PRIMA APPROVAZIONE: D.P. N. 83 DEL 29/09/2020

PROVINCIA DI COMO

REGOLAMENTO PER L'UTILIZZO DEI SISTEMI INFORMATIVI AZIENDALI

E PER IL TRATTAMENTO DEI DATI

SOMMARIO

1 PREMESSA

L'utilizzo delle risorse informatiche di proprietà della Provincia di Como poste a disposizione dei dipendenti per lo svolgimento dell'attività lavorativa deve avvenire in piena conformità alle norme legislative e regolamentari che disciplinano il rapporto di lavoro e delle obbligazioni contrattuali dei dipendenti della Provincia di Como ai sensi e per gli effetti dell'art. 2104 del C.C, nonché delle norme in materia di trattamento dati che il Titolare del Trattamento deve adottare secondo quanto previsto dall'art. 32 del Regolamento UE n. 2016/679 (in seguito, "GDPR").

Il presente regolamento è assunto nell'osservanza delle norme di legge sopra richiamate ed avuto riguardo agli indirizzi giurisprudenziali in materia di riservatezza della vita di relazione e nel contempo, di condanna dell'indebito utilizzo dei mezzi informatici per fini personali e illeciti o che cagionano danni patrimoniali alla Provincia di Como.

2 SCOPO E CAMPO DI APPLICAZIONE

Scopo del presente Regolamento è definire le regole relative alle modalità di utilizzo delle risorse informatiche messe a disposizione a tutti i dipendenti della Provincia di Como, con l'obiettivo di prevenire la modifica/alterazione dei dati contenuti negli archivi stessi e consentire un trattamento adeguato dei dati personali degli interessati. Il regolamento descrive altresì le modalità con cui saranno effettuati i controlli sul rispetto delle indicate regole. A tal fine, successivamente alla sua adozione, il presente Regolamento sarà portato a conoscenza dei dipendenti e dei collaboratori della Provincia di Como.

3 DEFINIZIONI

Ai fini del presente regolamento i termini e le espressioni definite avranno il significato di seguito indicato.

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

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

Categorie particolari di dati: i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale (anche indicati come dati sensibili nel presente documento).

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

Titolare del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali. Quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.

Responsabile del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

Interessato: La definizione di "interessato", non essendocene una diretta, è desumibile dall'articolo 5, comma 1, del GDPR che, definendo il "dato personale" dispone che: "*si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale*".

Consenso dell'interessato: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento.

Violazione dei dati personali: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

4 CLASSIFICAZIONE E MODALITÀ DI TRATTAMENTO DELLE INFORMAZIONI CHE SI POSSONO RIFERIRE A DATI PERSONALI

Confidenziale	Uso interno	Pubblico
Informazioni la cui divulgazione danneggerebbe la privacy o l'integrità di un soggetto: - informazioni relative al personale dipendente - dati appartenenti a categorie particolari di dati personali - immagini dell'impianto di videosorveglianza - informazioni sulla geolocalizzazione	Informazioni il cui accesso non autorizzato potrebbe influenzare e/o compromettere l'efficacia dell'azione amministrativa dell'Ente, o compromettere il rapporto fiduciario tra la Provincia di Como e gli utenti e fornitori, come ad esempio: - anagrafiche degli utenti - contatti commerciali - informazioni relative ad aspetti operativi delle attività istituzionali	Informazioni che non sono né a uso interno né confidenziali., come ad esempio: - contatti della Provincia di Como - informazioni reperibili dal sito istituzionale - informazioni reperibili da pubblici registri (es. tramite visura camerale) - comunicazioni di marketing

L'accesso a queste informazioni è consentito esclusivamente a figure aziendali specificamente autorizzate o fornitori esterni nominati Responsabili del Trattamento, nell'ambito di un incarico o di un mandato.	Le informazioni possono essere comunicate esclusivamente alle persone che necessitano di conoscerle per motivi operativi connessi alle loro mansioni o a fornitori a cui siano necessarie per l'esecuzione del contratto.	Le informazioni non sono riservate o confidenziali e possono essere divulgate pubblicamente senza alcuna ripercussione per la Provincia di Como.
È vietato creare copie cartacee di documenti confidenziali, fatta eccezione per quanto previsto dagli obblighi di legge. I documenti confidenziali devono essere archiviati nell'apposito armadio protetto da serratura. È fatto divieto assoluto di lasciare, anche temporaneamente, questi documenti incustoditi sulle scrivanie o negli spazi condivisi. La condivisione di questi file deve essere effettuata tramite file/cartella protetti da password.	I documenti riservati possono essere stampati e vanno archiviati nell'apposito armadio con serratura messo a disposizione. È fatto divieto assoluto di lasciare questi documenti incustoditi sulle scrivanie o negli spazi condivisi. È inoltre fatto divieto assoluto di condivisione delle informazioni riservate in formato cartaceo.	È possibile condividere questi documenti all'esterno della Provincia di Como.
La trasmissione per via orale di informazioni confidenziali deve avvenire in appositi spazi (es. sale riunioni), alla presenza delle sole persone interessate.	La trasmissione per via orale di informazioni riservate può avvenire all'interno di spazi aziendali delimitati (es. sale riunioni) in presenza delle persone o fornitori autorizzati al trattamento.	La trasmissione per via orale di informazioni pubbliche è libera e non sottoposta a regolamentazione specifica.

5 MISURE DI SICUREZZA

L'articolo 32 del GDPR "Sicurezza del Trattamento" così recita: "*Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio*". A tal fine, la Provincia di Como adotta le misure adeguate di sicurezza, che si differenziano a seconda della modalità del trattamento dei dati e pertanto sono di seguito individuate.

La Provincia di Como si riserva la facoltà di procedere alla rimozione di ogni file o applicazione che riterrà essere pericoloso per la sicurezza del sistema ovvero acquisito, salvato, o installato in violazione del presente Regolamento.

6 UTILIZZO DEI SISTEMI INFORMATICI AZIENDALI

La Provincia di Como è responsabile delle metodologie per la tutela dei dati gestiti con ausilio di strumenti informatici. Pertanto i personal computer (fissi o mobili), i tablet, gli smartphone ed ogni altro dispositivo mobile, nonché i relativi programmi e/o applicazioni affidati al dipendente, sono da considerarsi esclusivamente come strumenti di lavoro, specificando quanto segue:

1. tali strumenti devono essere custoditi in modo appropriato adottando le precauzioni necessarie ad evitare il furto del materiale informatico messo disposizione dalla Provincia di Como;
2. devono essere prontamente segnalati all'Amministratore di Sistema il furto, il danneggiamento o lo smarrimento di tali strumenti;
3. gli strumenti assegnati possono essere utilizzati solo per fini professionali in relazione alle mansioni assegnate e non per scopi personali, tantomeno per scopi illeciti;
4. qualunque anomalia riscontrata nel funzionamento del sistema informatico deve essere tempestivamente segnalata all'Amministratore di Sistema.

Tutto l'hardware, inclusi gli strumenti informatici, è opportunamente etichettato e catalogato all'interno di un inventario elettronico. Dipendenti e collaboratori devono conservare e utilizzare gli strumenti a loro disposizione in modo da non danneggiare o asportare il contrassegno o l'etichetta.

6.1 Utilizzo dei personal computer, dei tablet, degli smartphone e dei dispositivi mobili

Richiamato quanto in premessa ed anche al fine di evitare il grave pericolo di introdurre virus informatici nonché di alterare la stabilità degli applicativi, non è consentito installare programmi provenienti dall'esterno. In caso di introduzione di virus, trojan o programmi che possono rappresentare un rischio per la sicurezza del computer e/o di qualsiasi altro dispositivo in uso si deve contattare l'Amministratore di Sistema, astenendosi dal risolvere il problema per conto proprio. Si rammenta inoltre quanto segue:

1. Non è consentito l'uso di programmi non distribuiti ufficialmente dalla Provincia di Como.
2. Non è consentito scaricare alcun software se non con l'autorizzazione dell'Amministratore di Sistema.
3. Non è consentito utilizzare strumenti software e/o hardware atti ad intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici.
4. Non è consentito modificare le configurazioni impostate sul proprio PC rispetto a quelle autorizzate e predisposte.
5. Non è consentita l'installazione sul proprio PC di mezzi di comunicazione propri (come ad esempio modem Wi-Fi e memorie esterne).
6. Non sono consentiti la visualizzazione e il salvataggio di testi, immagini o registrazioni a carattere razzista, pornografico, pedopornografico, sessuale, violento, osceno o di natura simile, indipendentemente da quale ne sia la fonte e/o comunque di qualsiasi materiale che sia vietato dalle norme penali.

7. Al termine della giornata lavorativa, o comunque quando ci si allontana dalla propria postazione per periodi prolungati, è indicato, ove possibile, lo spegnimento del PC.
8. Non è consentito l'utilizzo di dispositivi personali per finalità connesse alle attività dell'Ente.

6.2 Utilizzo pc portatili

Gli utilizzatori di PC portatili devono osservare particolari cautele per evitare perdita o di dati o accessi da parte di persone non autorizzate, tra cui, ad esempio:

1. applicare al PC portatile assegnato le regole di utilizzo previste per i PC connessi in rete;
2. custodirlo con diligenza e in luogo protetto durante gli spostamenti;
3. evitare di salvare file in locale se non per necessità operative.

6.3 Utilizzo di supporti magnetici

I dati devono essere salvati sulle cartelle presenti sul server aziendale. L'utilizzo di supporti magnetici (es. hard-disk esterni, chiavette usb) deve essere limitato ad esigenze lavorative e secondo le seguenti modalità:

1. ogni dipendente è tenuto a custodire i supporti magnetici contenenti dati sensibili e giudiziari in armadi chiusi a chiave onde evitare che il loro contenuto possa essere trafugato, alterato e/o distrutto;
2. non è consentito scaricare file contenuti in supporti magnetici/ottici non aventi alcuna attinenza con la propria prestazione lavorativa.

6.4 Controlli contro malware

La Provincia di Como predispone gli strumenti dati in uso a dipendenti e collaboratori, in modo che siano adottate le misure più opportune per proteggere i sistemi da malware, attacchi hacker e intrusioni in genere. La Provincia di Como provvede all'installazione di opportuni software quali antivirus e configurazione di firewall.

È obbligo del dipendente verificare almeno ogni 15 giorni che questi software siano in funzione e aggiornati. Per qualsiasi informazione riguardo modalità di verifica o nel caso si sospettino malfunzionamenti il dipendente si può rivolgere all'Amministratore di Sistema, il quale, potrà anche intervenire direttamente sul dispositivo.

7 UTILIZZO DELLA RETE AZIENDALE

Le unità di rete sono aree di condivisione di informazioni strettamente professionali e non possono, in alcun modo, essere utilizzate per scopi diversi. Pertanto, qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità.

La Provincia di Como si riserva la facoltà di procedere alla rimozione di ogni file o applicazione che riterrà essere pericoloso per la sicurezza del sistema ovvero acquisito o installato in violazione del presente Regolamento.

8 UTILIZZO DELLA RETE INTERNET E DELLA POSTA ELETTRONICA

8.1. Internet

L'uso di Internet è consentito esclusivamente alle persone autorizzate per gli scopi attinenti alla propria attività lavorativa. Non è consentito scaricare file, inclusi file multimediali, in violazione delle leggi sul copyright. Si ricorda in particolare che nell'ambito dell'attività lavorativa:

1. Non è consentito navigare in siti non attinenti allo svolgimento delle mansioni assegnate, soprattutto in quelli che possono rivelare le opinioni politiche, religiose o sindacali, nonché altri dati sensibili del dipendente.
2. È vietata ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.
3. Non è consentita la consultazione o la memorizzazione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.

Ai fini di garantire una navigazione Internet sicura e prevenire il download e la diffusione di malware, la Provincia di Como si avvale di strumenti esterni per il filtraggio del traffico dati. In particolare, è in uso una soluzione di DNS filtering tramite un provider esterno. I dati non rivelano in alcun modo i contenuti delle comunicazioni in rete e sono utilizzati esclusivamente dal provider nel rispetto dei regolamenti.

I dati sono conservati per 30 giorni al fine di consentirne una analisi periodica.

L'eventuale prolungamento dei suddetti tempi di conservazione è eccezionale e può avere luogo solo in relazione all'indispensabilità del dato rispetto all'esercizio alla difesa di un diritto in sede giudiziaria oppure all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'Autorità Giudiziaria.

8.2. Posta elettronica

Al singolo lavoratore dipendente viene assegnato un indirizzo e-mail personale del tipo nome.cognome@provincia.como.it. I dipendenti sono tenuti a mantenere in ordine la propria casella, a prestare attenzione alla dimensione degli allegati inviati e, per la trasmissione di file, a preferire, quando possibile, l'utilizzo delle cartelle di rete condivise.

Si ricorda che anche la posta elettronica è uno strumento di lavoro, e che tutte le caselle di posta elettronica contrassegnate dagli indirizzi con estensione "@provincia.como.it" ed il contenuto delle stesse sono e restano di proprietà della Provincia di Como, che le concede in uso ai propri dipendenti esclusivamente per fini di lavoro.

Si ritiene pertanto utile segnalare che:

1. non è consentito utilizzare l'indirizzo di posta elettronica istituzionale (sia in entrata che in uscita) per motivi non attinenti allo svolgimento delle mansioni assegnate;
2. ogni messaggio di posta elettronica deve riportare nome e cognome;
3. è obbligatorio specificare l'oggetto della e-mail nel relativo campo;

4. è opportuno limitare l'uso della funzione "rispondi a tutti" solo ai casi strettamente necessari;
5. essendo vietata la diffusione degli indirizzi email senza il consenso dell'intestatario, si raccomanda di prestare attenzione agli invii a più persone, valutando, se del caso, l'utilizzo del campo "CCN:" (o "BCC:" per le postazioni con il software in inglese) al posto di "A:" e/o "CC:";
6. non è consentito inviare o memorizzare messaggi (interni ed esterni) di natura oltraggiosa (contenenti testi, immagini o registrazioni a carattere razzista, pornografico, pedopornografico, sessuale, violento, osceno o di natura simile) e/o comunque di qualsiasi materiale che sia vietato dalle norme penali e/o che sia discriminatorio per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;
7. non è consentito rispondere e/o inoltrare messaggi catalogabili come spam;
8. non è consentito l'utilizzo dell'indirizzo di posta elettronica istituzionale per la partecipazione a dibattiti, forum o mail-list, salvo diversa ed esplicita autorizzazione;
9. i messaggi elettronici in entrata vengono sistematicamente analizzati nella ricerca di virus; i messaggi contenenti virus sono automaticamente eliminati;
10. sono vietati i tentativi di accesso a messaggi elettronici di utenti o terzi;
11. è vietato inviare posta elettronica a nome di un altro utente, salvo sua espressa autorizzazione.

8.3. Gestione dei Social Network e dei programmi di messaggistica

L'uso dei Social Network è autorizzato esclusivamente per finalità di lavoro. È raccomandato di non inviare comunicazioni a soggetti estranei agli scopi istituzionali o professionali ovvero procedere alla diffusione dei dati non autorizzati.

Si ricorda che l'utilizzo di WhatsApp per scopi non professionali non è consentito.

Si ricorda che non è consentito l'invio di allegati tramite Skype, da utilizzarsi eventualmente esclusivamente per le comunicazioni interne ed esterne.

9 CREDENZIALI DI ACCESSO

Le credenziali di accesso alla postazione di lavoro e agli applicativi aziendali dei nuovi utenti sono comunicate dall'Amministratore di Sistema, in base al profilo di accesso corrispondente al ruolo e alle mansioni affidati all'utente.

Si rammenta che la password è personale e non può essere comunicata ad altre persone.

È severamente vietato usare la password e lo User-ID di un altro utente.

Le norme sopra elencate si applicano a tutte le credenziali distribuite agli utenti per accedere agli strumenti, agli applicativi e alle banche dati aziendali.

Al momento del rilascio delle credenziali verrà impostata una password generica che consentirà il primo accesso che dovrà obbligatoriamente essere cambiata con una ad esclusiva conoscenza dell'assegnatario. La password deve essere conforme ai seguenti requisiti minimi di complessità:

- lunghezza minima di 8 caratteri;
- non deve contenere nome e cognome dell'utente;
- deve essere costituita da caratteri appartenenti ad almeno tre dei seguenti quattro gruppi: 1-maiuscole, 2-minuscole, 3-numeri, 4-caratteri speciali.

I requisiti di complessità vengono verificati al momento sia della creazione, sia della modifica delle password. Le password scadono ogni 90 giorni. Non è possibile riutilizzare una delle ultime dieci password.

Le password non devono, per motivo alcuno, essere trascritte o risultare facilmente reperibili (ad esempio, non devono essere riportate su supporti cartacei).

Le postazioni di lavoro, siano Desktop, PC portatili, Smartphone o Tablet, non possono essere abbandonate senza che l'accesso sia protetto, pertanto sul proprio PC è obbligatorio impostare uno screensaver automatico con password o, in caso di abbandono della postazione, disconnettere l'utente.

La Provincia di Como provvederà a disabilitare tempestivamente le credenziali, comunque entro 15 giorni, a seguito della conclusione della collaborazione o qualora venga meno la necessità per cui queste sono state create.

10 RISERVATEZZA DEI DATI AZIENDALI NELLE COMUNICAZIONI CON L'ESTERNO

I documenti ed i file prodotti all'interno dalla Provincia di Como durante l'attività lavorativa quali documenti tecnici, anagrafiche, comunicazioni interne/esterne, file di posta, ecc. sono esclusivamente di proprietà della Provincia di Como. Non è consentito esportare alcun file tramite salvataggio su supporti esterni, stampa, invio e diffusione ad altri soggetti tramite e-mail se non espressamente autorizzati o attinenti con l'attività lavorativa.

E' severamente vietato rivelare informazioni riservate o di carattere confidenziale relative alla Provincia di Como, ai suoi collaboratori o ad altri soggetti con i quali si intrattengono rapporti istituzionali.

E' severamente vietata la diffusione di informazioni confidenziali relative alla Provincia di Como a soggetti indeterminati.

L'utilizzo dei loghi aziendali è consentito solo se previsto nell'ambito delle mansioni e attività assegnate; in ogni caso è vietato il riferimento a qualsiasi fatto, persona, tecnologie ed informazioni in generale riconducibili alla Provincia di Como a meno che non si tratti di contesto lavorativo.

11 DISPONIBILITÀ DEI DATI DURANTE I PERIODI DI ASSENZA

In caso di assenza prolungata superiore a due giorni al dipendente è richiesto di impostare un messaggio di risposta automatica che informi il mittente della propria indisponibilità fornendo un contatto alternativo.

Per particolari e specifiche necessità legate alla continuità operativa, ogni dipendente può individuare un fiduciario di posta elettronica autorizzato ad accedere alla propria casella di posta istituzionale in caso di assenza prolungata superiore a cinque giorni.

12 CESSAZIONE DEL RAPPORTO DI LAVORO

Quando un dipendente cessa il rapporto di collaborazione con la Provincia di Como (sia esso dipendente, collaboratore a progetto o stagista), l'incaricato è obbligato a consegnare al proprio responsabile gerarchico o all'Amministratore di Sistema gli strumenti aziendali e i dispositivi messi a disposizione, inclusi i supporti di memoria esterni.

L'Amministratore di Sistema provvederà a disattivare l'accesso ai corrispondenti archivi presenti sul server, alla casella di posta elettronica, e a tutti gli applicativi e servizi web messi a disposizione dall'ente. Per consentire la continuità operativa, sulla casella di posta dell'incaricato dimissionario sarà impostato un messaggio automatico che avvisa della disattivazione della casella e-mail e fornisce il nominativo di un altro utente.

Ricordando che la posta elettronica e tutti gli strumenti aziendali sono di proprietà dell'ente, si ritiene necessario ricordare che a cessazione del rapporto di lavoro è obbligatorio restituire integri e completi tutti gli strumenti che la Provincia di Como ha messo a disposizione, in particolare:

1. la casella di posta elettronica ed i messaggi e documenti in essa contenuti devono essere messi a disposizione dell'ente per consentire la continuità operativa;
2. eventuali messaggi privati o non pertinenti l'attività operativa devono essere eliminati;
3. PC portatili e smartphone devono essere tempestivamente consegnati, senza che il collaboratore ne effettui backup o copie per uso personale;
4. eventuali schede sim devono essere restituite.

Entro 15 giorni dal termine della collaborazione tutto l'hardware sarà formattato in modo da essere illeggibile e non più recuperabile, secondo gli standard internazionali più recenti.

13 CONTROLLI

Poiché in caso di violazioni contrattuali e giuridiche, sia la Provincia di Como sia il singolo lavoratore sono potenzialmente perseguibili con sanzioni, anche di natura penale, la Provincia di Como verificherà, nei limiti consentiti dalle norme legali e contrattuali, il rispetto delle regole e l'integrità del proprio sistema informatico.

Qualora le misure tecniche preventive non fossero sufficienti ad evitare eventi dannosi o situazioni di pericolo e/o gli strumenti ed i dispositivi di controllo segnalino anomalie nel normale utilizzo delle risorse, la Provincia di Como provvederà ad effettuare con gradualità, nel rispetto dei principi di pertinenza e non eccedenza, le verifiche di eventuali situazioni anomale attraverso le fasi successive.

13.1 Traffico di rete ed internet

Si riportano i controlli sui dati di traffico effettuati per verificare la presenza di eventuali anomalie:

1. analisi aggregata del traffico di rete riferito all'intera struttura lavorativa e rilevazione della tipologia di utilizzo (e-mail, file audio, accesso a risorse estranee alle mansioni, ecc.) e/o delle categorie di siti visitati;
2. emanazione di un avviso generalizzato relativo ad un riscontrato utilizzo anomalo, con l'invito ad attenersi scrupolosamente ai compiti assegnati ed alle istruzioni impartite;
3. in caso di successivo permanere dell'anomalia, effettuazione di controlli sul traffico generato dalle singole postazioni di lavoro, preservando comunque il rispetto della privacy del dipendente omettendo l'individuazione dei singoli siti visitati, a meno che ciò non sia richiesto dall'Autorità Giudiziaria.

13.2 Occupazione dello spazio di memorizzazione sui server aziendali

Si riportano i controlli relativi allo spazio occupato sui server aziendali:

1. analisi aggregata dei dati memorizzati sui server a livello di intera struttura lavorativa, rilevazione della tipologia di utilizzo (file audio, file video, immagini, software non autorizzato) e relativa pertinenza con l'attività lavorativa;
2. emanazione di un avviso generalizzato relativo ad un riscontrato utilizzo anomalo, con l'invito ad attenersi scrupolosamente ai compiti assegnati ed alle istruzioni impartite;
3. analisi aggregata dei dati memorizzati sui server a livello di singoli Settori/Servizi, rilevazione della tipologia di utilizzo (file audio, file video, immagini, software non autorizzato) e relativa pertinenza con l'attività lavorativa;
4. emanazione di un avviso al responsabile gerarchico relativo ad un riscontrato utilizzo anomalo, con l'invito ad attenersi scrupolosamente ai compiti assegnati ed alle istruzioni impartite;
5. in caso di successivo permanere dell'anomalia, è possibile procedere con un'analisi puntuale, anche sulle singole cartelle di file.

13.3 Controlli sulle postazioni di lavoro

Qualora a seguito degli accertamenti generali, risultino elementi presuntivi plurimi e concordanti in ordine all'anomalo utilizzo di una postazione di lavoro, il titolare o il responsabile gerarchico procederà alla contestazione delle anomalie al dipendente titolare della postazione di lavoro, assegnandogli un termine non inferiore a 5 giorni per la presentazione di controdeduzioni o giustificazioni Nell'ipotesi in cui le giustificazioni presentate non siano ritenute congrue o scusanti , con provvedimento motivato potrà essere autorizzata la verifica puntuale della postazione di lavoro che dovrà avvenire alla presenza ed in contraddittorio del titolare della postazione di lavoro stessa. Si ribadisce che ogni controllo verrà effettuato nel rispetto dei seguenti principi:

1. proporzionalità: il controllo e l'estensione dello stesso dovrà rivestire, in ogni caso, un carattere adeguato, pertinente e non eccessivo rispetto alla/alle finalità perseguite, ma resterà sempre entro i limiti minimi;
2. trasparenza: l'adozione del presente Regolamento ha l'obiettivo di informare gli utenti sui diritti ed i doveri di entrambe le parti.

Il soggetto preposto al controllo ed alla verifica del rispetto del presente regolamento è l'Amministratore di Sistema.

14 PROTEZIONE DEI DATI – ALTRE MISURE DI SICUREZZA

Al fine di tutelare dati trattati su supporto cartaceo, si ricorda infine quanto segue:

1. non trasportare al di fuori dell'ente documenti cartacei se non per scopi legati alle attività lavorative: devono essere conservati nei locali dedicati a cura degli incaricati;
2. non diffondere informazioni e documentazione riservate;
3. prestare particolare attenzione alla tutela delle chiavi e ai codici di accesso ai locali dell'ente.

I documenti che contengono dati personali o sensibili devono essere archiviati e custoditi in armadi provvisti di serratura, onde evitare accessi non autorizzati, asportazione o copiatura, la cui chiave deve essere conservata in luogo sicuro a cura dell'Ente o dell'Ufficio Interessato.

Stampanti, apparecchiature fax e fotocopiatrici, devono essere collocate in luoghi in cui sia agevole la sorveglianza o meglio a vista diretta degli incaricati. Si raccomanda di evitare la diffusione di copie e stampe se non necessario.

15 AZIONI A FRONTE DEI CONTROLLI

Tutte le anomalie riscontrate che possono costituire una violazione a quanto definito nel presente Regolamento devono essere segnalate all'Amministratore di Sistema secondo quanto previsto.

Qualora, ad esito di controllo, vengano rilevate delle anomalie sull'utilizzo dei sopracitati strumenti informatici che possano essere configurate quali attività non conformi al presente codice o comunque poste in violazione dei doveri inerenti il contratto di lavoro, verrà data informazione al Titolare del trattamento per l'adozione dei conseguenti provvedimenti disciplinari.

A seguito dell'accertamento della condotta illecita e, quindi, dell'adozione del provvedimento disciplinare, la Provincia di Como procederà altresì, qualora il fatto integri gli estremi di un reato, a segnalare l'abuso all'Autorità competente.

16 DEROGHE E MODIFICHE AL PRESENTE REGOLAMENTO

Il presente documento è pubblicato sul sito web istituzionale, adeguatamente diffuso a tutto il personale dell'Ente e ai collaboratori esterni e regolarmente aggiornato. L'ufficio competente provvederà a notificare a collaboratori e dipendenti la presenza di una eventuale versione aggiornata. Il presente documento viene regolarmente revisionato e approvato dall'ente.

Deroghe o modifiche di uno o più punti del presente Regolamento, non rendono invalidi gli altri punti.