:

- l'invio e/o il ricevimento di allegati contenenti filmati o brani musicali (es. mp3) non legati all'attività lavorativa;
- l'invio e/o il ricevimento di messaggi personali o per la partecipazione a dibattiti, aste on line, concorsi, forum o mailing-list;

- la partecipazione a catene telematiche (o c.d. “di Sant’Antonio”). Se si verificano occorre comunicarlo immediatamente al personale del Servizio ICT. Non si dovrà in alcun caso procedere all’apertura degli allegati a tali messaggi.

10.2 La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili o non costituenti corrispondenza commerciale e soprattutto allegati ingombranti. In caso di cessazione del rapporto di lavoro, il singolo dipendente è tenuto ad eliminare dalle proprie cartelle tutti i messaggi di posta elettronica ed i documenti non pertinenti l’attività aziendale e non utili alle esigenze aziendali, mantenendo integra, invece, tutta la corrispondenza e documentazione inerente alla attività lavorativa. Resta inteso che, di conseguenza, la documentazione presente nel profilo del singolo utente che cessa il rapporto di lavoro verrà considerata presuntivamente dall’azienda quale corrispondenza e documentazione lavorativa e non personale.

10.3 Poiché la casella di posta assegnata costituisce strumento di lavoro, è opportuno evidenziare che i messaggi ivi contenuti, avendo presuntivamente natura di corrispondenza commerciale, saranno conservati nei server aziendali a norma dell’art. 2220 del Codice civile per un periodo congruo alle finalità aziendali e non oltre ad anni 10.

10.4 È obbligatorio porre la massima attenzione nell’aprire i file allegati di posta elettronica prima del loro utilizzo (ad esempio non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).

10.5 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, il sistema, in caso di assenze programmate (ad es. per ferie o attività di lavoro fuori sede dell’assegnatario della casella) invierà automaticamente messaggi di risposta contenenti le coordinate di posta elettronica di un altro soggetto o altre utili modalità di contatto della struttura. In tal caso, la funzionalità deve essere attivata e disattivata dall’utente.

10.6 In caso di assenza non programmata (ad es. per malattia) la procedura - qualora non possa essere attivata dal lavoratore avvalendosi del servizio webmail entro due giorni - verrà attivata a cura del Servizio ICT appena comunicato dal Coordinatore di struttura.

10.7 Sarà comunque consentito al superiore gerarchico dell’utente o, comunque, sentito l’utente, a persona individuata dall’azienda, accedere alla casella di posta elettronica dell’utente per ogni ipotesi in cui si renda necessario (ad es.: mancata attivazione della funzionalità di cui al punto 10.5; assenza non programmata ed impossibilità di attendere i due giorni di cui al punto 10.6).

10.8 Il personale del Servizio ICT, nell’impossibilità di procedere come sopra indicato e nella necessità di non pregiudicare la necessaria tempestività ed efficacia dell’intervento, potrà accedere alla casella di posta elettronica per le sole finalità indicate al punto 5.3.

10.9 Al fine di ribadire agli interlocutori la natura esclusivamente aziendale della casella di posta elettronica, i messaggi devono contenere un avvertimento standardizzato nel quale sia dichiarata la natura non personale dei messaggi stessi precisando che, pertanto, il personale debitamente incaricato del Titolare potrà accedere al contenuto del messaggio inviato alla stessa casella secondo le regole fissate nella propria policy aziendale.

10.10 Il Titolare si riserva la facoltà, a proprio insindacabile giudizio, di assegnare o ritirare l’utilizzo della casella di posta elettronica in base alla propria esclusiva e insindacabile valutazione della necessità di utilizzo della stessa per lo svolgimento delle attività lavorative.

10.11 La casella di posta elettronica, unitamente alle credenziali di autenticazione per l’accesso alla rete, è disattivata al momento della conclusione del rapporto di lavoro che ne giustificava l’assegnazione. Il Titolare si riserva, tuttavia, di valutare a proprio esclusivo ed insindacabile giudizio la necessità di mantenere attiva in ricezione la casella per un congruo periodo di tempo al fine di garantire la funzionalità aziendale; in tal caso:

- avranno accesso alla casella esclusivamente dipendenti individuati dall’azienda in funzione alle mansioni lavorative assegnate;
- verranno inviate mail ai mittenti con indicazione della diversa casella di posta elettronica aziendale cui trasmettete i messaggi;
- è escluso, comunque, l’invio di messaggi da tale casella di posta;

- una copia della posta così rilasciata verrà salvata ai fini della conservazione di cui al precedente punto 10.3.

11. Navigazione in Internet

11.1 **Il PC assegnato al singolo utente ed abilitato alla navigazione in Internet costituisce uno strumento aziendale utilizzabile esclusivamente per lo svolgimento della propria attività lavorativa**. È quindi assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa.

11.2 In questo senso, a titolo puramente esemplificativo, **l'utente non potrà utilizzare internet** per:

- l'upload o il download di software anche gratuiti (freeware) e shareware, nonché l'utilizzo di documenti provenienti da siti web o http, se non strettamente attinenti all'attività lavorativa (filmati e musica) e previa verifica dell'attendibilità dei siti in questione (nel caso di dubbio, dovrà venir a tal fine contattato il personale del Servizio ICT);
- l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, fatti salvi i casi direttamente autorizzati dalla Direzione della Cooperativa (o eventualmente dal Coordinatore di struttura e/o del Servizio ICT) e comunque nel rispetto delle normali procedure di acquisto;
- ogni forma di registrazione a siti i cui contenuti non siano strettamente legati all'attività lavorativa;
- la partecipazione a Forum non professionali, l'iscrizione con account aziendale e la partecipazione personale a social network, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames) se non espressamente autorizzati dal Coordinatore di struttura;
- l'accesso, tramite internet, a caselle webmail di posta elettronica personale.

11.3 Al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa, il Titolare rende peraltro nota l'adozione di uno specifico sistema di blocco o filtro automatico che prevenga determinate operazioni quali l'upload o l'accesso a determinati siti o a determinate categorie di siti inseriti in una "black list". Su specifica richiesta dei responsabili di struttura al Servizio ICT di accesso a determinati siti web presenti nelle predette liste, e previa verifica della sicurezza dei siti stessi, anche da parte dell'ADS, quest'ultimo potrà inserire delle eccezioni relative a tali siti.

11.4 Gli eventuali controlli, compiuti dall'ADS, ai sensi del precedente punto 5.3, potranno avvenire mediante un sistema di controllo dei contenuti (Proxy server) o mediante "file di log" della navigazione svolta. Il controllo sui file di log non è continuativo ed i file stessi sono conservati non oltre sei mesi, ossia il tempo indispensabile per il corretto perseguimento delle finalità organizzative e di sicurezza del Titolare.

12. Protezione antivirus

12.1 Il sistema informatico del Titolare è protetto da software antivirus aggiornato quotidianamente. Ogni utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale mediante virus o mediante ogni altro software aggressivo.

12.2 Nel caso il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente sospendere ogni elaborazione in corso senza spegnere il computer nonché segnalare prontamente l'accaduto al personale del Servizio ICT.

12.3 Ogni supporto di archiviazione rimovibile di provenienza esterna al Titolare dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, dovrà essere prontamente consegnato al personale del Servizio ICT.

13. Gestione degli incidenti e data breach

13.1 Ogni incidente (ad es. malfunzionamento PC, indisponibilità dei servizi applicativi e di rete, furto o smarrimento di dispositivi e/o documenti cartacei, sottrazione di dati, invio accidentale di dati

all'esterno) deve essere segnalato dall'Utente immediatamente al servizio ICT e/o al DPO, che raccoglieranno le segnalazioni e avvieranno il relativo processo di classificazione e risoluzione dell'incidente medesimo al fine di minimizzare gli eventuali impatti negativi sul normale svolgimento delle attività lavorative.

13.2 Nel caso l'incidente possa determinare una violazione dei dati personali, cioè la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati (cd. "data breach"), l'utente dovrà prontamente avvisare il DPO e fornire la massima collaborazione per consentire al Titolare del trattamento di ottemperare agli obblighi previsti dagli artt. 33 e 34 del GDPR (notifica autorità di controllo, comunicazioni all'interessato, ecc.).

14. Gestione delle richieste di esercizio dei diritti degli interessati

14.1 Onde evitare che un uso non corretto dei dati personali possa danneggiare o ledere le libertà fondamentali e la dignità personale di ognuno, il GDPR 2016/679 ha ampliato e rafforzato il quadro di tutele assicurate all'interessato i cui dati personali sono oggetto di trattamento. Pertanto, si informano i lavoratori che, nello svolgimento della loro attività lavorativa, potrebbero ricevere richieste circa il trattamento dei dati personali da parte degli interessati. Gli Interessati coinvolti potranno essere a titolo indicativo e non esaustivo:

- Interessati riconducibili all'Area risorse umane: candidati, dipendenti, i familiari dei dipendenti ed ex dipendenti della Società, nonché i liberi professionisti che prestano la propria attività per la Società e i dipendenti di soggetti terzi che forniscono servizi in favore dello stesso;
- Interessati riconducibili all'Area Amministrazione: clienti, fornitori, studi professionali, consulenti, in relazione alla gestione dei contratti con essi stipulati e il relativo compimento di tutte le attività connesse, strumentali e/o complementari alla gestione del rapporto;
- Interessati riconducibili all'Area Servizi: utenti e beneficiari dei servizi, nonché loro familiari, genitori, tutori legali;
- Altri Interessati: utenti web nonché tutti gli individui, esterni all'organizzazione del titolare, che non sono riconducibili alle precedenti categorie.

14.2 In caso il lavoratore riceva una richiesta di esercizio dei diritti dell'interessato dovrà, quindi, provvedere prontamente, e comunque non oltre le 24 ore successive alla venuta a conoscenza della richiesta, a comunicare al coordinatore di struttura il quale, a sua volta, provvede a comunicarlo, se del caso, al DPO, il contenuto e le circostanze dettagliate della richiesta, nonché i riferimenti del richiedente.

14.3 Qualora la richiesta dovesse pervenire tramite e-mail, il lavoratore dovrà inoltrare la suddetta e-mail all'indirizzo del coordinatore di struttura, il quale provvederà ad inoltrarla, se del caso al DPO all'indirizzo dpo@interactive.coop .

14.4 Qualora la richiesta venisse effettuata di persona dall'interessato, il lavoratore dovrà verificare l'identità dello stesso tramite riconoscimento diretto o verifica di un documento d'identità, fornire, se del caso, all'interessato una copia del modulo per l'esercizio dei diritti degli interessati, per facilitarlo nella formulazione della richiesta, e provvedere a trasmettere il tutto entro i termini stabiliti al punto 14.2, al Coordinatore di struttura il quale provvederà ad inoltrarlo, se del caso, al DPO. Dovrà, inoltre, informare il richiedente del fatto che il Titolare del trattamento provvederà ad elaborare la sua richiesta, a ricontattarlo in caso necessiti di ulteriori informazioni e fornire un riscontro entro un mese.

14.5 In caso la richiesta dovesse pervenire attraverso altri canali (ad esempio via telefono) chi la riceve dovrà immediatamente informare l'interessato di inoltrare la sua richiesta via e-mail o via posta raccomandata, allegando una copia del documento d'identità.

14.6 L'interessato potrà inoltrare la propria richiesta anche tramite un terzo autorizzato. Il lavoratore dovrà, nel caso, verificare la presenza di apposita delega/mandato debitamente sottoscritto dall'interessato e copia di un documento d'identità dell'interessato.

15. Partecipazioni a social media

15.1 L'utilizzo a fini promozionali e commerciali dei social media – quali Facebook™, Twitter™, Linkedin™, dei blog e dei forum, anche professionali – nonché del sito web aziendale, sarà gestito ed organizzato esclusivamente dal Titolare attraverso specifiche direttive ed istruzioni operative al personale dell'Ufficio Progettazione, Fund Raising e Comunicazione a ciò espressamente addetto, rimanendo escluse iniziative individuali da parte dei singoli utenti (conformemente a quanto disposto al precedente punto 11.2).

15.2 Fermo restando il pieno ed inderogabile diritto della persona alla libertà di espressione ed al libero scambio di idee ed opinioni, il Titolare ritiene comunque opportuno indicare agli utenti alcune regole comportamentali, al fine di tutelare tanto la propria immagine ed il patrimonio aziendale, anche immateriale, quanto i propri collaboratori, i propri clienti e fornitori, gli altri partners, oltre che gli stessi utenti utilizzatori dei social media, fermo restando che è vietata la partecipazione agli stessi social media durante l'orario di lavoro. La policy qui dettata deve venir seguita dagli utenti sia che utilizzino dispositivi messi a disposizione dal Titolare, sia che utilizzino propri dispositivi, sia che partecipino ai social media a titolo personale, sia che lo facciano per finalità professionali, come dipendenti del Titolare.

15.3 La condivisione dei contenuti nei social media deve sempre rispettare e garantire la segretezza sulle informazioni aziendali considerate del Titolare riservate ed in genere, a titolo esemplificativo e non esaustivo, sulle informazioni finanziarie ed economiche, commerciali, sui piani industriali, sui clienti, sui fornitori ed altri partners del Titolare. Inoltre, ogni comunicazione e divulgazione di contenuti dovrà essere effettuata nel pieno rispetto dei diritti di proprietà industriale e dei diritti d'autore, sia di terzi che del Titolare; l'utente, nelle proprie comunicazioni, non potrà quindi inserire marchi od altri segni distintivi del Titolare, né potrà pubblicare disegni, modelli od altro connesso ai citati diritti. Ogni deroga a quanto sopra disposto potrà peraltro avvenire solo previa specifica autorizzazione della Direzione Generale del Titolare.

15.4 L'utente deve garantire la tutela della privacy delle persone; di conseguenza, non potrà comunicare o diffondere dati personali (quali dati anagrafici, immagini, video, suoni e voci) di colleghi e in genere di collaboratori aziendali, se non con il preventivo personale consenso di questi, e comunque non potrà postare nel social media immagini, video, suoni e voci registrati all'interno dei luoghi di lavoro aziendali, se non con il preventivo consenso del Coordinatore di struttura.

15.5 L'utente risponde personalmente dei propri comportamenti e deve astenersi dal realizzare, nei confronti in genere di terzi e specificatamente verso il Titolare, i colleghi, i clienti ed i fornitori, attività che possano essere penalmente o civilmente rilevanti; a titolo esemplificativo, sono quindi vietati comportamenti ingiuriosi, diffamatori e denigratori, discriminatori o che configurano molestie. In tal senso, è vivamente auspicato da parte di tutti un comportamento civile e sobrio, in particolar modo in qualunque occasione in cui l'espressione o il contesto in cui essa avviene possa essere collegata all'ambito aziendale.

15.6 Infine, in via generale ed ove non autorizzato in senso diverso dal proprio Coordinatore di struttura, l'utente, nell'uso dei social network, esprimerà unicamente le proprie opinioni personali; pertanto, ove necessario od opportuno per la possibile connessione con il Titolare, in particolare in forum professionali, l'utente dovrà precisare che le opinioni espresse sono esclusivamente personali e non riconducibili al Titolare.

16. Osservanza delle disposizioni in materia di Privacy

16.1 È obbligatorio attenersi alle disposizioni in materia di Privacy e di misure minime di sicurezza, come indicato nella lettera di designazione ad addetto del trattamento dei dati ai sensi del D.lgs.101/2018 e Reg. EU 679/2016 (GDPR).

16.2 Gli strumenti tecnologici considerati nel presente Regolamento costituiscono tutti strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa, anche ai sensi e per gli effetti dell'art. 4, comma secondo, della Legge n.300/1970; conseguentemente, le informazioni raccolte sulla base di quanto indicato nel Regolamento, anche conformemente al successivo punto 17, possono essere utilizzate a

tutti i fini connessi al rapporto di lavoro, essendone stata data informazione ai lavoratori sulle modalità di uso degli strumenti stessi, sugli interventi che potranno venir compiuti nel sistema informatico aziendale ovvero nel singolo strumento e sui conseguenti sistemi di controllo che potessero venir eventualmente compiuti (conformemente al successivo punto 18), fermo restando il rispetto della normativa in materia di protezione dei dati personali (ai sensi del D.lgs.101/2018 e Reg. EU 679/2016 - GDPR).

16.3 Si precisa che non sono installati o configurati sui sistemi informatici in uso agli utenti apparati hardware o strumenti software aventi come scopo il controllo a distanza dell'attività dei lavoratori; peraltro, laddove l'adozione di tali apparati risultasse necessaria per finalità altre, es. esigenze organizzative e produttive, di sicurezza del lavoro e/o di tutela del patrimonio aziendale, il Titolare provvederà conformemente a quanto disposto dall'art.4, comma primo, della Legge n. 300/1970, dandone opportuna informazione agli utenti stessi.

17. Accesso ai dati trattati dall'utente

17.1 Oltre che per motivi di sicurezza del sistema informatico, compresi i motivi tecnici e/o manutentivi (ad esempio, aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, etc.), per finalità di controllo e programmazione dei costi aziendali (ad esempio, verifica costi di connessione ad Internet, traffico telefonico, etc.), comunque estranei a qualsiasi finalità di controllo dell'attività lavorativa, è facoltà della Direzione Aziendale, tramite il personale del Servizio ICT o gli ADS, accedere direttamente, nel rispetto della normativa sulla privacy e delle procedure di cui ai precedenti 5.3. e 5.4, a tutti gli strumenti informatici aziendali e ai documenti ivi contenuti, nonché ai tabulati del traffico telefonico.

18. Sistemi di controlli graduali

18.1 In caso di anomalie, il personale incaricato del Servizio ICT e/o gli ADS effettueranno controlli anonimi che si concluderanno con avvisi generalizzati diretti ai dipendenti dell'area o del settore in cui è stata rilevata l'anomalia, nei quali si evidenzierà l'utilizzo irregolare degli strumenti aziendali e si inviteranno gli interessati ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite. Controlli su base più ristretta o anche individuale potranno essere computi solo in caso di successive ulteriori anomalie.

18.2 In nessun caso verranno compiuti controlli prolungati, costanti o indiscriminati.

19. Sanzioni

19.1 È fatto obbligo a tutti gli utenti di osservare le disposizioni portate a conoscenza con il presente Regolamento. Il mancato rispetto o la violazione delle regole sopra ricordate è perseguibile nei confronti del personale dipendente con provvedimenti disciplinari e risarcitori previsti dal vigente CCNL per le cooperative sociali, e nei confronti dei collaboratori, consulenti, agenti ed incaricati esterni di cui all'1.2, verificata la gravità della violazione contestata, con la risoluzione od il recesso dal contratto ad essi relativo nonché con tutte le azioni civili e penali consentite.

20. Aggiornamento e revisione

20.1 Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni motivate al presente Regolamento. Le proposte saranno esaminate dalla Direzione della Cooperativa.

20.2 Il presente Regolamento è soggetto periodicamente a revisione.

Torino, 30.05.2025