Regolamento per l’utilizzo delle risorse ICT

Documento adottato dal Consiglio di Amministrazione in data 15 luglio 2019

Precedenti modifiche del documento:

1ª approvazione Consiglio di Gestione in data 11 settembre 2014

15 luglio 2019

1 Premessa

La progressiva diffusione delle nuove tecnologie informatiche, ed in particolare il libero accesso alla rete tramite i personal computer, espone le organizzazioni aziendali a potenziali profili di responsabilità patrimoniale e penale in termini di sicurezza e di immagine.

La sicurezza delle informazioni ha il compito di tutelare la **riservatezza** (assicurare che le informazioni siano accessibili solo a chi è autorizzato), l'**integrità** (assicurare che i dati possano essere creati, modificati o cancellati solo dalle persone autorizzate a svolgere tale operazione) e la **disponibilità** (assicurare che l'informazione ed i servizi informatici devono essere a disposizione degli utenti del sistema compatibilmente con i livelli di servizio) delle informazioni, riducendo ad un livello accettabile il rischio di perdita, modifica o indisponibilità.

Deve essere inoltre garantita la **conformità** dei sistemi informativi rispetto ai requisiti di sicurezza previsti dall'ordinamento giuridico, ed in particolare dal Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati) (di seguito per brevità **"GDPR")** e dal D. Lgs. 30 giugno 2003, n. 196 e s.m.i., recante "Codice in materia di protezione dei dati personali" (di seguito per brevità **"Codice Privacy"**). Ogni attività prevista nel presente Regolamento deve essere posta in essere nel rispetto della predetta normativa e relativi regolamenti attuativi.

Le attività per il raggiungimento di tale obiettivo sono complesse e articolate e richiedono una continua evoluzione. Una corretta attuazione è possibile solo attraverso la collaborazione di tutti i soggetti coinvolti. È inoltre fondamentale il coordinamento ed il monitoraggio delle attività di sicurezza correnti e di innovazione tecnologica, soprattutto qualora affidate a fornitori esterni, anche attraverso una corretta identificazione dei ruoli e delle responsabilità dei fornitori dei servizi e degli utenti del sistema sulla consapevolezza e sensibilizzazione del personale attraverso il continuo aggiornamento delle politiche di comportamento da tenere nell'utilizzo degli strumenti informatici.

L'utilizzo delle risorse informatiche e telematiche deve sempre ispirarsi ai principi di diligenza e correttezza, atteggiamenti questi destinati a sorreggere ogni atto o comportamento posto in essere nell'ambito del rapporto di lavoro.

Le attrezzature informatiche, i relativi programmi e/o applicazioni, i dati e i documenti elettronici affidati in uso agli utenti sono strumenti di lavoro, di cui l'azienda può disporre indiscriminatamente, essendo titolare di qualsiasi diritto ad essi correlato. Tutto quanto messo a disposizione, ricevuto, rilasciato e comunque memorizzato per attività lavorative è e rimane di proprietà dell'azienda.

2 Scopo e campo di applicazione

La finalità del presente Regolamento è quella di disciplinare l'utilizzo delle risorse informatiche e promuovere l'osservanza delle regole in materia di protezione dei dati personali, al fine di garantire l'adeguata riservatezza, integrità e disponibilità dei dati gestiti dall'organizzazione.

In particolare S.C.R. Piemonte S.p.A. (di seguito per brevità S.C.R. o Società) adotta il presente Regolamento al fine di:

- evitare comportamenti inconsapevoli che possano innescare problemi o minacce alla sicurezza nel trattamento dei dati;
- informare gli utenti di quali sono le misure di tipo organizzativo e tecnologico adottate a livello aziendale per la sicurezza dei dati;
- illustrare quali sono le modalità di utilizzo consapevole e diligente delle risorse messe a disposizione;
- comunicare agli utenti le finalità e le modalità dei controlli che l'azienda potrebbe effettuare sulle risorse messe a disposizione per attività lavorative;
- fornire agli utenti una serie di indicazioni operative sulle corrette modalità di trattamento dei dati personali, delle informazioni e degli strumenti che permettono di gestirli.

Le prescrizioni contenute nel presente Regolamento si applicano all'insieme delle risorse informative, elettroniche, di comunicazione, di archiviazione, audiovisive e a qualsiasi altra tipologia di risorsa utilizzata per perseguire le finalità aziendali, siano essi di proprietà dell'azienda che di soggetti che operano in nome e per conto di essa.

Nel caso di soggetti esterni designati da S.C.R responsabili o sub-responsabili del trattamento ai sensi dell'art. 28 del Regolamento UE 2016/679, questi devono impegnarsi a rispettare e far rispettare gli stessi principi di sicurezza e di modalità di gestione delle informazioni presenti nel documento a tutti i propri dipendenti e ad eventuali altri soggetti.

3 Definizioni

TITOLARE DEL TRATTAMENTO DEI DATI: è la figura individuata dall'art. 4 GDPR, definita come 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. Vigila sulla puntuale osservanza di tutte le disposizioni in materia di trattamento dei dati. Designa tutte le altre figure coinvolte nel trattamento informatico dei dati.

RESPONSABILE DEL TRATTAMENTO DEI DATI: anch'esso previsto dall'art. 4 del GDPR, è definito come la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che tratta dati personali per conto del titolare del trattamento, all'interno o all'esterno dell'organizzazione, attenendosi alle istruzioni da quest'ultimo impartite, secondo quanto previsto dall'art. 28. I Responsabili devono presentare garanzie sufficienti per mettere in atto misure tecniche ed organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del Regolamento e garantisca la tutela dei diritti dell'interessato.

AUTORIZZATI AL TRATTAMENTO DEI DATI: sono le persone fisiche designate dal titolare del trattamento, a cui sono assegnati specifici compiti e funzioni connessi al trattamento dei dati; trattano i dati sia attraverso strumenti informatici che cartacei; operano attenendosi alle istruzioni impartite.

AMMINISTRATORI DI SISTEMA: sono le figure, designate dal Titolare o dai Responsabili, che provvedono operativamente alla gestione e manutenzione del sistema informatico sulla base delle misure organizzative fissate dal responsabile dei servizi informativi, in linea con quanto indicato dal Garante della Privacy nel suo provvedimento del 27 novembre 2008 e aggiornamenti successivi. Il provvedimento prevede la possibilità di nominare Amministratori di Sistema sia interni che esterni all'azienda: per le finalità del seguente documento si intendono gli Amministratori di Sistema preposti alla gestione interna delle risorse informatiche aziendali, siano essi interni o esterni.

SISTEMI INFORMATIVI E DI E-PROCUREMENT (di seguito, per brevità "Sistemi informativi"): è la struttura aziendale preposta alla gestione, alla configurazione, al coordinamento e al rilascio delle risorse informatiche aziendali, a cui fanno riferimento gli Amministratori di Sistema competenti per tale contesto.

INCARICATI DEL BACKUP: sono i soggetti individuati all'interno dei Sistemi Informativi che si occupano della gestione e verifica dei backup dei dati sulla base delle misure di sicurezza aziendali.

UTENTI: sono i soggetti ai quali il presente Regolamento si rivolge cui sono riconducibili le seguenti categorie: amministratori e dipendenti che utilizzano le risorse informatiche e telematiche proprie o fornite dalla Società nello svolgimento delle loro attività di carattere lavorativo o istituzionale, soggetti esterni che operano in nome e per conto della Società utilizzando risorse informatiche messe a disposizione dalla Società stessa.

TRACCIAMENTO: memorizzazione di eventi e operazioni effettuata automaticamente da un qualsivoglia dispositivo informatico, per finalità manutentive e di funzionamento dello stesso.

RILEVAZIONE: complesso di operazioni di raccolta, analisi, verifica, conservazione dei tracciamenti effettuati dai dispositivi e di qualsiasi altra forma di intervento di carattere professionale riferibile al funzionamento e all'utilizzo delle risorse informatiche, svolto a fronte di comprovate necessità definite nei capitoli seguenti del presente regolamento.

4 Osservanza del presente Regolamento

L'osservanza del presente Regolamento è un obbligo per tutti gli utenti delle risorse a cui lo stesso si riferisce in quanto il suo rispetto rappresenta una garanzia di corretta gestione della sicurezza dei sistemi e dei dati personali.

In caso si riscontrino delle criticità che possano ledere la sicurezza del sistema informativo, S.C.R potrà verificare che l'utilizzo delle risorse strumentali concesse in dotazione agli utenti sia conforme alle indicazioni riportate nel presente disciplinare. Qualora l'utilizzo delle risorse fornite in dotazione possa in qualche maniera rivelare dati personali relativi agli utilizzatori, la rilevazione verrà effettuata secondo i principi di pertinenza e non eccedenza del trattamento dei dati rispetto alle finalità di sicurezza per cui tali dati sono trattati.

Il mancato rispetto da parte degli utenti di quanto descritto nel presente Regolamento potrà avere conseguenze di natura disciplinare o contrattuale in rapporto alla gravità del comportamento e dei potenziali rischi per il sistema e per i dati personali.

5 *Dati trattati attraverso le risorse informatiche concesse in dotazione*

Le risorse informatiche sono messe a disposizione dall'azienda per l'esercizio delle attività correlate alle finalità dell'azienda stessa, pertanto l'utilizzo degli strumenti in dotazione e il trattamento è di prevalente carattere professionale.

È consentito l'utilizzo per finalità proprie (cioè non afferenti alle attività professionali dell'azienda) della risorsa messa a disposizione a condizione che:

- venga effettuato al di fuori dell'orario di lavoro o dell'attività effettuata per conto dell'azienda;
- non sia contrario alle regole di condotta indicate nei paragrafi successivi e non possa in alcun modo ledere l'immagine dell'azienda;
- non danneggi in alcun modo, diretto o indiretto, le proprietà dell'azienda;
- non comporti alcuna violazione di leggi;
- sia esplicito verso terzi che la responsabilità di qualsiasi operazione svolta per finalità personali sia imputabile esclusivamente all'utente;
- non comprometta le misure di sicurezza e di protezione dei dati attuate e definite da questo regolamento o dalle politiche aziendali.

È importante precisare che è consentito l'utilizzo privato esclusivamente delle risorse strumentali ma non delle informazioni trattate per conto dell'azienda; non è in alcun modo consentito trattare dati di cui l'azienda è Titolare o Responsabile esterno del Trattamento se non per attività correlate con le finalità dell'azienda stessa.

È ammessa la custodia di dati privati sugli strumenti forniti in dotazione a condizione che:

- siano riposti in cartelle di cui sia esplicitamente indicata la privatezza del dato (es. cartelle con dicitura "personale");
- siano esplicitamente differenziabili dai dati trattati per attività strumentali al perseguimento delle finalità aziendali;
- vengano rimossi prima del rilascio o della riconsegna delle risorse fornite.

Alla riconsegna delle risorse da parte degli utenti all'azienda, questa potrà liberamente disporre dei dati ivi presenti. Eventuali dati di carattere privato ancora residenti al momento della riconsegna della postazione verranno trattati secondo i principi di pertinenza e non eccedenza previsti dalla normativa sulla protezione dei dati personali. La risorsa potrà essere ripristinata con valori predefiniti (o ripulita) ed assegnata ad altri soggetti.

L'azienda si riserva la facoltà di rimuovere tutti i dati presenti sulle risorse riconsegnate qualora si ritenga necessario per la riassegnazione della stessa.

6 *Utilizzo delle postazioni di lavoro*

La postazione di lavoro affidata agli utenti è uno **strumento di lavoro**. Ogni utilizzo non pertinente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza per cui va assolutamente evitato l'utilizzo improprio dello stesso.

Non è consentito installare programmi provenienti dall'esterno salvo preventiva autorizzazione degli Amministratori di Sistema debitamente incaricati, i quali, in rispondenza alle politiche di sicurezza aziendali ed alla normativa vigente, verificheranno l'opportunità (in termini di sicurezza dei sistemi) dell'installazione, onde evitare il grave pericolo di introdurre vulnerabilità, virus, nonché di alterare la stabilità delle applicazioni dell'elaboratore.

Non è consentito l'uso di programmi diversi da quelli messi a disposizione o autorizzati dall'azienda, in quanto l'inosservanza di questa disposizione, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre l'azienda a gravi responsabilità civili e penali in caso di violazione della normativa sulla tutela del diritto d'autore (Legge 633 del 22 aprile 1941 sulla tutela della proprietà intellettuale, D. Lgs. 518 del 29 dicembre 1992 sulla tutela giuridica del software e aggiornamenti successivi), che impone la presenza nel sistema di software provvisto di regolare licenza d'uso.

Gli utenti che sono eventualmente in possesso di privilegi amministrativi attraverso i quali hanno la possibilità di effettuare installazioni sulla postazione di lavoro, devono comunque richiedere l'autorizzazione ai Sistemi Informativi prima di procedere all'installazione. Solamente in casi eccezionali di motivata urgenza possono procedere all'installazione formalizzando l'autorizzazione successivamente. In questo caso le verifiche di sicurezza (virus, vulnerabilità, compatibilità con il sistema etc.) che normalmente vengono effettuate dai Sistemi Informativi prima dell'inserimento di un software del sistema informatico, dovranno essere effettuate da chi effettua l'installazione.

Le attrezzature vengono consegnate all'utente con una configurazione coerente con le misure organizzative e di sicurezza impostate dall'azienda: non è consentito all'utente modificare le caratteristiche impostate, salvo preventiva autorizzazione degli Amministratori di Sistema incaricati.

La postazione di lavoro deve essere spenta prima di lasciare la sede di lavoro o in caso di assenze prolungate dalla postazione, salvo specifica disposizione degli Amministratori di Sistema e/o a seguito di pianificazione dello spegnimento automatico. In ogni caso, poiché lasciare un sistema di elaborazione incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'uso indebito, l'utente che si allontana dalla postazione deve bloccarne l'uso tramite la combinazione dei tasti CTRL + ALT + CANC e successivo INVIO dopo la scelta dell'opzione che dispone il blocco del computer.

Il blocco dello schermo deve essere attivato con la richiesta di password per lo sblocco e deve partire automaticamente non oltre il tempo di 15 minuti di non utilizzo.

Ogni utente deve prestare la massima cautela nell'utilizzo dei supporti rimuovibili di origine esterna. Prima dell'apertura del supporto deve provvedere alla sua scansione tramite il software antivirus. L'utente deve avvertire immediatamente gli Amministratori di Sistema nel caso in cui vengano rilevate minacce dal sistema antivirus.

Non è consentito l'utilizzo di giochi o altre applicazioni di tipo ludico anche se comprese nel sistema operativo installato.

Non sono permesse, a meno di specifiche e documentate autorizzazioni le seguenti attività:

- caricare, memorizzare, pubblicare, diffondere, distribuire, tramite risorse aziendali documenti, informazioni, immagini, filmati ecc. in generale, ed in particolare:
    - a carattere violento, pornografico o contrario alla pubblica decenza, o suscettibile di mancare di rispetto agli esseri umani o alla loro dignità, con contenuto discriminatorio razziale ed etnico, contrario al buon costume, oltraggioso nei confronti dei minori, contrario all'ordine pubblico, diffamatorio o che contenga contenuti illeciti penalmente o civilmente riconducibili a categorie qui non espressamente indicate;
    - illeciti in base alla normativa sul diritto d'autore;
    - pregiudizievoli per le risorse aziendali e per l'integrità e la conservazione dei dati dell'azienda stessa;
    - pregiudizievoli per l'immagine e il buon nome dell'azienda anche all'esterno del ristretto contesto aziendale;
- accedere a server web trattanti materie o soggetti ricadenti nelle categorie sopra elencate;
- tenere comportamenti che possano indurre taluno ad effettuare invii di materiale rientrante nelle tipologie sopra elencate; laddove l'utente si trovi a ricevere anche contro il suo volere tali materiali, è tenuto a informare il personale dei Sistemi Informativi ed attenersi alle istruzioni impartite circa il trattamento di tali materiali;
- utilizzare le risorse aziendali con fini di molestia, minaccia o comunque violando le norme di legge in vigore;
- caricare, memorizzare, trasmettere o utilizzare programmi, software, procedure o altre utilità che siano protetti dalle leggi sulla proprietà intellettuale, a meno che l'azienda non ne detenga regolare licenza e/o autorizzazione del produttore;
- utilizzare strumentazioni, programmi, software, procedure, ecc. messi a disposizione dall'azienda in violazione delle leggi sulla proprietà intellettuale, delle regole di buona tecnica applicabili e delle prescrizioni emanate dall'azienda;
- caricare o trasmettere, con volontà, archivi o programmi contenenti virus o dati alterati;
- manomettere sistemi o archivi in maniera tale da inficiare la riservatezza, la disponibilità e/o l'integrità dei dati;
- inviare messaggi in massa ("spam") o favorire il propagarsi di notizie riconducibili a catene telematiche (c.d. "catene di S. Antonio");
- utilizzare le risorse aziendali in modo da consentire a soggetti non abilitati l'accesso ai dati e ad alle informazioni riservate, se non nei casi espressamente previsti dalla legge e/o da regolamenti interni.

Poiché alcune attività sopra elencate possono avere conseguenze di natura penale, esse originano in capo al trasgressore tutte le responsabilità previste dalla normativa vigente.

È ritenuto statisticamente probabile che l'utilizzo di applicazioni di comunicazione (internet, posta elettronica, ecc.) e di supporti rimovibili comporti la trasmissione di virus informatici o di programmi e archivi che in grado di alterare, distruggere o monitorare l'attività e i contenuti dei personal computer. La postazione viene fornita provvista di sistemi anti malware: l'utente deve verificare l'effettivo aggiornamento di tali sistemi.

In caso di anomalie dell'hardware e del software affidatogli, l'utente deve immediatamente bloccarne l'operatività, fermare le eventuali elaborazioni in corso ed informare immediatamente i Sistemi Informativi per le incombenze di competenza.

L'esecuzione automatica dei contenuti dinamici (es. macro) presenti nei file deve essere mantenuta disattivata.

7 *Utilizzo Notebook e altri dispositivi elaborativi portatili*

Ai dispositivi portatili si applicano le regole di utilizzo previste per le postazioni di lavoro connesse alla rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna.

Gli utenti di dispositivi portatili si impegnano, dovunque dovessero trovarsi, a mettere in sicurezza la strumentazione utilizzata e i dati nella stessa contenuta.

Danni arrecati alle attrezzature o la loro perdita dovuta ad incauta custodia saranno a carico dell'utente utilizzatore.

L'utente è responsabile delle attrezzature informatiche portatili assegnategli dall'azienda e deve custodirle con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

Il dispositivo non deve essere lasciato incustodito in zone a libero accesso, al fine di ridurre il rischio di furti. In caso di trasferte, il dispositivo non deve essere lasciato in macchina, nemmeno per brevi periodi, in parcheggi pubblici o comunque zone non custodite.

Qualora tali dispositivi dovessero essere smarriti o rubati, l'affidatario deve immediatamente segnalare l'evento agli Amministratori di sistema, al fine di approntare le necessarie misure di mitigazione del danno.

Ogni utente deve prestare la massima attenzione ai supporti di origine esterna. Prima dell'apertura del supporto deve provvedere alla sua scansione tramite il software antivirus. L'utente deve avvertire immediatamente gli Amministratori di Sistema nel caso in cui vengano rilevate minacce.

L'utente deve avvertire immediatamente i Sistemi Informativi nel caso in cui vengano rilevate minacce.

8 *Utilizzo dei supporti rimuovibili*

I supporti di memorizzazione rimuovibili attraverso i quali sono trattati dati dell'azienda devono essere utilizzati solo per attività lavorative.

Tutti i supporti esterni (cassette, secure drive, cd, dvd, dischi esterni USB, chiavette USB, SD cards, ecc…) contenenti dati personali trattati in ambito professionale devono essere utilizzati con particolare cautela onde evitare che il loro contenuto possa essere trattato da soggetti non autorizzati.

I dati personali salvati su supporti rimuovibili devono essere protetti tramite adeguati sistemi di cifratura, a tutela di possibili furti o smarrimenti.

I supporti contenenti dati personali, ancor più se sensibili e/o giudiziari, devono essere conservati con la massima attenzione da parte del personale che li utilizza: ogni eventuale conseguenza derivante dall'utilizzo inadeguato di detti supporti comporta una diretta responsabilità da parte dell'utilizzatore.

L'utente è responsabile dei supporti portatili assegnati dai Sistemi Informativi e deve custodirli con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

Possono essere utilizzati anche supporti rimuovibili privati, a condizione che, qualora su tali supporti si trattino dati di carattere professionale, si applichino le stesse cautele previsti per i supporti forniti dall'azienda, fra cui la cifratura dei dati e la custodia in sicurezza.

Ogni utente deve prestare la massima attenzione ai supporti di origine esterna. Prima dell'apertura del supporto deve provvedere alla sua scansione tramite il software antivirus. L'utente deve avvertire immediatamente i Sistemi Informativi nel caso in cui vengano rilevate minacce.

Occorre mantenere impostata la disattivazione dell'esecuzione automatica dei contenuti al momento della connessione dei dispositivi rimuovibili.

9 *Trasferimento dei media all'esterno dell'organizzazione*

I supporti magnetici contenenti dati personali o informazioni rilevanti non possono generalmente essere portati all'esterno delle sedi dell'organizzazione, all'interno della quale devono comunque essere custoditi con cautela. Qualora si renda necessario portare all'esterno supporti di memorizzazione contenenti dati personali o rilevanti, si dovranno valutare con i Sistemi Informativi le opportune misure atte a garantire la sicurezza dei dati.

10 Dismissione di media o dispositivi

In caso di necessità di dismissione di un apparato o strumento, lo stesso dovrà essere consegnato ai Sistemi Informativi che si occuperanno di effettuare una dismissione sicura dell'apparato rendendo illeggibili i dati contenuti e dismettendolo nella maniera corretta.

In caso di dismissione di DVD, chiavette USB o hard disk, questi potranno essere consegnati ai Sistemi Informativi o dismessi direttamente dall'utente assegnatario effettuando una dismissione sicura (illeggibilità e distruzione).

Nel caso di riutilizzo di un dispositivo, i Sistemi Informativi effettueranno la cancellazione dei dati precedentemente presenti prima di metterlo a disposizione per il nuovo utilizzo.

11 Dispositivi BYOD (Bring Your Own Device – BYOD)

È possibile utilizzare dispositivi di proprietà (Bring Your Own Device - BYOD) per trattare dati dell'azienda solo se tale utilizzo è compatibile con le procedure di sicurezza previste nel contesto aziendale e se preventivamente approvato dal rispettivo referente. Sul dispositivo dovranno essere applicate le medesime misure di sicurezza in uso per gli strumenti aziendali.

12 *Utilizzo della rete LAN e delle risorse condivise*

Al fine di garantire la disponibilità dei dati e un'efficace politica di backup, gli utenti che operano con postazioni fisse collegate alla LAN aziendale devono salvare su cartelle di rete tutti i file di lavoro ed astenersi dal salvarli sul disco locale della postazione di lavoro (si specifica che la cartella "desktop" si trova sulla postazione in locale, pertanto è inadatta al salvataggio dei file perché non sottoposta a procedure di backup).

È consentito conservare documenti di natura professionale sui dispositivi portatili dati in dotazione, con la consapevolezza che non sono sottoposti a procedure di backup e che pertanto la messa in sicurezza di tali dati è demandata agli utenti che hanno ricevuto tali attrezzature in dotazione.

Le cartelle/unità di rete sono aree di condivisione di 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.

Sulle cartelle/unità di rete vengono svolte regolari attività di amministrazione e backup secondo le politiche di configurazione e salvataggio definite al livello aziendale.

Le credenziali di ingresso alla rete ed ai programmi sono personali: è assolutamente vietato entrare nella rete e nei programmi con credenziali assegnate ad altri utenti.

Gli Amministratori di Sistema, nell'espletamento delle mansioni attribuite loro per l'esercizio delle proprie attività, possono in qualunque momento procedere alla rimozione di ogni file o applicazione che riterranno essere potenzialmente pericolosi per la sicurezza, sia sulle postazioni di lavoro sia sui server.

La struttura preposta alla gestione delle risorse umane dovrà comunicare ai Sistemi Informativi ogni variazione di carattere amministrativo ed organizzativo relativa al personale dell'azienda, al fine di consentire agli Amministratori di Sistema la creazione/modifica/cancellazione dei permessi di accesso alle risorse informatiche, affinché siano coerenti con le mansioni affidate al personale e il relativo trattamento dei dati. Allo stesso modo, i Sistemi Informativi coordineranno la consegna e il ritiro delle risorse informatiche.

Per la trasmissione di file all'interno dell'azienda è possibile utilizzare la posta elettronica, prestando attenzione alla dimensione degli allegati, oppure è possibile utilizzare le cartelle di scambio create a tale scopo. Le cartelle devono essere tenute in ordine, eliminando i file non più necessari anche al fine di non consentire il trattamento dei dati da parte di persone non espressamente autorizzate.

Gli utenti dovranno effettuare la stampa dei dati solo se strettamente necessaria e dovranno ritirarla prontamente dai vassoi delle stampanti nel caso di utilizzo di stampanti condivise.

È consentito il collegamento alla rete interna di personal computer portatili o di attrezzature informatiche non di proprietà aziendale, se disciplinato nelle modalità definite all'articolo precedente.

Gli utenti dovranno partecipare alla corretta gestione degli archivi informatici:

- verificando la coerenza delle cartelle con i trattamenti individuati a norma di legge;

verificando ed eventualmente variando, avvalendosi degli Amministratori di Sistema, le "permission" di accesso a tali risorse affinché siano coerenti con le autorizzazioni al trattamento dei dati.

13 Utilizzo di piattaforme in cloud di file sharing

È possibile utilizzare piattaforme di file sharing solo se facenti parte delle piattaforme consentite dai Sistemi Informativi o facenti parte della dotazione aziendale (es. Google Drive).

L'utilizzo di piattaforme alternative deve essere limitato allo stretto indispensabile ed autorizzato dagli Amministratori di Sistema o da soggetti incaricati dall'azienda del coordinamento di tali aspetti.

14 *Acquisizione software*

Sulle postazioni è consentita l'installazione esclusivamente delle seguenti categorie di software:

- software commerciale dotato di licenza d'uso (es. pacchetti di Office Automation);
- software gestionale acquisito specificatamente dall'azienda per lo svolgimento delle proprie mansioni lavorative (es. applicativi in uso ai vari servizi);
- software gratuito (freeware) e shareware prelevato dai siti internet, solo se espressamente autorizzato dai Sistemi Informativi;
- qualsiasi altro software si renda necessario per l'esercizio delle attività lavorative, provvisto di una licenza non in contrasto con la normativa sul diritto d'autore ed a seguito di autorizzazione da parte degli Amministratori di Sistema.

I Sistemi Informativi elaborano e mantengono un documento chiamato "Configurazione standard delle postazioni di lavoro" in cui sono indicati gli specifici software autorizzati e definiti come base per le postazioni di lavoro. Ogni ulteriore necessità dovrà essere valutata con i Sistemi Informativi al fine di individuare la soluzione applicativa che risolva le esigenze di attività lavorativa e non comprometta la sicurezza del sistema informatico e dei dati.

L'acquisto e la conseguente installazione di software devono essere sempre preventivamente valutati, autorizzati ed effettuati in collaborazione con i Sistemi Informativi, al fine di garantire la stabilità dei sistemi presenti e la compatibilità del software con gli stessi.

15 *Dispositivi con impatto sui sistemi informatici*

L'acquisizione di qualsiasi dispositivo o strumento che interagisca con la rete e/o la strumentazione informatica aziendale o possa avere un impatto con essi, qualora non venga eseguita direttamente dai Sistemi Informativi, deve essere concordata preventivamente con questi, onde evitare malfunzionamenti, cadute prestazionali o altri problemi alla sicurezza e all'immagine dell'azienda stessa.

Qualora nell'esercizio di attività aziendali sia prevista la fornitura di software accessorio, la struttura competente provvede a consultare i Sistemi Informativi nelle fasi preliminari del processo di acquisizione per la corretta definizione delle caratteristiche del software, al fine della verifica che esso risulti:

- compatibile con il sistema informatico preesistente,
- conforme alle misure di sicurezza adottate dall'azienda con particolare riguardo alla sicurezza degli accessi logici,
- certificato per l'installazione sulle macchine in dotazione (server e pc),
- installato correttamente.

In caso di mancata consultazione preventiva dei Sistemi Informativi non verrà effettuata alcuna installazione.

Qualora venga affidata all'esterno la gestione di dati aziendali per l'erogazione di servizi, l'ufficio competente deve concordare preventivamente con i Sistemi Informativi le modalità e i formati con cui questi dati devono essere scambiati, sia in ingresso che in uscita, e le condizioni di consegna dei dati al termine del rapporto di collaborazione.

16 Gestione delle password e degli accessi

L'utente deve utilizzare sempre una password ogni qualvolta sia richiesto, avendo cura che nessuno ne venga a conoscenza.

La password di ingresso al dominio aziendale viene attribuita dai Sistemi Informativi all'utente per il primo accesso. Dopo il primo accesso il sistema chiederà all'utente di modificare la password, la quale sarà conosciuta solo dall'utente stesso. Qualora si renda necessario (per manutenzione, aggiornamenti, assenza prolungata imprevista che renda indisponibili risorse gestite dall'utente) che gli Amministratori di Sistema debbano debba entrare nel sistema con il profilo dell'utente, la password di accesso dell'utente stesso verrà modificata. Al successivo accesso da parte dell'utente gli Amministratori gli rilasceranno una password di cortesia che verrà immediatamente modificata dall'utente stesso.

L'accesso agli applicativi e ai sistemi può a sua volta essere regolato da un'ulteriore password: le modalità di gestione e di scadenza di dette password sono specifiche per ogni ambiente. All'utente sarà fornito un profilo personale e verranno attivate procedure per garantire all'utente stesso la conoscenza esclusiva della propria password. Nel caso il sistema non lo consenta o sia necessario l'intervento degli Amministratori di Sistema per garantire la disponibilità dei dati, verranno concordate procedure specifiche per la gestione degli accessi.

La combinazione dell'accesso al dominio e agli applicativi garantirà la riservatezza dei dati personali e delle informazioni aziendali in conformità al GDPR ed al sistema di sicurezza delle informazioni aziendale.

Se le credenziali sono comunicate agli utenti tramite comunicazioni elettroniche, user-id e password non devono essere comunicate tramite lo stesso canale di comunicazione. Qualora i canali di comunicazione utilizzati siano entrambi consultabili tramite un dispositivo (es smartphone, notebook, tablet, ecc), tale dispositivo deve essere a sua volta protetto dall'accesso di soggetti terzi.

Le password del dominio e degli applicativi, salvo impossibilità dovute all'obsolescenza del software, devono essere modificate ogni 3 mesi, devono essere formate con un livello di complessità adeguato alla tipologia dei dati trattati e non devono contenere riferimenti agevolmente riconducibili all'utente.

Qualora l'utente utilizzi credenziali amministrative di un sistema o ambiente (applicativo o sistemistico) che tratti dati di altri soggetti, la password deve essere adeguata alle policy di sicurezza specificate per gli Amministratori di Sistema.

Nel caso in cui si sospetti che una password abbia perso la segretezza, l'utente provvederà ove possibile a modificarla personalmente oppure con il supporto di uno degli Amministratori di Sistema.

Non è consentito utilizzare il profilo personale di altri soggetti per accedere ai sistemi. Qualora l'utente venga a conoscenza delle password di un altro utente, è tenuto a darne immediata notizia all'utente stesso o a un Amministratore di sistema.

L'utente è tenuto ad assicurare la segretezza delle password utilizzate per attività lavorative, al fine di garantire la sicurezza dei dati e dei servizi utilizzati.

17 Attività di backup dei dati utente

Sono oggetto di attività di salvataggio centralizzato:

- i file salvati sulle cartelle/unità di rete messe a disposizione dai Sistemi Informativi secondo le politiche di backup definite a livello aziendale;
- le banche dati di applicativi ed i relativi file di sistema in uso per funzioni aziendali, secondo le politiche aziendali definite;
- il contenuto delle caselle di posta elettronica gestite all'interno della Gmail di Google, secondo le politiche di backup definite a livello aziendale;
- il contenuto delle cartelle Google Drive, secondo le politiche di backup definite a livello aziendale;
- il contenuto del calendario Google, secondo le politiche di backup definite a livello aziendale.

I dati che risiedono sulle postazioni di lavoro non sono soggetti a operazioni di backup centralizzato.

18 Attività e strumenti di assistenza remota

Per finalità di carattere manutentivo sono utilizzati presso l'azienda strumenti di assistenza remota che consentono agli Amministratori di Sistema di connettersi alle postazioni degli utenti per fornire supporto in tempo reale e assistere gli utenti nella risoluzione di problematiche di carattere informatico.

Gli strumenti utilizzati manifestano esplicitamente la connessione alla postazione da parte dell'Amministratore: l'utente dovrà consentire tramite autorizzazione verbale o informatica l'intervento remoto.

Qualora sia necessario consentire l'accesso e/o il controllo remoto da parte di soggetti esterni all'azienda per attività di carattere professionale, questo può essere fatto solo previa verifica dell'identità del soggetto che si connette alla risorsa e dell'effettiva necessità. Le attività effettuate da remoto devono essere monitorate durante il loro svolgimento. Qualora debba essere effettuato in orari di assenza del personale aziendale, prima di rilasciare l'accesso alla risorsa è necessario prendere dovute precauzioni al fine di ridurre l'accesso remoto solamente ai contesti per i quali si è reso necessario, senza che sia possibile per l'operatore remoto accedere, anche accidentalmente, ad altre informazioni.

19 *Posta elettronica*

La casella di posta elettronica, assegnata dall'azienda all'utente, è uno strumento esclusivo di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

Le caselle di posta aziendali possono essere utilizzate solo per finalità correlate alle attività aziendali, pertanto si assume che le informazioni veicolate tramite tale strumento non siano di carattere personale.

Qualsiasi attività istituzionale realizzata tramite utilizzo di posta elettronica deve essere svolta con l'esclusivo utilizzo di caselle registrate sotto il dominio di posta aziendale o tramite caselle di posta elettronica certificata registrate dall'azienda stessa. L'eventuale utilizzo di caselle non registrate sotto il dominio aziendale è consentito solo previa autorizzazione dei Sistemi Informativi: gli utilizzatori devono garantire il presidio di tali caselle e limitarne l'utilizzo allo stretto necessario.

È fatto divieto di utilizzare le caselle di posta elettronica aziendale per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mailing-list salvo diversa ed esplicita autorizzazione da parte dei Sistemi Informativi per esigenze di lavoro.

È inoltre da evitare ove possibile l'invio di messaggi con allegati di grandi dimensioni al fine di evitare eventuali sovraccarichi al sistema informatico e nuocere all'efficacia della comunicazione.

La casella di posta deve essere tenuta in ordine evitando contenuti inutili.

Per la trasmissione di file all'interno dell'azienda è possibile utilizzare la posta elettronica, prestando attenzione alla dimensione degli allegati, oppure è possibile utilizzare le cartelle di scambio create a tale scopo.

È vietato inviare mail con allegati i cui formati sono ritenuti pericolosi (es. estensione .exe, .bat, ecc.). I Sistemi Informativi potranno impostare attraverso sistemi hardware o software il blocco di invio o ricezione di un tipologie di file ritenute pericolose o non attinenti all'attività aziendale ai fini della protezione dei dati e dei sistemi informatici.

È vietato aderire a catene telematiche che richiedono la divulgazione e circolazione di messaggi di posta di carattere non lavorativo. Se si dovessero ricevere messaggi di tale tipo, si dovrà cancellare il messaggio ricevuto senza divulgarlo in alcun modo. Non si dovranno in alcun caso attivare gli allegati di tali messaggi.

Qualora si ricevessero messaggi sospetti di richiesta di password o altre informazioni oppure di invito a svolgere operazioni sulla propria postazione di lavoro (es. apertura o cancellazione di file, installazione aggiornamenti, ecc.) di cui non è certa la provenienza, l'utente è tenuto a verificarli e, nel caso lo ritenga necessario per attività di prevenzione, a segnalarli immediatamente ai Sistemi Informativi prima di effettuare qualsiasi azione.

Al fine di garantire la continuità di servizio, sono previste 2 differenti modalità per la gestione delle assenze, programmate o non, degli operatori preposti alla lettura dei messaggi di una specifica casella di posta:

1) ASSENZA PROGRAMMATA: attivazione da parte dell'utente di un risponditore automatico che segnali la temporanea indisponibilità all'accesso alla casella di posta, indicando eventualmente un indirizzo di posta alternativo a cui inviare il messaggio in caso di necessità di carattere professionale;
2) ASSENZA NON PROGRAMMATA: in caso di necessità, su specifica richiesta agli Amministratori di Sistema da parte del Responsabile dell'utente assente, quest'ultimo verrà contattato da un Amministratore il quale gli chiederà l'esplicito permesso verbale di accesso alla casella di posta elettronica. A seguito di tale assenso, l'Amministratore di Sistema provvederà ad inoltrare al

responsabile o ad un suo incaricato i messaggi di posta ritenuti necessari. In caso non sia stato possibile raggiungere l'utente assente, il suo responsabile autorizzerà l'Amministratore di Sistema all'accesso alla casella di posta dell'utente assente, richiedendo l'inoltro dei messaggi ritenuti necessari. Al termine dell'operazione, l'Amministratore di Sistema redigerà un rapporto dell'intervento effettuato, indicando il nominativo di colui che ha autorizzato l'accesso. Il rapporto verrà inviato all'utente assente, al suo responsabile e ai Sistemi Informativi.

È vietato utilizzare client di posta elettronica differenti da quelli installati e configurati dagli Amministratori di Sistema, a meno che la cosa non sia stata preventivamente concordata con i Sistemi Informativi. L'apertura automatica dei messaggi di posta elettronica deve essere disattivata.

Le caselle di posta elettronica in uso presso l'azienda sono di 2 tipologie:

1) caselle nominative, assegnate con la convenzione <*nome.cognome*>@scr.piemonte.it. Tali caselle sono intestate personalmente agli utenti: nonostante le caselle siano intestate ad un individuo, sono da considerarsi esclusivamente uno strumento aziendale e non corrispondenza privata; pertanto, l'utilizzo verso destinatari esterni dovrà essere corretto e coerente con le funzioni aziendali.

2) caselle di posta assegnate ad un ufficio o ad una struttura sul dominio @scr.piemonte.it. Tali caselle sono configurate per lo scambio di posta verso l'esterno e possono essere assegnate a più persone. La continuità nella gestione della corrispondenza e delle attività ad essa correlate dovrà essere assicurata dal Responsabile di competenza, o dai Sistemi Informativi, attraverso opportune scelte organizzative.

Gli Amministratori di Sistema, nell'espletamento delle loro funzioni, potranno accedere alle caselle di posta assegnate per finalità manutentive solo in presenza dell'assegnatario (o su sua esplicita autorizzazione) della casella o su richiesta del diretto superiore in caso di indisponibilità dell'assegnatario stesso.

Al termine del rapporto di collaborazione di volta in volta i Sistemi Informativi decideranno se:

- attivare sulla casella dell'utente non più operativo un risponditore automatico che segnalerà la cessazione del rapporto e indicherà un indirizzo alternativo aziendale da contattare in caso di necessità di carattere professionale. I messaggi di posta pervenuti verranno reindirizzati ad un'altra casella, al fine di garantire la continuità delle attività aziendali;
- chiudere direttamente l'account in modo che non possa più ricevere posta;

La casella di posta verrà chiusa definitivamente entro un anno, per garantire che eventuali rinnovi di servizi aziendali associati alla casella vengano adeguatamente reindirizzati.

20 *Navigazione Internet*

Per lo svolgimento delle proprie mansioni lavorative, è consentita la navigazione internet agli utenti.

La connessione ad Internet è uno strumento messo a disposizione per lavoro finalità correlate all'attività dell'azienda: è consentita la navigazione per motivi diversi da quelli strettamente legati all'attività aziendale stessa a condizione che:

- non venga effettuata in contemporanea con attività lavorative;
- non sia contraria alle regole di condotta indicate nel presente regolamento e non possa in alcun modo ledere l'immagine dell'azienda;
- non danneggi in alcun modo, diretto o indiretto, le proprietà dell'azienda;
- non comporti alcuna violazione di leggi;
- sia esplicito verso terzi che la responsabilità di qualsiasi operazione svolta per finalità personali sia imputabile esclusivamente all'utente.

Ogni utilizzo non inerente all'attività aziendale può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.

Pertanto, per garantire quanto previsto dalla normativa vigente, presso la sede aziendale è attivo un filtro che blocca l'accesso ai siti ritenuti palesemente non pertinenti con le attività aziendali o pericolosi per la sicurezza dei sistemi e dei dati personali.

Il filtro adottato utilizzerà sistemi di scarto di siti facenti parte di categorie appositamente selezionate. Qualora, per lo svolgimento della attività aziendali, un utente necessitasse di accedere a un sito scartato dai sistemi di filtraggio, potrà richiedere l'autorizzazione all'Amministratore di Sistema competente che provvederà a consentirne l'accesso, se ritenuto opportuno all'abilitazione di navigazione.

È fatto assoluto divieto all'utente lo scarico di software gratuito (freeware) e shareware prelevato dai siti internet, se non espressamente autorizzato dai Sistemi Informativi.

È tassativamente vietata ogni forma di registrazione e connessione a siti i cui contenuti non siano legati all'attività aziendale.

È vietata la partecipazione a Forum non professionali, l'utilizzo di chat line, di blog e di bacheche elettroniche, esclusi gli strumenti autorizzati per esigenze correlate all'attività aziendale.

A fini statistici, di qualità del servizio e di sicurezza, l'occupazione di banda generata dal traffico internet e dallo scambio di posta elettronica è soggetta a periodiche verifiche e controllo da parte dell'azienda sotto forma di dati aggregati ed anonimi, in osservanza dei limiti posti dalla legge in materia di protezione dei dati personali.

Qualora i sistemi di sicurezza segnalino delle potenziali criticità che possano minare l'integrità dei dati e la stabilità del sistema stesso, potrebbero essere effettuati dei controlli sulla navigazione internet effettuata tramite le reti aziendali. Tali controlli si opereranno secondo stadi successivi:

1) controlli generici sulle pagine visitate, senza che vengano tracciati gli utenti che le visitano;
2) controlli aggregati sulle pagine visitate con suddivisione del traffico effettuato per aree lavorative;
3) controlli specifici sulle pagine visitate, con tracciamento dell'indirizzo IP da cui si effettua la visita o dell'utente che la effettua.

I controlli aggregati e specifici verranno effettuati solo qualora i trattamenti generici non abbiano consentito di risolvere le criticità riscontrate e verranno comunque segnalati in forma preventiva agli utenti.

Tutti i dati di traffico internet sono comunque sottoposti a tracciamento da parte di sistemi automatici implementati presso l'azienda e custoditi per limitati periodi di tempo. La consultazione e conservazione di tali dati, al di fuori dei casi indicati precedentemente, è consentita:

- all'azienda per attività difensive ovvero per far valere o difendere un diritto in sede giudiziaria. Qualsiasi trattamento verrà svolto dall'azienda nel rispetto della libertà e della dignità dell'utente, in osservanza ai principi di pertinenza e non eccedenza;
- alle forze dell'ordine per attività di carattere ispettivo consentite dalla normativa sulla protezione dei dati delle persone fisiche.

21 Social Network

Non è consentito l'utilizzo di social network durante l'orario di lavoro, a meno che tali piattaforme non vengano espressamente impiegate in maniera strumentale per lo svolgimento delle proprie attività aziendali.

È assolutamente vietato esprimere opinioni personali relative all'azienda o ai suoi clienti, così come condividere informazioni e riferimenti di carattere professionale inerenti alle attività svolte. Tale divieto è da intendersi anche al di fuori dell'orario di lavoro ed eventualmente oltre la cessazione dell'attività svolta in S.C.R.

Per qualsiasi danno che potesse derivare all'immagine aziendale o dei clienti dell'azienda imputabile a comportamenti non conformi alle indicazioni sopra riportate, l'azienda si potrà rivalere direttamente sul soggetto che lo ha causato.

22 Crittografia

L'utilizzo di sistemi di crittografia sulle risorse tramite cui vengono trattati dati di carattere professionale deve essere concordato con gli Amministratori di Sistema, al fine di garantirne la conformità alle politiche di crittografia definite a livello aziendale.

Ogni attività di trasferimento verso l'interno e l'esterno dell'Ente di dati crittografati (sia tramite la connessione internet che tramite supporti fisici) dovrà essere concordata con i Sistemi Informativi.

S.C.R potrà effettuare verifiche sui sistemi e sulle attività di copia scarico, trasmissione dati e custodia, per verificare l'eventuale presenza di dati crittografati non preventivamente concordati.

23 Sicurezza generale e perimetrale

Presso l'azienda è attivato un sistema di sicurezza perimetrale a difesa dei sistemi e dei dati, che traccia eventi che possono essere indizio di minacce informatiche. Il sistema è soggetto a procedure di aggiornamento automatico per quanto riguarda la lista e le caratteristiche delle minacce.

È gestito da soggetti debitamente incaricati da S.C.R., i quali effettuano attività di verifica delle segnalazioni attivate dal sistema stesso, con lo scopo di comprendere e prevenire eventuali minacce esterne.

Qualora il sistema attivato rilevi delle minacce a specifici indirizzi IP interni delle postazioni di lavoro, il personale dei Sistemi Informativi verificherà le cause della minaccia rilevata insieme all'utente/utenti che abitualmente utilizza/utilizzano la postazione, con l'obiettivo di comprendere la natura dell'intrusione e prevenire eventuali danni.

Una volta individuate le cause dell'evento rilevato verranno adottati provvedimenti correttivi, con segnalazione al Titolare dei trattamenti di eventuali violazioni alle regole indicate nel presente disciplinare.

24 *Telefonia mobile*

I dispositivi di telefonia mobile forniti dall'azienda agli utenti costituiscono uno strumento di lavoro.

L'utente deve fare tutto ciò che è nelle sue facoltà per prevenire eventuali furti di dispositivi in dotazione, prestando cautela nella loro custodia.

Al fine di ridurre il rischio di accesso ai dati residenti sul cellulare da parte di soggetti non autorizzati, l'utente deve attivare sistemi di blocco schermo con protezione con password numerica o con segno grafico composto sullo schermo.

Deve inoltre essere attivato automaticamente il blocco dello schermo entro un massimo di 1 minuto di inattività.

A causa della sempre maggiore interazione tra i dispositivi telefonici e informatici, l'abuso di tali strumenti può costituire una potenziale fonte di minaccia ai sistemi aziendali. Pertanto è vietato:

- navigare su siti ritenuti non in linea con le indicazioni specificate nei precedenti capitoli relativi alla navigazione internet;
- installare applicazioni sui dispositivi cellulari assegnati dall'azienda senza prima aver concordato tale installazione con i Sistemi Informativi;
- installare sulle postazioni di lavoro in ufficio programmi di sincronizzazione/backup dei dati contenuti sui dispositivi cellulari potenzialmente dannosi senza la preventiva autorizzazione dei Sistemi Informativi.

In caso di disservizio o di problemi di funzionamento software, il personale dei Sistemi Informativi potrà effettuare dei controlli sulla configurazione dei programmi installati sul telefono concesso in uso con finalità di protezione del patrimonio aziendale. I controlli verranno effettuati nel rispetto della libertà e della dignità degli utenti; il trattamento di eventuali dati personali verrà effettuato nel rispetto dei principi di pertinenza e non eccedenza. Qualora si ravvisino installazioni di programmi il cui funzionamento potrebbe aver danneggiato il patrimonio aziendale, il fatto verrà segnalato all'azienda che valuterà l'eventuale adozione di provvedimenti disciplinari.

Al momento della restituzione dei dispositivi, il personale assegnatario dovrà cancellare eventuali contenuti personali sul cellulare (es. rubrica telefonica, SMS, contenuti multimediali, ecc).

App o informazioni di natura lavorativa che possono essere utili all'azienda dovranno essere lasciati a disposizione.

Qualora il dispositivo restituito contenga dati personali, questi verranno cancellati indiscriminatamente dal personale incaricato dall'azienda prima di un'eventuale assegnazione successiva.

25 Controlli

Le risorse messe a disposizione degli utenti sono strumenti attraverso i quali vengono perseguiti gli obiettivi aziendali, su cui l'azienda gode di diritti esclusivi di proprietà e utilizzo. Il datore di lavoro ha diritto di ottenere una corretta prestazione lavorativa e di attuare misure di sicurezza idonee alla difesa del patrimonio aziendale.

Sulle risorse messe a disposizione degli utenti potrebbero essere effettuati dei controlli, con le seguenti finalità:

- difendere il patrimonio aziendale;
- far valere o difendere un diritto in sede giudiziaria;
- tutelare gli interessi dei clienti che si affidano all'azienda per la messa in sicurezza dei propri sistemi.

A questi fini, è prevista la possibile attuazione dei seguenti controlli:

- verifica di files e programmi presenti sui dispositivi che possano contravvenire le indicazioni specificate nel presente disciplinare, con la finalità di prevenire eventuali reati;
- controllo della linea internet e dei sistemi perimetrali in caso di minacce segnalate dai sistemi di sicurezza o di lentezza di banda, con il fine di garantire il buon funzionamento della rete aziendale. Il controllo potrà riguardare l'occupazione di banda, l'utilizzo di sistemi di file sharing o la verifica di minacce segnalate dai sistemi di sicurezza;
- controllo della navigazione internet al fine di prevenzione di possibili minacce che possano compromettere la sicurezza dei sistemi aziendali. Il controllo verrà effettuato a seguito della rilevazione di eventi non conformi agli standard di buon funzionamento, e verrà effettuato con profondità graduale come specificato nel precedente capitolo dedicato alla navigazione internet;
- accesso alla casella di posta degli utenti in caso di loro assenza e di necessità di dovervi accedere per motivi di continuità dell'attività lavorativa. In caso di accesso alla casella di posta, verrà redatto un apposito rapporto di intervento in cui verranno specificate le azioni intraprese, che verrà consegnato all'utente al termine del periodo di assenza;
- analisi del cellulare aziendale, con finalità di controllo della spesa e protezione dei dati ivi presenti. Le modalità di controllo sono specificate nell'apposito capitolo relativo alla telefonia mobile;
- controllo dell'esito dei backup effettuati sui sistemi server aziendali, con la finalità di garantire l'eventuale ripristino di dati o documenti in caso di necessità. Le verifiche potrebbero riguardare il controllo dell'esito dei backup o il ripristino casuale di un dato durante le fasi di test di ripristino effettuate per esaminare il buon funzionamento del sistema;
- controllo della messa in sicurezza dei dati lavorativi residenti sui dispositivi dati in uso, con la finalità di garantire la riservatezza e la disponibilità dei dati aziendali. Tale controllo riguarderà la verifica della localizzazione dei dati in spazi logici criptati e di misure di backup.

Qualsiasi controllo verrà effettuato nel rispetto della libertà e delle dignità degli utenti. Eventuali dati personali rilevati saranno trattati nel rispetto dei principi di pertinenza e non eccedenza.

Qualora da tali controlli si rilevassero dei comportamenti non conformi rispetto a quanto indicato nel presente disciplinare e/o rispetto alle misure di sicurezza definite, l'azienda si riserva di intraprendere provvedimenti disciplinari.

A seguito di eventi che abbiano comportato un danneggiamento del patrimonio aziendale, qualora emergano degli elementi che potrebbero fondatamente evidenziare che dei comportamenti di un lavoratore possano aver potuto provocare tale danneggiamento, l'azienda ha diritto di attuare controlli difensivi occulti con la finalità tutelare le risorse in uso, se da essi fosse possibile riscontrare e sanzionare un comportamento idoneo improprio da parte degli utenti.

26 *Sistemi di monitoraggio attivo dei dispositivi e del software*

I dispositivi elettronici tracciano una serie di eventi di sistema per attività amministrative, manutentive e/o di sicurezza, che variano a seconda della tipologia dei dispositivi stessi.

Sono attivi specifici sistemi di monitoraggio di rete, server, personal computer, notebook, ecc. che premettono di ottenere informazioni sui sistemi e sul traffico generato dagli stessi al fine di monitorare il corretto funzionamento di tutto il sistema informativo, prevenire e correggere.

Tali sistemi effettuano il monitoraggio in maniera automatica e senza richiedere il consenso agli utenti delle postazioni monitorate.

Esempi di tali tipologie di monitoraggio sono:

- Rilevazione e inventario dispositivi hardware utilizzati
- Rilevazione e inventario dei software presenti sui dispositivi
- Analisi software presente sui dispositivi non compreso nell'elenco dei software autorizzati
- Sistemi di monitoraggio e alert in caso di anomalie del traffico di rete interna e funzionamento postazioni di lavoro
- Sistemi di installazione automatica sulle postazioni di lavoro di applicazioni ed aggiornamenti
- Filtraggio dei messaggi di posta elettronica con sistemi antispam o similari
- Filtraggio dei messaggi di posta elettronica per blocco tipologie di file ritenute pericolose
- Filtraggio e contenuti del traffico web per blocco tipologie di file ritenute pericolose
- Blocco di esecuzione di file ed applicativi ritenuti pericolosi attraverso il sistema di antivirus
- Raccolta log di sistemi operativi, applicativi, utility, sistemi di protezione
- Filtraggio e blocco siti web ritenuti non adeguati
- Filtraggio e segnalazione trasferimenti di files criptati non previsti
- Analisi ed identificazione delle vulnerabilità e dei sistemi
- Discovery di sistemi e attività che possano ledere la sicurezza delle risorse
- Tracciamento dati contabili relativi al traffico telefonico ed internet di smartphone e tablet.

Il servizio informatico potrà impostare attraverso sistemi hardware o software il blocco di invio o ricezione di un tipologie di file ritenute pericolose ai fini della protezione dei dati e dei sistemi informatici.

Per quanto riguarda i controlli che potrebbero essere svolti sulla navigazione internet degli utenti si rimanda al precedente capitolo dedicato al tema.

27 Gestione chiavi e altri strumenti di accesso fisico

Per lo svolgimento delle proprie attività professionali, gli utenti potranno essere dotati di chiavi o altri strumenti di accesso fisico (smartcard, dispositivi OTP, chiavi RFID, codici alfanumerici) a risorse aziendali.

Gli utenti sono tenuti ad utilizzare tali strumenti con la massima cautela, garantendone la messa in sicurezza. Tali strumenti non devono essere lasciati incustoditi in zone a libero accesso, al fine di ridurre il rischio di furti. In caso di trasferte, non devono essere lasciati in macchina, nemmeno per brevi periodi, in parcheggi pubblici o comunque zone non custodite.

Qualora tali strumenti dovessero essere smarriti o rubati, l'affidatario deve immediatamente segnalare l'evento ai Sistemi Informativi, al fine di approntare le necessarie misure di mitigazione del danno.

28 Rapporto con soggetti terzi

Prima di rilasciare documenti e dati informatici o credenziali a soggetti terzi, occorre verificare l'identità dei destinatari e la presenza di adeguate motivazioni ed autorizzazioni al rilascio.

Non è consentito fornire tramite email, fax, accesso remoto o telefonicamente dati, credenziali o accessi ai sistemi senza specifica e preventiva identificazione del richiedente e conseguente autorizzazione.

In caso di richieste di informazioni o documenti occorre confrontarsi prontamente con i Sistemi Informativi sul da farsi.

Qualora le informazioni e le risorse vengano trattate in nome e per conto di soggetti terzi (Titolari del trattamento), per cui S.C.R agisca in qualità di Responsabile ai sensi dell'art. 28 GDPR, S.C.R. dovrà concordare con il referente del Titolare le azioni da intraprendere.

29 *Incidenti di sicurezza e Data Breach*

Un qualsiasi incidente, occorso su documenti e dati informatici o credenziali di accesso, può compromettere la sicurezza dei dati personali e in generale delle informazioni.

In caso di particolare gravità, l'incidente può comportare una vera e propria violazione, denominata *data breach*, che è obbligatorio notificare all'Autorità Garante dei dati personali ai sensi dell'art. 34 del GDPR.

Si riporta di seguito un elenco, esemplificativo ma non esaustivo, di tipologie di data breach:

- Distruzione (dati non più disponibili)
- Perdita (dati non disponibili per il Titolare ma probabilmente in possesso di altri soggetti
- Modifica (senza possibilità di ripristino)
- Divulgazione non autorizzata
- Accesso non autorizzato
- Indisponibilità temporanea del dato

Qualora si riscontri un incidente di sicurezza sulle risorse in dotazione a personale S.C.R, è necessario comunicarlo immediatamente al proprio superiore e scrivere una email a rpd@scr. piemonte.it, documentando l'accaduto, al fine di approntare prontamente adeguate misure di mitigazione del danno. Eventuali procedure di gestione degli incidenti, generali o specificamente dedicate a particolari contenti, saranno rese disponibili nella intranet aziendale.

30 Osservanza delle regole relative alla normativa in tema di protezione dei dati personali e agli standard aziendali

Oltre a quanto indicato nel presente documento, è obbligatorio tenere comportamenti conformi alla normativa in tema di protezione dei dati personali e a tutti i regolamenti aziendali.

In particolare per quanto riguarda i contesti operativi di propria competenza, gli utenti sono tenuti a fare quanto nelle loro possibilità per l'adozione di adeguate misure di sicurezza, ai sensi dell'art. 32 del GDPR.

Qualora, nell'ambito delle proprie attività lavorative, un soggetto riscontri che il trattamento di dati effettuato in qualche modo possa contravvenire alle prescrizioni del GDPR o del D. Lgs. 196/2003 e s.m.i. ("Codice della Privacy"), è tenuto ad informarne prontamente i Sistemi Informativi al fine di concordare ed intraprendere i necessari interventi di adeguamento.

31 Segretezza delle informazioni

L'attività svolta potrebbe comportare la conoscenza incidentale di dati personali di cui S.C.R è Titolare o Responsabile esterno del trattamento. È pertanto necessario improntare le attività mantenendo la massima riservatezza sulle informazioni di cui si potrebbe venire a conoscenza.

L'impegno alla riservatezza dovrà essere osservato anche in seguito a modifica dell'incarico conferito e/o cessazione del rapporto di lavoro.