COMUNE DI SERLE

Disciplinare di utilizzo risorse informatiche e di trattamento dei dati

Revisione: 1; Data: 05/06/2020

MODIFICHE ED INTEGRAZIONI

Revisione/ data	Modifiche apportate	Approvazione
05/06/2020	Modifiche sommarie e commenti	
13/08/2020	Versione definitiva	OK

1. Premessa

La progressiva diffusione delle nuove tecnologie informatiche, ed in particolare il libero accesso alla rete tramite i personal computer, espone le organizzazioni a rischi di un coinvolgimento sia patrimoniale sia penale, creando problemi alla sicurezza e all'immagine.

L'utilizzo delle risorse informatiche e telematiche deve sempre ispirarsi al principio di diligenza e correttezza, atteggiamenti questi destinati a sorreggere ogni atto o comportamento posto in essere nell'ambito dell'attività svolta dall'organizzazione.

Le attrezzature informatiche, i relativi programmi e/o applicazioni, i dati e documenti affidati in uso agli utenti sono strumenti di lavoro, di cui l'organizzazione 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'organizzazione stessa.

Quanto indicato nel presente disciplinare rappresenta istruzioni operative che permettono di effettuare una gestione dei sistemi a garanzia della sicurezza delle informazioni in conformità a quanto richiesto dal Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (da ora in poi RGPD).

2. Scopo e campo di applicazione

Alla luce di quanto premesso, l'organizzazione adotta il presente disciplinare al fine di:

- evitare comportamenti inconsapevoli che possano innescare problemi o minacce alla sicurezza nel trattamento dei dati;
- informare i soggetti che trattano dati con le risorse informatiche di quali sono le misure di tipo organizzativo e tecnologico adottate all'interno dell'organizzazione 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'organizzazione potrebbe effettuare sulle risorse messe a disposizione;
- 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 documento si applicano a tutto l'insieme delle risorse informative, elettroniche, di comunicazione, di archiviazione, audiovisive, cartacee e a qualsiasi altra tipologia di risorsa utilizzata per perseguire le finalità istituzionali, siano esse di proprietà dell'organizzazione che di soggetti che operano in nome e per conto di essa.

Nel caso di soggetti esterni designati dall'ente 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

ORGANIZZAZIONE: è la persona giuridica che adotta il presente documento, al fine di disciplinare l'utilizzo delle risorse informative, elettroniche, di comunicazione, di archiviazione, audiovisive, cartacee all'interno del proprio perimetro organizzativo e operativo di competenza.

TITOLARE DEL TRATTAMENTO DEI DATI: è la figura individuata dall'art. 4 RGPD, definita come la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri soggetti, 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 e/o autorizza tutte le altre figure coinvolte nel trattamento dei dati. In questo specifico contesto è rappresentato dall'organizzazione che adotta il presente documento, ad eccezione di specifiche e definite circostanze in cui l'organizzazione agisce come responsabile del trattamento dei dati.

SISTEMI INFORMATIVI: è l'abbreviazione della struttura preposta alla gestione, alla configurazione, al coordinamento e al rilascio delle risorse informatiche dell'organizzazione, a cui fanno riferimento gli Amministratori di Sistema competenti per tale contesto. Quando tale struttura è esterna all'organizzazione, essa svolge le proprie attività in nome e per conto di essa, agendo in qualità di responsabile del trattamento dei dati ai sensi dell'art. 28 RGPD.

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'organizzazione: per le finalità del seguente documento si intendono gli Amministratori di Sistema preposti alla gestione delle risorse informatiche del Titolare, siano essi interni o esterni.

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.

UTENTI: sono i soggetti destinatari del presente disciplinare, a cui sono assegnate le risorse informatiche del Titolare. Possono essere dipendenti, collaboratori o altri soggetti a cui le risorse sono assegnate per lo svolgimento di attività correlate alle finalità perseguite dal Titolare.

DATO PERSONALE: qualsiasi informazione che possa ricondurre, in forma diretta o indiretta, ad una persona fisica identificata o identificabile. Se non diversamente espresso, il dato personale è sempre quello trattato dagli utenti esclusivamente per attività correlate alle proprie funzioni all'interno dell'organizzazione di riferimento.

DATO PRIVATO: qualsiasi informazione afferente ad utenti, non correlata alle funzioni da essi svolte nell'organizzazione di riferimento; tale contesto di riferimento non è pertinente o strumentale alle attività istituzionali del Titolare.

DATO PROFESSIONALE: qualsiasi informazione trattata dagli utenti nello svolgimento delle proprie attività e funzioni esercitate nell'organizzazione del Titolare.

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 disciplinare.

DISPOSITIVO: qualsiasi strumento di elaborazione elettronica utilizzato per lo svolgimento delle attività che fanno capo all'organizzazione, il cui utilizzo rientra nel perimetro di competenza del presente disciplinare. Rientrano in tale definizione, a titolo esemplificativo e non esaustivo, desktop computer, notebook, tablet, ecc.

SUPPORTO DI ARCHIVIAZIONE: qualsiasi supporto elettronico destinato all'archiviazione e la custodia dei dati, come ad esempio chiavette USB, hard disk esterni, CD e DVD, ecc.

RGPD: viene così definito nel presente documento il Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

4. Obbligo di rispetto del presente disciplinare

Il rispetto del presente disciplinare è un obbligo per tutti coloro che utilizzano le risorse dell'organizzazione, in quanto rappresenta una garanzia di corretta gestione della sicurezza dei sistemi e dei dati personali.

Il mancato rispetto di quanto descritto dal presente disciplinare rappresenta una mancanza che potrà avere conseguenze di natura disciplinare o contrattuale – oltre che di potenziale rilevanza amministrativa o penale - 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'organizzazione per l'esercizio delle attività correlate alle finalità istituzionali, pertanto l'utilizzo degli strumenti in dotazione e il trattamento è di prevalente carattere professionale.

E' consentito l'utilizzo per finalità proprie (cioè non afferenti alle attività istituzionali) delle risorse messe a disposizione a condizione che:

- si attenga esclusivamente alle prescrizioni indicate nei successivi capitoli, per cui sono definiti specifici limiti definiti per ogni tipologia di risorsa;
- venga effettuato al di fuori dell'orario di lavoro o dell'attività effettuata per conto dell'organizzazione;
- non sia contrario alle regole di condotta indicate nei paragrafi successivi e non possa in alcun modo ledere l'immagine dell'organizzazione;
- non danneggi in alcun modo, diretto o indiretto, le proprietà dell'organizzazione;
- 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 disciplinare o dalle politiche di sicurezza dell'organizzazione.

E' importante precisare che è consentito l'utilizzo privato esclusivamente delle risorse strumentali ma non delle informazioni trattate per conto del Titolare; non è in alcun modo consentito trattare dati di cui l'organizzazione è Titolare del trattamento (o, in casi specificamente, responsabile del trattamento) se non per attività strumentali al perseguimento delle finalità istituzionali dell'organizzazione.

E' 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 istituzionali;
- vengano rimossi prima del rilascio o della riconsegna delle risorse fornite;
- non siano in alcun modo riposti su sistemi server e/o altre risorse di archiviazione fruibili attraverso condivisioni di rete.

Alla riconsegna delle risorse da parte degli utenti all'organizzazione, questa potrà liberamente disporre dei dati ivi presenti. Eventuali dati di carattere privato ancora residenti al momento della riconsegna della risorsa 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'organizzazione 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 dell'ente 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 del dispositivo.

Non è consentito l'uso di programmi diversi da quelli messi a disposizione o autorizzati dall'organizzazione, in quanto l'inosservanza di questa disposizione, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre l'organizzazione 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 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 agli utenti con una configurazione coerente con le misure organizzative e di sicurezza impostate dall'organizzazione: non è loro consentito 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 sede, salvo specifica disposizione dell'Amministratore di Sistema o per espresse e specifiche contingenze che rendano necessario, in via del tutto eccezionale, derogare a tale prescrizione. 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 lascia incustodita la postazione accesa 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'accesso alle risorse contenute nel supporto deve provvedere alla sua

scansione tramite il software antivirus. L'utente deve avvertire immediatamente l'Amministratore 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 dell'organizzazione documenti, informazioni, immagini, filmati etc. 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 dell'organizzazione e per l'integrità e la conservazione dei dati dell'organizzazione stessa;
    - pregiudizievoli per l'immagine e il buon nome dell'organizzazione anche all'esterno del ristretto contesto dell'organizzazione stessa;
- 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 riceva - anche involontariamente - 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 dell'organizzazione con fini di molestia, minaccia o comunque violando le norme di legge in vigore;
- caricare, memorizzare, trasmettere o utilizzare programmi, software, procedure od altra utilità che siano protetti dalle leggi sulla proprietà intellettuale, a meno che l'organizzazione non ne detenga regolare licenza e/o autorizzazione del produttore;
- utilizzare strumentazioni, programmi, software, procedure, etc. messi a disposizione dall' organizzazione in violazione delle leggi sulla proprietà intellettuale, delle regole di buona condotta applicabili e delle prescrizioni emanate dall'organizzazione;
- 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 ciò che abitualmente viene definito "catena di S. Antonio";
- utilizzare le risorse dell' organizzazione 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.

E' ritenuto statisticamente probabile che l'utilizzo di applicazioni di comunicazione (internet, posta elettronica, etc.) e di supporti rimovibili comporti la trasmissione di virus informatici o di programmi e archivi in grado di alterare, distruggere o monitorare l'attività e i contenuti dei personal computer. La postazione viene fornita provvista di sistemi antimalware: 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 i personal computer connessi alla rete.

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

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

L'utente è responsabile delle attrezzature informatiche portatili assegnategli dall'organizzazione e deve custodirle con diligenza, sia durante gli spostamenti sia durante l'utilizzo presso i luoghi 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 in zone non custodite.

Qualora tali dispositivi dovessero essere smarriti o rubati, l'affidatario deve immediatamente segnalare l'evento all'Amministratore 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 l'Amministratore di Sistema ed i Sistemi Informativi nel caso in cui vengano rilevate minacce.

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

Nei casi in cui i dispositivi portatili siano di utilizzo condiviso e vengano messi a disposizione per attività episodiche (es. trasferte, presentazioni, meeting, etc.), l'utente deve considerare che tali risorse saranno messe a disposizione di altri utenti in momenti successivi, pertanto deve tassativamente rimuovere qualsiasi contenuto elaborato sui dispositivi prima della riconsegna, al fine di evitare incontrollate diffusioni di dati.

E’ in ogni caso tassativo rimuovere eventuali dati personali prima della riconsegna dei dispositivi.

8. Accesso remoto alle risorse informatiche dell’organizzazione

In caso sia necessario consentire ad un utente l’accesso remoto alle risorse informative, questo deve essere preventivamente concordato con i Sistemi Informativi e deve attenersi ad eventuali disposizioni regolamentari già adottate dall’organizzazione.

9. Utilizzo dei supporti rimuovibili

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

Tutti i supporti esterni (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 e deve custodirli con diligenza sia durante gli spostamenti sia durante l’utilizzo nel luogo di lavoro.

E' vietato l’utilizzo promiscuo di supporti per la custodia di dati privati e professionali: qualora un supporto sia dedicato alla custodia di dati afferenti all’organizzazione di riferimento, non può essere utilizzato per custodire anche dati privati. Analogamente, un supporto dedicato alla custodia di dati privati non può essere utilizzato anche per dati di carattere professionale afferente all’organizzazione di riferimento.

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.

10. Trasferimento dei supporti di memorizzazione all'esterno dell'organizzazione

I supporti informatici di memorizzazione 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 di particolare rilevanza, si dovranno valutare con i Sistemi Informativi le opportune misure atte a garantire la sicurezza dei dati.

L'assegnazione di risorse per l'accesso remoto ai sistemi deve essere adeguatamente tracciato, al fine di garantire idonee misure tecniche e organizzative di sicurezza.

11. Dismissione di dispositivi o supporti

In caso di necessità di dismissione di un dispositivo messo a disposizione dell'organizzazione, lo stesso dovrà essere preso in carico dai Sistemi Informativi che si occuperanno di effettuare una dismissione sicura dello strumento rendendo illeggibili i dati contenuti e dismettendolo nella maniera corretta.

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.

In caso di dismissione di supporti di memorizzazione contenenti dati afferenti all'organizzazione di riferimento, l'utente è tenuto a fare in modo che i dati ivi contenuti non siano in alcun modo intelliggibili, tramite distruzione fisica dei supporti o cancellazione a basso livello dei documenti contenuti, in modo da garantire l'impossibilità di ricostruire i dati.

12. Trattamento di dati tramite dispositivi di proprietà

Qualora, durante lo svolgimento di attività correlate alle funzioni svolte per conto del Titolare, gli utenti acquisiscano dati attraverso dispositivi di proprietà (ad esempio immagini, fotografie, filmati, registrazioni audio, documenti, ecc acquisite dagli utenti tramite smartphones o tablet di proprietà e traferiti o comunicati tramite sistemi di messaggistica on line), l'utente deve rimuoverli quanto prima degli archivi del proprio dispositivo, onde evitare che lo smarrimento o il furto dello stesso possa mettere a disposizione di soggetti non autorizzati dati personali trattati per conto del Titolare.

Qualora delle caselle di posta elettronica del Titolare siano consultate tramite un dispositivo privato, è obbligatorio bloccare lo stesso tramite sistemi di blocco schermo con protezione con password numerica, con segno grafico composto sullo schermo o tramite riconoscimento dell'impronta digitale.

In caso di smarrimento o furto di un dispositivo contenente dati personali trattati per conto dell'ente, è necessario segnalare immediatamente la circostanza ai Sistemi Informativi, al fine di valutare eventuali azioni di mitigazione del danno.

13. Dispositivi BYOD (Bring Your Own Device – BYOD)

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

Per garantire l'utilizzo in sicurezza di tali strumenti potranno essere previste specifiche procedure e istruzioni per l'uso ad integrazione del presente disciplinare.

14. 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 dell'organizzazione 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" sulla propria postazione di lavoro si trova in ambiente locale, pertanto è inadatta al salvataggio dei file perché non sottoposta a procedure di backup).

E' 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 strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto qualunque file privato 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 a livello organizzativo.

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

L'Amministratore di Sistema, nell'espletamento delle mansioni attribuitegli per l'esercizio delle proprie attività, può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere potenzialmente pericolosi per la sicurezza, sia sulle postazioni di lavoro sia sui server.

L'ufficio Personale dell'organizzazione dovrà comunicare ai Sistemi Informativi ogni variazione di carattere amministrativo relativa al personale dell'organizzazione, 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 agli utenti e il relativo trattamento dei dati.

In caso si rilevino variazioni di tipo organizzativo non opportunamente segnalate, i Sistemi Informativi provvederanno ad adottare opportune misure organizzative, in collaborazione

con gli uffici coinvolti con cui si verificherà la variazione riscontrata, per garantire il corretto accesso alle informazioni (modifiche dei permessi di accesso, eventuali disabilitazioni degli utenti, ecc).

Per la trasmissione di file all'interno dell'organizzazione 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.

E' consentito il collegamento alla rete interna di personal computer portatili o di attrezzature informatiche non di proprietà dell'organizzazione, solo se espressamente concordato con i Sistemi Informativi.

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 dell'Amministratore di Sistema, i permessi di accesso a tali risorse affinché siano coerenti con le autorizzazioni al trattamento dei dati.

15. Utilizzo di piattaforme in cloud di file sharing

I Sistemi Informativi mettono a disposizione un ambiente di file sharing per la condivisione di dati e documenti. Gli utenti devono attenersi all'esclusivo utilizzo di tale ambiente, astenendosi dall'utilizzo di strumenti alternativi non contrattualmente regolamentati.

Per qualsiasi necessità relativa a tale ambito gli utenti devono rivolgersi al personale dei Sistemi Informativi al fine di allestire una soluzione adeguata alle necessità riscontrate.

16. 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'organizzazione 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 dei Sistemi Informativi.

I Sistemi Informativi configurano e rendono disponibili le attrezzature assegnate agli utenti con configurazioni idonee a garantire la sicurezza dei sistemi ed adeguate alle necessità

rilevate dall'organizzazione per gli utenti. Ogni ulteriore necessità dovrà essere valutata con i Sistemi Informativi al fine di individuare la soluzione applicativa che soddisfi 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.

17. Dispositivi con impatto sui sistemi informatici

La messa in opera di qualsiasi dispositivo o strumento che interagisca con la rete e/o la strumentazione informatica dell'organizzazione 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'organizzazione stessa.

Qualora nell'esercizio di attività istituzionali sia prevista la fornitura di software accessorio, l'unità organizzativa 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'organizzazione 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 potrà essere garantito il supporto.

Qualora venga affidata all'esterno la gestione di dati dell'organizzazione 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.

18. 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 dell'organizzazione 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 un Amministratore 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, l'Amministratore gli rilascerà 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 dell'Amministratore 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 dell'ente in conformità al RGPD ed al sistema di sicurezza delle informazioni dell'ente stesso.

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, devono essere modificate ogni 3 mesi, devono essere formate da almeno una maiuscola, una minuscola, un carattere numerico e un carattere speciale ($,*,% ecc); devono avere una lunghezza di almeno 8 caratteri e non devono contenere riferimenti agevolmente riconducibili all'incaricato.

Complessità, lunghezza e scadenza possono variare per i vari ambienti di lavoro e sono specifiche per ogni ambiente. I Sistemi Informativi impostano le politiche di gestione delle password in ottemperanza agli obblighi di legge e tenendo conto della necessità di garantire adeguate misure di sicurezza delle informazioni.

Qualora l'utente utilizzi credenziali amministrative di un sistema o ambiente (applicativo o sistemistico) che tratti dati di altri soggetti, la password deve essere di almeno 14 caratteri.

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.

19. 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 organizzativo;
- le banche dati di applicativi ed i relativi file di sistema in uso per funzioni istituzionali, secondo le politiche di sicurezza definite;

- il contenuto delle caselle di posta elettronica gestite all'interno della piattaforma utilizzata dall'organizzazione, secondo le politiche di backup definite a livello organizzativo;
- il contenuto delle cartelle di rete assegnate agli utenti, secondo le politiche di backup definite a livello organizzativo.

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

20. Attività e strumenti di assistenza remota

Per finalità di carattere manutentivo sono utilizzati, sui dispositivi in dotazione, 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'organizzazione e ai tecnici dei Sistemi Informativi 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 dell'organizzazione, 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.

21. Posta elettronica

La casella di posta elettronica, assegnata dall'organizzazione 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 assegnate possono essere utilizzate solo per finalità correlate alle attività istituzionali, pertanto si assume che le informazioni veicolate tramite tale strumento non siano di carattere privato.

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

E’ fatto divieto di utilizzare le caselle di posta elettronica dell’organizzazione per l’invio di messaggi privati o per la partecipazione a dibattiti, forum o mailing-list salvo diversa ed esplicita autorizzazione da parte dei Sistemi Informativi per esigenze professionali.

E’ 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’organizzazione è possibile utilizzare la posta elettronica, prestando attenzione alla dimensione degli allegati, oppure è possibile utilizzare le cartelle di scambio create a tale scopo.

E’ vietato inviare email con allegati i cui formati sono ritenuti pericolosi (es. estensione .exe, .bat, etc.). 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 istituzionale ai fini della protezione dei dati e dei sistemi informatici.

E’ vietato aderire a catene telematiche (o di S. Antonio) che richiedono la divulgazione e circolazione di messaggi di posta di carattere non professionale. 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, apertura di una pagina web che richieda l’inserimento di credenziali, 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 da parte del responsabile dell’utente assente, quest’ultimo verrà contattato da un Amministratore di Sistema 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 comunicato all’utente assente, al suo responsabile e ai Sistemi Informativi.

E’ vietato utilizzare client di posta elettronica differenti da quelli installati e configurati dall’Amministratore 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'organizzazione sono di 2 tipologie:

1) caselle nominative. Tali caselle sono intestate personalmente agli utenti: nonostante le caselle siano intestate ad un individuo, sono da considerarsi esclusivamente uno strumento professionale e non corrispondenza privata; pertanto, l'utilizzo verso destinatari esterni dovrà essere corretto e coerente con le funzioni istituzionali.
2) caselle di posta assegnate ad un ufficio o ad una funzione sul dominio dell'organizzazione. 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.

E' fondamentale rilevare che l'utilizzo della casella di posta elettronica è strumentale all'attività istituzionale dell'organizzazione, ma non è il canale ufficiale per le comunicazioni che impegnino l'organizzazione verso terzi. Per tutti quei procedimenti aventi rilevanza esterna, le comunicazioni dovranno essere veicolate attraverso canali collegati al protocollo informatico dell'organizzazione, come la posta elettronica certificata istituzionale.

Al termine del rapporto intercorso fra l'utente e l'organizzazione, sulle caselle di posta nominative verrà attivato un risponditore automatico che segnalerà la cessazione del rapporto e indicherà un indirizzo alternativo nel dominio dell'organizzazione da contattare in caso di necessità di carattere professionale. La casella non sarà oggetto di consultazione, salvo che sia espressamente richiesto per finalità di continuità di servizio dell'organizzazione. In tal caso, l'accesso dovrà essere adeguatamente motivato ed espressamente autorizzato dal responsabile dell'utente; il trattamento effettuato dovrà essere documentato.

La casella di posta verrà chiusa definitivamente entro un periodo di sei mesi, per garantire che eventuali comunicazioni su rinnovi automatici di servizi associati alla casella vengano adeguatamente reindirizzati. Al termine di tale periodo il i Sistemi Informativi potranno procedere alla cancellazione dell'utenza.

In caso di situazioni di contenzioso o di precontenzioso tra l'utente e l'organizzazione, il contenuto della casella potrà essere conservato per tutta la durata del correlato procedimento, fino alla conclusione di tutti i gradi di giudizio.

22. 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 finalità correlate all'attività dell'organizzazione: è consentita la navigazione per motivi diversi da quelli strettamente legati all'attività istituzionale a condizione che:

- non venga effettuata in contemporanea con attività lavorative;
- non sia contraria alle regole di condotta indicate nel presente disciplinare e non possa in alcun modo ledere l'immagine dell'organizzazione;
- non danneggi in alcun modo, diretto o indiretto, le proprietà dell'organizzazione;
- non comporti alcuna violazione di normei;
- 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 istituzionale può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.

Pertanto, per garantire quanto previsto dalla normativa vigente, presso il sistema informativo dell'organizzazione è attivo un filtro che blocca l'accesso ai siti ritenuti palesemente non pertinenti con le attività istituzionali 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 istituzionali, un utente necessitasse di accedere a un sito scartato dai sistemi di filtraggio, potrà richiedere l'autorizzazione ai Sistemi Informativi che provvederanno a consentirne l'accesso, se ritenuto opportuno.

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

Sugli ambienti di lavoro virtuali tassativamente vietata ogni forma di registrazione e connessione a siti i cui contenuti non siano legati all'attività istituzionale utilizzando credenziali e caselle di posta assegnate dall'organizzazione.

E' 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 istituzionale.

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 controlli da parte dell'organizzazione sotto forma di dati aggregati ed anonimi, in osservanza dei limiti posti dalle normative 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 la rete dell'organizzazione. 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'organizzazione e custoditi per limitati periodi di tempo. La consultazione e conservazione di tali dati, al di fuori dei casi indicati precedentemente, è consentita:

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

23. 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 correlate alle finalità perseguite dal Titolare.

E' assolutamente vietato esprimere opinioni personali relative all'organizzazione, così come condividere informazioni e riferimenti inerenti alle attività svolte per conto dell'organizzazione. Tale divieto è da intendersi anche al di fuori dell'orario di lavoro ed eventualmente oltre la cessazione dell'attività svolta presso l'organizzazione.

Per qualsiasi danno che potesse derivare all'immagine dell'organizzazione imputabile a comportamenti non conformi alle indicazioni sopra riportate, essa si potrà rivalere direttamente sul soggetto che lo ha causato.

24. Crittografia

L'utilizzo di sistemi di crittografia sulle risorse tramite cui vengono trattati dati di carattere professionale deve essere concordato con i Sistemi Informativi, al fine di garantirne la conformità alle politiche di crittografia definite a livello organizzativo.

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

L'organizzazione 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.

25. Sicurezza generale e perimetrale

All'interno dell'infrastruttura tecnologica 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.

E' gestito da soggetti debitamente designati dall'organizzazione, 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, i Sistemi Informativi verificheranno 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.

26. Dispositivi mobili dati in dotazione

Tablet e altri dispositivi mobili forniti in dotazione ad utenti dell'organizzazione costituiscono uno strumento finalizzato al perseguimento di attività istituzionali e di carattere professionale.

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 tablet da parte di soggetti non autorizzati, l'utente deve attivare sistemi di blocco schermo con protezione con password numerica, con segno grafico composto sullo schermo o tramite riconoscimento dell'impronta digitale (in quest'ultimo caso deve essere messa a disposizione una modalità alternativa di accesso, per consentirne l'utilizzo anche ad altri utenti autorizzati).

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

Il Titolare del tablet è responsabile dell'aggiornamento software, delle APP installate nel dispositivo e del sistema Antivirus.

A causa della sempre maggiore interazione tra i dispositivi mobili e i sistemi informatici, l'abuso di tali strumenti può costituire una potenziale fonte di minaccia ai sistemi dell'organizzazione. 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'organizzazione senza prima aver concordato la cosa con il responsabile dell'ufficio che ha in dotazione i dispositivi, sentito il parere dei 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 del responsabile dell'ufficio che ha in dotazione i dispositivi, sentito il parere dei Sistemi Informativi.

In caso di disservizio o di problemi di funzionamento software, i Sistemi Informativi e le altre strutture preposte alla manutenzione dei dispositivi, potranno effettuare dei controlli sulla configurazione dei programmi installati sull'apparato concesso in uso con finalità di protezione del patrimonio informativo. I controlli verranno effettuati nel rispetto della libertà e della dignità dei lavoratori; il trattamento di eventuali dati personali verrà effettuato nel rispetto dei principi di pertinenza e non eccedenza.

L'organizzazione effettua dei controlli della spesa relativa ai consumi di traffico dati, che non comportano la consultazione dei siti visitati. Nel caso vengano ravvisati costi non previsti o spese eccedenti rispetto a quanto contrattualmente definito derivanti dall'utilizzo del dispositivo, potranno essere attivati dei controlli sul dispositivo stesso e sul suo impiego, ai fini di verifica della spesa e di tutela del patrimonio dell'organizzazione.

Qualora da tali controlli sopra menzionati dovesse emergere un utilizzo inadeguato delle attrezzature (fra cui l'installazione di programmi potenzialmente dannosi), che contravvenga le prescrizioni impartite, tale circostanza verrà comunicata alle strutture competenti che valuteranno l'eventuale adozione di provvedimenti.

Al momento della restituzione dei dispositivi, il personale assegnatario dovrà cancellare eventuali contenuti personali (es. e-mail, contenuti multimediali, ecc).

Allorché il dispositivo restituito contenga dati personali, questi verranno cancellati indiscriminatamente da soggetti specificamente incaricati dall'organizzazione prima di un'eventuale assegnazione successiva.

APP o informazioni di natura lavorativa che possano essere di utilità per l'organizzazione dovranno essere lasciati a disposizione.

Per dispositivi particolari utilizzati per specifiche finalità (es. bodycam, attrezzature fotografiche mobili, ecc) si rimanda a specifica documentazione regolamentare prevista dall'organizzazione.

In caso di smarrimento o furto di un dispositivo, è necessario segnalare immediatamente la circostanza ai Sistemi Informativi, al fine di valutare eventuali azioni di mitigazione del danno.

27. Telefonia cellulare

Per i dispositivi cellulari valgono tutte le prescrizioni relative ai dispositivi mobili dati in dotazione di cui al punto precedente.

Si raccomanda di rimuovere il prima possibile immagini, video, audio e altri contenuti multimediali acquisiti tramite i dispositivi per qualsiasi motivo, al fine di evitare il rischio di divulgazione di dati personali in caso di furto o di smarrimento degli apparati.

Potrebbero inoltre essere effettuati controlli dei dati contabili relativi al traffico telefonico, per finalità di controllo della spesa. Tali controlli potranno prevedere la consultazione dei numeri chiamati parzialmente oscurati, che non potranno essere visionati per intero; potrà

essere chiesto all'utente di indicare le telefonate effettuate per attività professionale e quelle effettuate per fini privati.

28. Controlli

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

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

- difendere il patrimonio dell'organizzazione;
- far valere o difendere un diritto in sede giudiziaria;
- tutelare gli interessi dei soggetti terzi che l'organizzazione è tenuta a salvaguardare nel perseguimento delle proprie attività istituzionali.

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 dei sistemi di accesso internet e di sicurezza perimetrale in caso di minacce segnalate dai sistemi di sicurezza o di lentezza di banda, con il fine di garantire il buon funzionamento della rete dell'organizzazione. 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 informativi dell' organizzazione. 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 dell'organizzazione. In caso di accesso alla casella di posta, verrà redatto un apposito rapporto di intervento in cui verranno specificate la azioni intraprese, che verrà consegnato all'utente al termine del periodo di assenza;
- analisi dei dispositivi mobili messi a disposizione per attività di tipo professionale, con finalità di controllo della spesa e protezione dei dati ivi presenti. Le modalità di controllo sono specificate nell'apposito capitolo relativo ai dispositivi mobili in dotazione e alla telefonia mobile;
- controllo dell'esito dei backup effettuati sui sistemi server dell'organizzazione, 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 dell'organizzazione. Tale controllo riguarderà la verifica della localizzazione dei dati in spazi logici protetti e di misure di backup.

Qualsiasi controllo verrà effettuato nel rispetto della libertà e delle dignità degli utenti. Eventuali dati privati 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'organizzazione si riserva di intraprendere provvedimenti disciplinari.

A seguito di eventi che abbiano comportato un danneggiamento del patrimonio di proprietà dell'organizzazione, qualora emergano degli elementi che possano fondatamente evidenziare degli atteggiamenti inadeguati potenziale causa dei danni rilevati, l'organizzazione ha diritto di attuare controlli difensivi occulti con la finalità di tutelare le risorse in uso, se da essi fosse possibile riscontrare e sanzionare un comportamento idoneo improprio dal parte degli utenti.

29. 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 etc… che permettono 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 eventuali disfunzioni.

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 del software presente sui dispositivi non compreso nell'elenco dei software autorizzati
- Monitoraggio ed alert in caso di anomalie del traffico di rete interna e del funzionamento delle postazioni di lavoro
- 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
- Analisi dei contenuti del traffico web per filtraggio 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.

I Sistemi Informativi potranno 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.

30. Gestione chiavi e altri strumenti di accesso fisico

Per lo svolgimento delle proprie attività correlate con le finalità perseguite dall'organizzazione, gli utenti possono essere dotati di chiavi o altri strumenti di accesso fisico (smartcard, chiavi RFID, codici alfanumerici) a risorse istituzionali.

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.

31. Gestione documenti cartacei

La scrivania e i tavoli di lavoro non devono mostrare in chiaro dati personali di cui possano venire a conoscenza visitatori occasionali. I documenti devono essere sempre presidiati o messi in sicurezza.

I dati trattati devono essere custoditi in luoghi non accessibili a soggetti non autorizzati. La custodia in sicurezza può essere garantita attraverso la chiusura a chiave di armadi e/o interi locali.

E' necessario procedere all'archiviazione definitiva, nei luoghi predisposti, dei supporti cartacei e dei supporti elettronici una volta terminate le attività di consultazione ed elaborazione.

I documenti cartacei non più utilizzati devono essere eliminati con macchine distruggi-documenti o ridotti a «coriandoli» che non rendano possibile la ricostruzione delle informazioni contenute.

32. Rapporto con soggetti terzi

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

E' vietato 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 il responsabile competente sul da farsi.

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

33. Incidenti di sicurezza e Data Breach

Un qualsiasi incidente, occorso su dati informatici, cartacei 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 per la protezione dei dati personali ai sensi dell'art. 33 del RGPD.

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 messe a disposizione dall'organizzazione è necessario comunicarlo immediatamente al proprio superiore e contattare il Responsabile Protezione dati - 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 contenuti, saranno rese disponibili nella intranet dell'organizzazione.

34. Osservanza del presente disciplinare

La finalità del presente documento è quella di regolamentare l'utilizzo delle risorse messe a disposizione dall'organizzazione per trattare dati e promuovere l'osservanza delle regole in merito alla protezione dei dati personali, al fine di garantire l'adeguata riservatezza, integrità e disponibilità dei dati gestiti dall'organizzazione.

A tali scopi, in caso si riscontrino delle criticità che possano ledere la sicurezza del sistema informativo, l'organizzazione 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 delle regole e delle misure di sicurezza elencate nel presente documento implica la responsabilità personale dell'utente.

35. Osservanza delle regole relative alla normativa in tema di protezione dei dati personali e agli standard di sicurezza dell'organizzazione

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 dell'organizzazione.

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 RGPD.

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

36. Segretezza delle informazioni

L'attività svolta potrebbe comportare la conoscenza incidentale di dati personali di cui l'organizzazione è Titolare o Responsabile esterno del trattamento. E' pertanto necessario improntare le proprie 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 e/o cessazione del rapporto di lavoro.

37. Entrata in vigore e aggiornamenti successivi

Il presente documento è in vigore a partire dal 09/09/2020.

Gli uffici competenti provvederanno a comunicare ai collaboratori l'esistenza del presente disciplinare, la cui versione più recente potrà in ogni momento essere reperita presso la intranet dell'organizzazione.

E' compito dei collaboratori tenersi al corrente sull'ultima versione disponibile del presente documento attraverso verifica sulla pagina intranet.