COMUNE DI PANDINO

Provincia di Cremona

Area Affari Generali

26025 - Via Castello n° 15 - P.IVA 00135350197

☎ 0373/973300 - 🖷 0373/970056 ✉ e-mail:segreteria@comune.pandino.cr.it

CODICE ENTE: 107708 PANDINO

DELIBERAZIONE N° 22 del 21/02/2022

V E R B A L E D I D E L I B E R A Z I O N E D E L L A G I U N T A C O M U N A L E

OGGETTO: APPROVAZIONE REGOLAMENTO PER L'UTILIZZO DEGLI STRUMENTI E SERVIZI INFORMATICI

L'anno **DUEMILAVENTIDUE**, addì **VENTUNO** del mese di **FEBBRAIO** alle ore **13:00,** convocata nei modi di legge, si è riunita la Giunta Comunale.

La seduta viene svolta interamente in videoconferenza e si attesta la contestuale presenza dei componenti:

All'appello risultano:

COGNOME E NOME	QUALIFICA	PRESENTE
BONAVENTI PIERGIACOMO	Sindaco	SI
SAU FRANCESCA	Assessore e Vice Sindaco	SI
VANAZZI FRANCESCO	Assessore	SI
BOSA RICCARDO	Assessore	SI
SGRO' SARA	Assessore	SI

PRESENTI: 5 ASSENTI: 0

I componenti sono tutti collegati da remoto con videocamera e dispositivo informatico

Partecipa e verbalizza il Segretario Comunale Dott. Cameriere Enrico Antonio collegato da remoto con dispositivo informatico.

Il Presidente, accertato con l'ausilio del Segretario Comunale, il numero legale dei componenti della Giunta presenti in videoconferenza simultanea, nonché accertato che gli stessi hanno dichiarato che il collegamento in videoconferenza assicura una qualità sufficiente per comprendere gli interventi e constatare le votazioni, dichiara aperta la seduta ed invita la Giunta Comunale a trattare il seguente argomento:

OGGETTO: APPROVAZIONE REGOLAMENTO PER L'UTILIZZO DEGLI STRUMENTI E SERVIZI INFORMATICI

LA GIUNTA COMUNALE

CONSIDERATO che:
-il Comune di Pandino dispone di una rete informatica e telematica, costituita da un insieme di strumenti e mezzi informatici quali le componenti hardware e software (personal computer, notebook, server, strumenti per la stampa e la riproduzione, programmi, ecc.) e dei necessari collegamenti telematici che veicolano le informazioni da e verso le banche dati comunali;
- con l'emanazione della circolare AGID 2/2017 del 08/04/2017, venivano fornite indicazioni operative per la verifica delle condizioni minime di sicurezza ICT e del trattamento dei dati;

DATO ATTO che l'utilizzo della rete informatica e telematica, di internet e della posta elettronica, sono strumenti ormai indispensabili per perseguire con efficienza, efficacia ed economicità le funzioni istituzionali e gestionali dell'Ente come imposto dalle normative vigenti ,che sempre più tendono alla globalità delle informazioni telematiche;

RITENUTO di dovere regolamentare la disciplina per la gestione e l'utilizzo degli strumenti informatici e telematici comunali, utilizzata dai dipendenti e dagli amministratori comunali, al fine di evitare un uso non corretto;

CONSIDERATO che:
– è compito del Comune assicurare la piena funzionalità del sistema informatico e promuovere ogni opportuna misura, organizzativa e tecnologica, volta a prevenire il rischio di utilizzi impropri delle strumentazioni e delle banche dati;
- risulta fondamentale individuare il complesso delle misure che configurano il livello minimo di protezione del sistema informatico comunale e del patrimonio informativo digitale dell'Ente;
- per dare attuazione a tali esigenze è necessario fornire agli utenti (amministratori, responsabili di servizio, dipendenti e collaboratori) specifiche disposizioni circa le modalità da seguire per un corretto utilizzo degli strumenti e delle risorse informatiche messe loro a disposizione per lo svolgimento delle proprie mansioni istituzionali, in modo che ciascun utente possa collaborare attivamente alle politiche di sicurezza poste in atto dall'Amministrazione;
- risulta altresì necessario disciplinare le misure con le quali il Comune può eventualmente accertare e inibire le condotte illecite sull'utilizzo delle predette risorse, ponendo in essere adeguati e commisurati sistemi di controllo sul corretto utilizzo degli strumenti informatici, senza che ciò possa in alcun modo invadere e violare la sfera personale del lavoratore e quindi il suo diritto alla riservatezza e dalla dignità, come sancito dallo Statuto dei Lavoratori (L.20/05/1970 n.300);
- ogni utente è responsabile civilmente e penalmente, del corretto utilizzo delle risorse informatiche, dei servizi a cui ha accesso e dei dati trattati a fini istituzionali; –
- per rispondere alle suddette esigenze operative è stato elaborato uno specifico "Regolamento per l'utilizzo degli strumenti informatici, di Internet, della posta elettronica e dei servizi di telefonia";
- tale regolamento è conforme alle indicazioni del Garante per la Protezione dei dati personali, nonché alle altre disposizioni normative in materia;
- tali prescrizioni si aggiungono ed integrano le specifiche istruzioni che vanno fornite a tutti gli incaricati in attuazione del Regolamento Europeo 679/16 "General Data Protection Regulation" (Reg.679/16 o GDPR);

VISTO lo schema di regolamento per la gestione e l'utilizzo dei sistemi informatici (AllegatoA);

VISTO lo statuto comunale;

VISTO il D.Lgs.30/03/2001 n.165;

VISTO il T.U. delle leggi sull'ordinamento degli enti locali, approvato con D.Lgs.267/20000 e s.m.i.;

ACQUISITO il parere favorevole ai sensi dell'art.49 del D.Lgs.267/2000 in ordine alla regolarità tecnica del presente provvedimento da parte di tutti i Responsabili di servizio nominati Responsabili interni del trattamento di dati personali con decreti sindacali

AD UNANIMITÀ di voti favorevoli espressi nelle forme di legge per appello nominale ed in forma palese ed espressa, in conformità alla lett. c) delle linee guida sullo svolgimento delle giunte a distanza di cui alla delibera di Giunta Comunale n. 42 del 18/03/2020,

DELIBERA

1) di dare atto che le premesse costituiscono parte integrante e sostanziale del presente atto;

2) di approvare il Regolamento per l'utilizzo dei sistemi informatici, allegato alla presente come parte integrante e sostanziale (Allegato A), costituito da n.25 punti;

3) di dare disposizioni al Servizio Personale affinché copia del regolamento sia consegnato e fatto sottoscrivere ai nuovi assunti, contestualmente alla sottoscrizione del contratto di lavoro;

4) di pubblicare il Regolamento nel sito istituzionale dell'Ente nella sezione Amministrazione Trasparente – Atti generali;

Con votazione separata

AD UNANIMITÀ di voti favorevoli espressi nelle forme di legge per appello nominale ed in forma palese ed espressa, in conformità alla lett. c) delle linee guida sullo svolgimento delle giunte a distanza di cui alla delibera di Giunta Comunale n. 42 del 18/03/2020,

DELIBERA

di dichiarare la presente deliberazione immediatamente eseguibile ai sensi dell'art. 134 – IV comma del D. Lgs. N. 267/00.

Letto, confermato e sottoscritto

IL SINDACO
Bonaventi Piergiacomo
Firmato digitalmente

Il Segretario Comunale
Dott. Cameriere Enrico Antonio
Firmato digitalmente

COMUNE DI PANDINO

Provincia di Cremona

26025 - Via Castello n° 15 - P.IVA 00135350197

☎ 0373/973300 - 🖷 0373/970056 ✉ e-mail:segreteria@comune.pandino.cr.it

PROPOSTA DI DELIBERAZIONE DELLA GIUNTA COMUNALE

OGGETTO : APPROVAZIONE REGOLAMENTO PER L'UTILIZZO DEGLI STRUMENTI E SERVIZI INFORMATICI

PARERE DI REGOLARITA' TECNICA

Si esprime parere favorevole di regolarità tecnica espresso ai sensi dell'art. 49 del T.U. approvato con D.Lgs. 18 Agosto 2000 n. 267, in quanto la proposta che precede è conforme alle norme legislative e tecniche che regolamentano la materia.

Pandino**,** lì **18/02/2022**

Il Segretario Comunale
CAMERIERE ENRICO ANTONIO /
INFOCERT SPA
Firmato digitalmente

COMUNE DI PANDINO

Provincia di Cremona
Area Affari Generali
26025 - Via Castello n° 15 - P.IVA 00135350197
☎ 0373/973300 - 🖷 0373/970056 ✉ e-mail:segreteria@comune.pandino.cr.it

CODICE ENTE: 107708 PANDINO

DELIBERAZIONE N° 22 del 21/02/2022

OGGETTO: APPROVAZIONE REGOLAMENTO PER L'UTILIZZO DEGLI STRUMENTI E SERVIZI INFORMATICI

ADEMPIMENTI RELATIVI ALLA PUBBLICAZIONE

La sopra estesa deliberazione:

- ai sensi dell'art. 124, comma primo, D. Lgs. 18/08/2000 n. 267, viene pubblicata all'Albo Pretorio del Comune in data odierna ed ivi rimarrà per 15 giorni consecutivi;

- è stata comunicata in data odierna ai Capigruppo Consiliari ai sensi dell'art. 125 del D. Lgs. 18/08/2000 n. 267.

Pandino, lì 24/02/2022

Responsabile Area Affari Generali
MANZONI MARGHERITA MARIA /
INFOCERT SPA
Firmato digitalmente

COMUNE DI PANDINO

Provincia di Cremona
Area Affari Generali
26025 - Via Castello n° 15 - P.IVA 00135350197
☎ 0373/973300 - 🖷 0373/970056 ✉ e-mail:segreteria@comune.pandino.cr.it

CODICE ENTE: 107708 PANDINO

DELIBERAZIONE N° 22 del 21/02/2022

OGGETTO: APPROVAZIONE REGOLAMENTO PER L'UTILIZZO DEGLI STRUMENTI E SERVIZI INFORMATICI

CERTIFICATO DI ESECUTIVITA'

La presente deliberazione è divenuta esecutiva in data odierna, decorsi 10 giorni dalla pubblicazione, ai sensi dell'art. 134, comma 3°, del T.U. approvato con D. Lgs. 18 agosto 2000 n. 267.

Pandino, lì 21/03/2022

Responsabile Area Affari Generali
MANZONI MARGHERITA MARIA /
InfoCamere S.C.p.A.
Firmato digitalmente

COMUNE DI Pandino

REGOLAMENTO PER L'UTILIZZO DEGLI STRUMENTI E SERVIZI INFORMATICI

Norme per il Corretto Utilizzo delle Risorse Informatiche.

Misure per la prevenzione e il monitoraggio degli usi impropri.

Art. 1 - Oggetto ed ambito di applicazione

Il presente Regolamento contiene le disposizioni riguardanti i corretti modi d'uso della rete informatica dell'ente e di tutte le risorse informatiche, in conformità e nel rispetto di quanto previsto dalla specifica normativa di settore e dalle ulteriori disposizioni emanate dall'ente stesso.

Gli strumenti informatici oggetto del presente Regolamento sono tutti i servizi e gli apparati di proprietà dell'ente resi disponibili agli Utenti per il quotidiano svolgimento delle proprie prestazioni lavorative.

Essi sono essenzialmente individuabili nei seguenti elementi: computer, apparati mobili, apparati rimovibili, sistemi di identificazione ed autenticazione informatica, Internet, strumenti di scambio file, posta elettronica e qualsiasi altro programma/apparecchiatura informatica destinata a memorizzare oppure a trasmettere dati e informazioni.

L'applicazione ed il rispetto puntuale delle disposizioni contenute nel presente Regolamento è responsabilità di tutti i soggetti che utilizzano gli strumenti informatici messi a disposizione dall'ente.

Ferme restando le disposizioni normative in materia e tutte le prescrizioni previste per il trattamento dei dati sensibili o giudiziari, il contenuto del presente Regolamento costituisce disposizione di servizio.

Il presente Regolamento si applica a tutto il personale dipendente dell'ente, senza distinzione di ruolo o livello, ed a tutti i collaboratori a prescindere dal rapporto contrattuale con essi intrattenuto (collaboratori a progetto, stagisti e borsisti, liberi professionisti, collaboratori terzi, ecc.).

Sono esentati dall'applicazione del presente Regolamento, limitatamente a quanto necessario per il corretto svolgimento delle proprie funzioni, gli Amministratori di Sistema, o i facenti tale funzione.

Pertanto, data la progressiva diffusione delle nuove tecnologie informatiche, ed in particolare il libero accesso alla rete Internet dai Personal Computer, al fine di non esporre l'ente ai rischi di un coinvolgimento sia patrimoniale che penale, creando problemi alla sicurezza e danni di immagine, l'utilizzo delle risorse informatiche e telematiche deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che comunque normalmente dovrebbero essere adottati nell'ambito di un rapporto di lavoro, al fine di evitare che condotte inconsapevoli possano innescare

complessità o minacce alla sicurezza nel trattamento dei dati.

Per qualsiasi dubbio relative all'applicazione pratica o all'interpretazione autentica delle disposizioni contenute nel presente Regolamento è possibile rivolgersi al personale del Servizio Sistemi Informativi o di chi ne fa funzione.

Art. 2 - Entrata in vigore, pubblicità e revisione

Il presente Regolamento entra in vigore ai sensi di legge e come stabilito dallo Statuto comunale. Sarà pubblicato nell'apposita sezione del sito web istituzionale denominata "Amministrazione Trasparente", garantendone la massima diffusione a tutto il personale.

Il Regolamento potrà essere soggetto a revisioni periodiche sulla base dell'evoluzione normativa e tecnologica nonché sulla base delle nuove esigenze di sicurezza e relative azioni correttive che si dovranno eventualmente intraprendere.

Stante l'elevata dinamicità della materia, eventuali adeguamenti di natura prettamente tecnica verranno introdotti e adeguatamente comunicati dal responsabile del Servizio Sistemi Informativi (o di chi ne fa funzione) agli utenti, e recepiti e ratificati nel testo mediante le periodiche revisioni annuali.

Art. 3 - Definizioni

Ai sensi del Regolamento UE 2016/679 (GDPR), si intende per:

- "trattamento" - qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;

- "trattamento informatico" - trattamento effettuato con l'ausilio di strumenti elettronici;

- "dato personale" - qualunque informazione riguardante persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;

- "dati identificativi" - i dati personali che permettono l'identificazione diretta

dell'interessato;

- "dati particolari” - 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;

- "dati giudiziari" - i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;

- "titolare" - la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali ed agli strumenti utilizzati, ivi compreso il profilo della sicurezza;

- "responsabile esterno del trattamento” - la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali; in riferimento al trattamento dei dati con strumenti elettronici particolare rilevanza assume il “responsabile del trattamento dei dati informatici e telematici”, di cui al punto successivo;

- “responsabile del trattamento dei dati informatici e telematici” (denominato D.I.T.) - per le sue specifiche competenze è identificato nel Responsabile del Servizio Sistemi Informativi. Le competenze del Responsabile di cui sopra riguardano l’attività di controllo e gestione degli impianti di elaborazione o di sue componenti, di basi di dati, di reti, di apparati di sicurezza e di sistemi software complessi (nella misura in cui consentono di intervenire su dati), l’individuazione ed attuazione di tutte le procedure fisiche, logiche ed organizzative per tutelare la sicurezza e la riservatezza nel trattamento dei dati informatici. Il Responsabile del trattamento dati informatici e telematici designa, per iscritto, gli amministratori di sistema, previa individuazione delle caratteristiche di esperienza, capacità ed affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

- "autorizzati”, le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;

- “amministratore di sistema”, la persona fisica dedicata alla gestione ed alla manutenzione di impianti di elaborazione o di sue componenti e tutte le figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati personali, quali gli amministratori di basi di dati, di reti informatiche, di apparati di sicurezza e di sistemi software complessi, nella misura in cui consentano di intervenire sui dati personali; soggetti che, pur non essendo preposti ordinariamente ad operazioni implicanti una comprensione del dominio applicativo (significato dei dati, formato delle rappresentazioni e semantica delle funzioni), possono, nelle loro consuete attività, essere concretamente responsabili di specifiche fasi lavorative comportanti elevate criticità rispetto alla protezione dei dati personali. Vanno considerati a tutti gli effetti alla stregua di trattamenti di dati personali il salvataggio dei dati (backup/recovery), l’organizzazione dei flussi di rete, la gestione dei supporti di memorizzazione e la manutenzione hardware, anche quando non consultati “in chiaro” dall’amministratore;

- "interessato", la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;

- “utente”, soggetto che accede ed utilizza i servizi e gli strumenti del sistema informatico dell’ente;

- "comunicazione", il dare conoscenza dei dati personali ad uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal Responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

- "diffusione", il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

- "dato anonimo", il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;

- "banca di dati", qualsiasi complesso organizzato di dati, ripartito in una o più unità dislocate in uno o più siti;

- "comunicazione elettronica", ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico. Sono escluse le informazioni trasmesse al pubblico tramite una rete di comunicazione elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad un abbonato o utente ricevente, identificato o

identificabile;

- "reti di comunicazione elettronica", i sistemi di trasmissione, le apparecchiature di commutazione o di instradamento ed altre risorse che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, incluse le reti satellitari, le reti terrestri mobili e fisse a commutazione di circuito e a commutazione di pacchetto, compresa Internet, le reti utilizzate per la diffusione circolare dei programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica, nella misura in cui sono utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato;

- "rete pubblica di comunicazioni", una rete di comunicazioni elettroniche utilizzata interamente o prevalentemente per fornire servizi di comunicazione elettronica accessibili al pubblico;

- "misure minime", il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31;

- “risorse informatiche”, sono annoverate tra le risorse informatiche:
- i server;
- le workstation, i personal computer, i notebook e qualsiasi altra tipologia di elaboratore elettronico, compresi i dispositivi mobili;
- le stampanti, i plotter, i fotocopiatori e i fax;
- tutti gli strumenti informatici interconnessi con la rete dell’ente;
- gli apparati di rete;
- tutto il software e i dati acquisiti o prodotti da parte degli utenti o di terzi autorizzati;
- file di qualsiasi natura, archivi di dati anche non strutturati ed applicazioni informatiche.

Art. 4 - Principi generali

I trattamenti devono rispettare le garanzie in materia di protezione dei dati e svolgersi nell'osservanza di alcuni cogenti principi sanciti nel Regolamento UE 2016/676 (GDPR):

A. il principio di necessità, secondo cui i sistemi informativi ed i programmi informatici devono essere configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi in relazione alle finalità perseguite (art. 5 e 6 GDPR);

B. il principio di correttezza, secondo cui le caratteristiche essenziali dei trattamenti devono essere rese note ai lavoratori (art. 37 GDPR). Le tecnologie dell'informazione (in

modo più marcato rispetto ad apparecchiature tradizionali) permettono di svolgere trattamenti ulteriori rispetto a quelli connessi ordinariamente all'attività lavorativa e ciò all'insaputa o senza la piena consapevolezza dei lavoratori, considerate anche le potenziali applicazioni di regole non adeguatamente conosciute dagli interessati (v. par. 3);

C. i trattamenti devono essere effettuati per finalità determinate, esplicite e legittime (art. 6 GDPR), osservando il principio di pertinenza e non eccedenza. Il datore di lavoro deve trattare i dati "nella misura meno invasiva possibile"; le attività di monitoraggio devono essere svolte solo da soggetti preposti ed essere "mirate sull'area di rischio, tenendo conto della normativa sulla protezione dei dati e, se pertinente, del principio di segretezza della corrispondenza" (Parere n.8/2001, cit., punti 5 e 12).

Art. 5 - Linee guida generali

L’ente, consapevole delle potenzialità fornite dagli strumenti informatici e telematici, li mette a disposizione dell’Utente esclusivamente per finalità di tipo lavorativo.

Non è quindi permesso utilizzare questi strumenti per altre finalità non connesse all’attività lavorativa o in modo che violino le leggi italiane vigenti in materia.

Ad esempio, non é consentito:
- accedere a siti ed acquisire o comunque diffondere prodotti informativi lesivi del comune senso del pudore;
- diffondere prodotti informativi lesivi dell’onorabilità, individuale e collettiva;
- diffondere prodotti informativi di natura politica;
- diffondere in rete, o con qualsiasi altro mezzo di comunicazione, informazioni riservate di qualunque natura;
- svolgere ogni tipo di attività commerciale;
- compiere attività che possano rappresentare una violazione della legge in materia di Copyright, fra le quali la copia non autorizzata di software, supporti audio e video, clonazione o programmazione di smartcard;
- compiere attività che compromettano in qualsiasi modo la sicurezza delle risorse informatiche e della rete aziendale.

L’ente adotterà ogni accorgimento tecnico necessario a tutelarsi da eventuali comportamenti non permessi, salvaguardando il rispetto della libertà e della dignità dei lavoratori; gli eventuali trattamenti effettuati saranno ispirati a canoni di trasparenza.

Art. 6 - Titolarità

L’ente è titolare di tutte le risorse hardware e software messe a disposizione degli utenti.

L’hardware ed il software in dotazione ai Servizi Comunali devono essere acquisiti in accordo con le specifiche tecniche fornite dal Servizio Sistemi Informativi o di chi ne svolge la funzione.

Le risorse informatiche assegnate devono essere custodite con cura evitando ogni possibile forma di danneggiamento.

Gli utenti assegnatari sono responsabili del corretto utilizzo degli strumenti messi loro a disposizione e della loro custodia e sono tenuti a segnalare tempestivamente al Servizio Sistemi Informativi o di chi ne fa la funzione, eventuali situazioni anomale, guasti e/o difetti di funzionamento dei dispositivi hardware e software.

Art. 7 - Competenze e responsabilità

Il Responsabile del Servizio Sistemi Informativi o chi ne fa funzione è tenuto a:

- elaborare le regole per un utilizzo ragionevolmente sicuro del sistema informativo dell’ente;
- applicare, con l’ausilio di personale incaricato interno/esterno, le regole di sicurezza sul sistema informativo dell’ente;
- monitorare, con l’ausilio di personale incaricato del Servizio Sistemi Informativi o chi ne fa funzione, e/o di personale incaricato interno/esterno, i sistemi per individuare un eventuale uso scorretto degli stessi, nel rispetto della privacy degli utenti;
- segnalare prontamente ai Dirigenti/Responsabili delle Strutture interessate ogni eventuale attività non autorizzata sul sistema informativo dell’ente;
- attenersi alle prescrizioni previste nel “Documento di adozione delle misure e accorgimenti prescritti dal Garante per la Protezione dei Dati Personali ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema”.

I Dirigenti/Responsabili dell’ente sono tenuti a:

- informare il personale dipendente e/o assimilato sulle disposizioni in merito all’uso consentito delle risorse del sistema informativo dell’ente;
- assicurare che il personale a loro assegnato si uniformi alle regole ed alle procedure descritte nel presente Regolamento;
- assicurare che i fornitori e/o il personale incaricato esterno si uniformino alle regole ed alle procedure descritte nel presente Regolamento;
- adempiere a tutti gli obblighi inerenti la responsabilità loro affidata in materia di trattamento di dati personali e sensibili gestiti dall’ente;
- segnalare prontamente al Responsabile del Servizio Sistemi Informativi ogni eventuale attività non autorizzata sul Sistema Informativo dell’ente.

Il personale del Servizio Sistemi Informativi e/o l'eventuale personale esterno incaricato che concorre alla gestione/implementazione del sistema informativo è tenuto a:
- garantire la massima riservatezza sulle informazioni acquisite direttamente o indirettamente nell'esercizio delle proprie funzioni;
- segnalare prontamente al Responsabile del Servizio Sistemi Informativi ogni eventuale attività non autorizzata sul sistema informativo dell'ente.

Gli Utenti del sistema informativo dell'ente sono responsabili per ciò che concerne:
- il rispetto delle regole dell'ente per l'uso consentito del sistema informativo;
- l'uso delle credenziali di autenticazione loro assegnate secondo le modalità previste nel presente Regolamento;
- la pronta segnalazione al competente Dirigente/Responsabile in merito ad ogni eventuale attività non autorizzata sul sistema informativo dell'ente di cui vengano a conoscenza.

Art. 8 - Credenziali di accesso

I sistemi di controllo degli accessi assolvono il compito di prevenire l'accesso, da parte di persone non autorizzate, a un sistema informatico ed alle relative applicazioni.

Lo scopo è di cautelare l'ente ed i suoi dipendenti da ogni tipo di manomissione, furto o distruzione di dati oltre che di limitare l'accesso a specifici dati da parte di personale non autorizzato.

Art. 8.1 Password

Ove l'accesso al sistema avviene tramite autenticazione delle credenziali (normalmente nome utente e password), l'Utente dovrà:
- custodire con diligenza le proprie credenziali e non comunicarle ad altre persone (es.: non scrivere la password su carta o post-it lasciandoli sulla scrivania o attaccati al monitor; non comunicare, né condividere con altri la propria password);
- durante la digitazione della propria password, assicurarsi che nessuno stia osservando la tastiera con l'intenzione di memorizzarla.

La password deve essere composta da almeno dodici caratteri e deve essere "robusta": una password si dice robusta quando è difficile ricostruirla e cioè quando risponde ad alcuni principi:
- all'aumentare della sua lunghezza, aumenta la difficoltà a carpirla;
- può includere cifre, lettere e caratteri speciali;
- non sono composte da semplici sequenze di tasti sulla tastiera, come ad esempio "asdfghjkl", o da ripetizioni del proprio nome utente (ad es. se il proprio utente è Rossi; la password "rossirossi" sarà inopportuna).

Ad esempio, una password sicura può essere composta dall'unione fuori contesto di parole di uso comune, con alternanza di maiuscole e minuscole e l'aggiunta di caratteri speciali, ad esempio "**Lun4pien4nelciel0?**".

L'Utente s'impegna a comunicare quanto prima al Servizio Sistemi Informativi o di chi ne fa funziona l'eventuale furto o smarrimento della propria password.
In particolare, in caso di furto, l'Utente s'impegna a modificare tempestivamente la password utilizzando le procedure automatiche a sua disposizione.

In ogni caso, resta inteso che l'Utente sarà responsabile delle conseguenze derivanti dal furto, dalla perdita o dallo smarrimento di tale password.

Art. 9 - Computer

Il computer è uno strumento di lavoro fornito dall'ente e rappresenta una dotazione strumentale della sede ove è ubicato.

Il suo eventuale utilizzo non inerente all'attività lavorativa è vietato perché può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza dell'intera infrastruttura tecnologica dell'ente.

Il computer può essere affidato ad uso singolo o condiviso, sulla base della richiesta effettuata dal Responsabile della Struttura e tenuto conto della prevalenza delle funzioni che devono essere espletate.

Il computer è fornito con configurazione software predefinita che non può essere per alcun motivo modificata da parte dell'utente.

Le richieste di installazione di nuovo software o di modifica della configurazione devono essere approvate dal Servizio Sistemi Informativi o da chi ne fa funzione, che solo a seguito di tale accettazione provvederà ad effettuarle.

L'utente non può modificare le impostazioni autonomamente; di conseguenza:
- non verranno forniti privilegi di "amministratore";
- non è consentita l'installazione sul proprio PC di mezzi di comunicazione propri (come ad esempio modem e dispositivi Bluetooth);
- non è consentito utilizzare strumenti software e/o hardware atti ad intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici;
- non è consentito copiare sul proprio computer file contenuti in supporti magnetici,

ottici e dispositivi usb non aventi alcuna attinenza con la propria prestazione lavorativa;
- il computer, salvo ulteriori disposizioni, deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio o in caso di non utilizzo;
- occorre bloccare il computer o disconnettersi, in caso di postazioni condivise e non, qualora ci si allontani dalla propria postazione (per il sistema operativo Windows, premendo contemporaneamente i tasti Windows[1] + L, oppure Alt+Ctrl+Canc e cliccando su blocca computer) o in alternativa attivando la protezione sul proprio screensaver; a tal proposito i Sistemi Informativi o chi ne fa funzione si riservano di attivare automaticamente la funzionalità il blocco del computer a seguito di inattività;
- non è consentito utilizzare strumenti potenzialmente in grado di consentire accessi non autorizzati alle risorse informatiche (es.: programmi di condivisione dati quali IRC, ICQ, o software di monitoraggio della rete in genere);
- non è consentito configurare o utilizzare servizi quali DNS, DHCP, server internet (Web, FTP,...) diversi da quelli messi a disposizione;
- non è consentito intercettare pacchetti sulla rete (sniffing); è conseguentemente vietato l'uso di software dedicati a carpire, in maniera invisibile, dati personali, password e ID dell'utente oppure atti a controllare ogni attività, ivi inclusa la corrispondenza ed i dati personali;
- non è consentito impostare password nel bios;
- non è consentito disassemblare il computer, asportare, scollegare, aggiungere, spostare o semplicemente scambiare tra un PC e l'altro qualsiasi apparecchiatura in dotazione all'Utente salvo diretta e specifica indicazione del personale tecnico del Servizio Sistemi Informativi o facente funzione;
- non è consentito avviare il personal computer con sistemi operativi diversi da quello installato dal Servizio Sistemi Informativi o facente funzione, incluse versioni live, salvo preventiva autorizzazione;
- non è consentito utilizzare connessioni in remoto per l'accesso a risorse dell'ente, al di fuori del perimetro aziendale e fatte salve le connessioni realizzate ed autorizzate da parte del Servizio Sistemi Informativi o facente funzione.

Art. 9.1 - Computer portatili (e dispositivi mobili)

L'Utente è responsabile dell'integrità del PC portatile affidatogli dal Responsabile della Struttura di appartenenza e dei dati ivi contenuti e deve custodirlo con diligenza sia durante gli spostamenti che nell'utilizzo nel luogo di lavoro.

Ai PC portatili (e dispositivi mobili) si applicano le regole di utilizzo previste per i personal computer.

---

1 [1]I tasti con l'emblema di Windows posti ai due lati della barra spaziatrice.

Nel caso di utilizzo comune con altri Utenti, prima della riconsegna occorre provvedere alla rimozione definitiva di eventuali file elaborati.

I dischi dovranno essere criptati, secondo modalità indicate dai Sistemi Informativi o funzione relativa, al fine di evitare, in caso di furto o di smarrimento, l'accesso a dati riservati e/o personali da parte di soggetti non autorizzati.

L'utente assegnatario che, venendo meno al dovere di diligenza nella custodia causi il danneggiamento o smarrimento delle dotazioni informatiche affidategli risponderà personalmente del danno patrimoniale arrecato.

Art. 10 - Stampanti

Per quanto concerne l'utilizzo delle stampanti, gli utenti sono tenuti a:

- stampare documenti ed atti solo se strettamente necessari per lo svolgimento delle proprie funzioni lavorative;
- stampare in bianco/nero e fronte/retro al fine di ridurre i costi, laddove possibile;
- utilizzare le stampanti ad alto carico dipartimentali (multifunzioni), tipicamente poste nei corridoi o in luoghi raggiungibili da tutti i dipendenti, nel caso si debbano stampare documenti con più di 25 pagine:
- utilizzare le funzionalità di stampa privata (laddove disponibili) per tutte le stampe inviate su stampanti non direttamente accessibili dalla postazione di lavoro; qualora ciò non fosse possibile, in caso di stampa di documenti contenenti dati o informazioni riservate, l'utente dovrà aver cura di monitorare la stampante e preservare, limitatamente alle oggettive possibilità, la conoscibilità di tali dati o informazioni da parte di terzi non autorizzati.

Art. 11 - Scanner di Rete

L'utilizzo delle scansioni deve essere orientato al miglior utilizzo in termini di dimensioni e leggibilità dei files.

Le impostazioni devono essere orientate ad avere la migliore leggibilità con le minori dimensioni possibili del file.

Una volta che il file è stato scaricato sul proprio pc per l'utilizzo, è necessario eliminarlo dalla memoria dello scanner.

Art. 12 - Rete

In assenza di specifica autorizzazione da parte delle Servizio Sistemi Informativi o facente funzione non è consentito accedere ai locali ed ai box riservati alle apparecchiature di rete.

Non è consentito collegare alle prese di rete apparecchiature non autorizzate da parte del Servizio Sistemi Informativi o facente funzione, quali: hub, switch, access point o altre componenti personali.

Non è inoltre consentito installare o utilizzare qualsiasi altra apparecchiatura atta a gestire comunicazioni quali, a titolo esemplificativo: modem, router, Internet key

Non è infine consentito effettuare spostamenti o modifiche di risorse collegate alla rete aziendale (es.: pc, stampanti, fotocopiatori e altro) senza una preventiva autorizzazione.

Art. 13 - Unità di archiviazione di rete

Gli spazi delle unità di rete messi a disposizione sono aree di condivisione e di archiviazione di informazioni strettamente lavorative e non possono pertanto essere utilizzate per la memorizzazione di file non attinenti ad attività lavorative.

In queste aree dovranno essere salvati i documenti lavorativi afferenti alla Struttura di appartenenza, al fine di renderli disponibili, in caso di necessità, agli altri utenti della Struttura.

Le attività di controllo statistico, amministrazione, backup e restore su queste unità sono competenza del personale del Servizio Sistemi Informativi o facente funzione.

Gli accessi alle unità di rete condivise devono essere autorizzati da parte del Responsabile del trattamento dei dati di pertinenza, il quale provvederà a richiedere al Servizio Sistemi Informativi dell'ente la creazione/rimozione dei diritti di accesso e ad effettuare periodicamente la verifica delle abilitazioni attive.

Possono essere fornite ulteriori aree deputate allo scambio di file tra strutture diverse (es.: cartella "Scambio/Transito", file scansionati da scanner di rete).

Onde evitare la saturazione di questi spazi, cessato lo scopo contingente, i file salvati nelle aree comuni dovranno essere rimossi a cura dell'utente che li ha memorizzati; diversamente, verranno rimossi mediante la programmazione di apposite procedure di

cancellazione automatica la cui frequenza verrà resa nota agli Utenti interessati.

In nessuna risorsa di rete è consentito salvare file audio, video, eseguibili ed archivi di posta ad eccezione di quelli strettamente attinenti a esigenze lavorative e dietro specifica e motivata richiesta da parte del Responsabile di Struttura.

Per tali tipologie di file ed archivi sono effettuati interventi di pulizia attivati d'ufficio da parte del Servizio Sistemi Informativi o facente funzione.

Può essere prevista una modalità di archiviazione "a freddo" di archivi che si intende conservare nel lungo periodo. Tali archivi dovranno essere creati raggruppando in modo omogeneo i files, ad esempio per anno o per tipologia, in un archivio compresso dotato di password concordata con i Sistemi Informativi o facente funzione. Gli archivi dovranno essere corredati di un indice che ne espliciti il contenuto per il successivo recupero.

Art. 14 - Internet

L'utilizzo della connessione Internet aziendale è consentita per i soli scopi lavorativi e nell'ambito delle mansioni affidate ai singoli lavoratori.

L'utilizzo degli strumenti aziendali può essere richiesto e concesso per svolgere attività che non rientrano tra i compiti istituzionali per assolvere incombenze amministrative e burocratiche senza allontanarsi dal luogo di lavoro (ad esempio per adempimenti nei confronti di pubbliche amministrazioni), purché contenuta nei tempi strettamente necessari allo svolgimento delle transazioni.

A titolo esemplificativo, non è consentito:

- l'upload o il download di software, di documenti o file di qualsiasi altra natura, se non strettamente attinenti all'attività lavorativa e previa verifica dell'attendibilità dei siti in questione;
- ogni forma di registrazione utilizzando riferimenti dell'ente a siti i cui contenuti non siano strettamente legati all'attività lavorativa;
- la partecipazione a Forum non professionali, l'utilizzo di chat, di social network, di strumenti di condivisione, di bacheche elettroniche e le registrazioni in guestbooks anche utilizzando pseudonimi (nickname) se non espressamente autorizzati dal proprio Responsabile.

Al fine di prevenire, per quanto e ove possibile, comportamenti scorretti durante la navigazione in Internet, o per esigenze tecniche, l'ente (laddove la strumentazione informatica lo permetta) si avvale di appositi filtri opportunamente configurati che impediscono l'accesso a siti non ritenuti idonei.

I filtri sopracitati limitano l’accesso ai siti Internet che presentano i seguenti contenuti:
- illegali o non etici, stupefacenti, razzismo e odio, estremismo, violenza, occultismo,plagio;
- materiale per adulti, nudità, pornografia;
- giochi, scommesse, intermediazione e trading, download software freeware;
- social network, radio e tv via Internet (salvo i casi espressamente autorizzati dalla Direzione Generale);
- peer to peer;
- malware, spyware, hacking, bypass proxy, phishing.

Qualsiasi altra tipologia di contenuti o siti che la Direzione Generale / Segretario / Sindaco riterrà di non dover rendere accessibile dalla rete aziendale, verrà preventivamente comunicata agli utenti.

La navigazione, ovvero l’accesso ai siti Internet, potrebbe avvenire previa autenticazione dell’Utente sul proxy.

I file contenenti le registrazioni della navigazione sul web sono conservati per il tempo strettamente necessario, determinato dalle norme in vigore e da esigenze di sicurezza.

Art. 14.1 - Utilizzo dei Social Network per scopi istituzionali

L’utilizzo dei Social Network per scopi istituzionali è consentito a coloro i quali sono stati individuati dalla propria struttura quali referenti.

Dal momento che si tratta di comunicazione effettuata in nome e per conto dell’ente, l’associazione tra il singolo utente e il profilo dell’ente deve essere esplicitamente autorizzata.

Nel caso di account social intitolati all’ente o a qualsiasi struttura ad esso riferibile le credenziali di accesso devono essere custodite dai Sistemi Informativi o facente funzione, secondo le regole di cui al punto 8.1 del presente regolamento. Le persone incaricate di operare in nome e per conto dell’ente verranno quindi abilitate singolarmente.

In considerazione del pubblico di riferimento, stile e contenuti delle comunicazioni effettuate tramite Social Network dovranno essere redatti secondo le indicazioni fornite dal dirigente/responsabile di riferimento.

Art. 15 - Posta Elettronica

Il servizio di posta elettronica è un mezzo istituzionale di comunicazione dell'ente ed il suo utilizzo deve avvenire nel rispetto delle norme in materia di protezione dei dati personali.

Sono attribuiti indirizzi di posta elettronica a:

- Strutture organizzative e per lo svolgimento di particolari funzioni (es:ufficio@comune.nome.cr.it);
- Utenti dell'ente (es: inizialenome.cognome@comune.nome.cr.it).

L'uso degli indirizzi di Struttura deve essere dedicato alle comunicazioni ufficiali sia interne che esterne all'ente.

Non è consentito l'utilizzo dell'indirizzo di posta nominativo o di Struttura per scopi diversi da quelli prettamente lavorativi.

L'assegnazione di un indirizzo di posta elettronica avviene contestualmente all'assegnazione delle credenziali di autenticazione dell'Utente; di norma l'indirizzo di posta viene creato utilizzando il carattere iniziale del nome + il "." + l'intero cognome sotto lo stesso dominio istituzionale: @comune.nome.cr.it.

I casi di omonimia sono gestiti aggiungendo il secondo (terzo, quarto...) carattere iniziale del nome.

L'accesso al servizio di posta elettronica da parte di un Utente avviene mediante le credenziali di autenticazione (nome utente e password).

Gli utenti assegnatari delle caselle di posta elettronica sono i diretti responsabili del corretto utilizzo delle stesse e rispondono personalmente dei contenuti trasmessi.

In particolare l'Utente è tenuto a rispettare quanto segue:

1. non utilizzare il servizio per scopi illegali o non conformi al presente Regolamento o in maniera tale da recare danno o pregiudizio all'ente o a terzi;

2. non utilizzare il servizio in modo da danneggiare, disattivare, sovraccaricare, pregiudicare o interferire con la fruibilità del servizio da parte degli altri utenti;

3. non utilizzare la posta elettronica per inviare, anche tramite collegamenti o allegati in qualsiasi formato (testo, fotografico, video, grafico, audio, codice, ecc.), messaggi che contengano o rimandino ad esempio a: pubblicità non istituzionale, manifesta o occulta; prodotti di natura politica; comunicazioni commerciali private; materiale pornografico o simile; materiale discriminante o lesivo in relazione a razza, sesso,

religione, ecc.; materiale che violi la legge sulla privacy; contenuti o materiali che violino i diritti di proprietà di terzi; altri contenuti illegali. In nessun caso l'Utente potrà utilizzare la posta elettronica per diffondere codici dannosi per i computer quali virus e simili.

Di seguito si elencano alcune norme di comportamento che ciascun Utente è tenuto ad osservare al fine di preservare l'efficienza del servizio di posta elettronica e delle comunicazioni con esso veicolate:

- l'Utente è tenuto a visionare regolarmente la casella di posta elettronica di propria competenza;
- i messaggi devono essere preferibilmente di solo testo, evitando ove possibile ogni formattazione e inserzione di immagini;
- è buona norma inviare messaggi sintetici che descrivano in modo chiaro il contenuto;
- è necessario indicare sempre chiaramente l'oggetto, in modo tale che il destinatario possa immediatamente individuare l'argomento del messaggio ricevuto, facilitandone la successiva ricerca per parola chiave;
- non superare la dimensione complessiva di 10 Megabyte degli allegati inviati con un singolo messaggio;
- limitare l'invio di messaggi di posta elettronica a indirizzi plurimi (decine di destinatari) e trasmetterli solo in casi motivati da esigenze di servizio.

L'Utente, infine, si impegna a non inviare messaggi di natura ripetitiva (catene di S. Antonio) anche quando il contenuto sia volto a segnalare presunti o veri allarmi (esempio: segnalazioni di virus).

Particolare attenzione va riposta agli allegati:

- aprire solo allegati di cui si conosce natura del mittente e di cui si è certi della necessità;
- non aprire email o allegati per cui si abbia anche il minimo dubbio dell'origine o del contenuto. Contattare i Sistemi Informativi o chi ne fa la funzione prima di procedere.

Art. 15.1 - Le liste di distribuzione (mailing list)

Allo scopo di facilitare l'interscambio di informazioni relative a scopi istituzionali è possibile l'uso delle liste di distribuzione (mailing list).

In linea di principio sarebbe da perseguire, per gli interscambi formali all'interno dell'ente e verso l'esterno, l'uso delle liste di distribuzione di struttura.

Occorre incentivare e favorire l'uso di tali liste evitando trasmissioni al singolo dipendente ma favorendo gli invii delle comunicazioni formali da indirizzi di struttura

verso le liste delle strutture cui afferiscono i destinatari.

Per facilitare lo scambio di informazioni funzionali alle attività svolte, è possibile far attivare più liste all'interno della stessa Struttura che rispecchino particolari funzioni: la soluzione deve essere funzionale all'organizzazione delle Strutture ed all'ottimizzazione della comunicazione interna e per questo, quindi, deve rispondere a principi di semplificazione.

Al fine di non duplicare le comunicazioni è opportuno che una comunicazione e-mail inviata ad una lista di distribuzione non venga anche contemporaneamente inviata all'indirizzo individuale.

La richiesta di attivazione di una lista di distribuzione (es: account di Struttura, di progetto o di una particolare attività o funzione condivisa) deve essere avanzata da parte di un Responsabile (di Struttura o di Progetto) e contenere l'elenco dei nominativi che devono essere inseriti nella relativa lista di distribuzione.

Il Responsabile sopracitato è tenuto a verificare, almeno annualmente, la necessità di mantenere attive le liste di distribuzione a lui afferenti e l'elenco dei nominativi abilitati.

Una lista generale di distribuzione comprendente tutti gli utenti è gestita centralmente da parte degli amministratori di posta elettronica.

L'utilizzo di questa lista è consentito a particolari Strutture appositamente autorizzate da parte della Direzione Generale.

Art. 15.2 - Regole d'uso, accesso alternativo e cessazione caselle mail

Le caselle di posta hanno una dimensione predefinita e di norma non estendibile; occorre pertanto mantenere in ordine la propria casella di posta badando a ripulirla con regolarità e salvando gli allegati ingombranti.

Al fine di garantire la continuità all'accesso dei messaggi da parte dei soggetti adibiti ad attività lavorative che richiedono la condivisione di una serie di documenti si consiglia e si incoraggia l'utilizzo abituale di caselle di posta elettronica condivise tra più lavoratori o delle caselle di posta istituzionali dell'ente eventualmente affiancandole a quelle individuali.

In caso di assenza prolungata programmata del dipendente, si consiglia e si raccomanda al dipendente di attivare il sistema di risposta automatica ai messaggi di posta elettronica ricevuti indicando, nel messaggio di accompagnamento, le coordinate

di un collega o della struttura di riferimento che può essere contattata in sua assenza e/o altre modalità utili di contatto della Struttura organizzativa dell'ente presso cui presta la propria attività lavorativa.

Nell'ipotesi di assenza o impossibilità, temporanea o protratta nel tempo, del dipendente, qualora per ragioni di sicurezza o comunque per garantire l'ordinaria operatività aziendale sia necessario accedere a informazioni o documenti di lavoro presenti sul personal computer del dipendente, inclusi i messaggi di posta elettronica in entrata ed in uscita, il dipendente può delegare un altro dipendente a sua scelta (fiduciario) il compito di verificare il contenuto di messaggi ed inoltrare al responsabile della Struttura in cui lavora quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa.

Di tale attività deve essere redatto apposito verbale ed informato il dipendente interessato alla prima occasione utile.

In caso di assenza o impossibilità, temporanea o protratta nel tempo, del dipendente, qualora per ragioni di sicurezza o comunque per garantire l'ordinaria operatività aziendale sia necessario accedere a informazioni o documenti di lavoro presenti sul personal computer del dipendente, inclusi i messaggi di posta elettronica in entrata e in uscita, e il dipendente non abbia delegato un altro dipendente (fiduciario), secondo quanto sopra specificato, il responsabile della struttura cui afferisce il dipendente può chiedere all'Amministratore del Sistema ed al Dirigente Responsabile del Servizio Sistemi Informativi o facente funzione di accedere alla postazione e/o alla casella di posta elettronica del dipendente assente, in modo che si possa prendere visione delle informazioni e dei documenti necessari.

Contestualmente, il responsabile della struttura deve informare il dipendente appena possibile, fornendo adeguata spiegazione e redigendo apposito verbale.

Le caselle di posta individuali hanno validità pari alla durata della permanenza in servizio del dipendente, fatte salve eventuali situazioni di congedo, distacco e comando.

Nel caso in cui il dipendente non presti più la sua attività lavorativa presso l'ente, la casella di posta elettronica sarà prontamente disattivata.

Su richiesta dell'interessato la casella di posta potrà restare attiva per ulteriori 3 mesi dalla data di cessazione del rapporto di lavoro, durante il quale sarà inserita una risposta automatica d'ufficio.

Se per esigenze lavorative sorge la necessità di accedere al contenuto di tale casella di posta, il Responsabile della Struttura organizzativa a cui il dipendente era assegnato potrà inoltrare motivata richiesta all'Amministratore di Sistema ed al Dirigente Responsabile del Servizio Sistemi Informativi o facente funzione.

Nell'ipotesi di assenza o impossibilità, temporanea o protratta nel tempo, del dipendente qualora per ragioni di sicurezza o comunque per garantire l'ordinaria operatività aziendale sia necessario accedere a informazioni o documenti di lavoro presenti sul personal computer del dipendente il dipendente lo può effettuare da remote attraverso la modalità del telelavoro/smart working, garantendo lo stesso livello di protezione del dato ed impedendo a terzi di accedere a questa modalità di lavoro attraverso la comunicazione delle sue credenziali personali, dei dati contenuti nel server del Comune oppure in ogni altra forma che permettano ad un terzo non autorizzato la vision dei dati del Comune in ogni forma o modalità.

Art. 16 - Creazione di programmi o documenti automatizzati

In caso di creazione di software e altre procedure informatiche da parte di Strutture dell'ente o commissionati a soggetti terzi, devono essere resi disponibili all'ente

- l'accesso al codice sorgente ed alle basi dati;
- l'analisi e la documentazione sul funzionamento e l'installazione;
- i metadati sulle strutture dati eventualmente implementate.

La proprietà di quanto sopra, inclusi i diritti derivanti, sono dell'ente salvo il diritto di essere riconosciuto autore dell'invenzione [Titolo IX del Libro Quinto del Codice Civile, D.lgs. 518 del 29 dicembre 1992 che novella la legge 633/41].

Art. 17 - Proprietà intellettuale e delle licenze d'uso

Tutto il software in uso nel sistema informativo dell'ente in cui sia prevista una licenza d'uso deve essere registrato a nome dell'ente stesso.
Tutto il software deve essere individuato dall'Area Funzionale competente in materia, anche dietro suggerimento e supervisione dell'RTD (Responsabile della Transizione al Digitale).

Non è possibile installare, duplicare o utilizzare software acquisiti al di fuori di quanto consentito dagli accordi di licenza e da quanto approvato dai Sistemi Informativi, da RTD o da chi ne fa funzione.

Tutti gli utenti sono tenuti al rispetto delle leggi in materia di tutela della proprietà

intellettuale, sia per quanto riguarda il software che per quanto riguarda i file di qualsiasi altra natura.

Art. 18 - Crittografia e controllo dei dati informatici

Fatto salvo quanto previsto dal Regolamento UE 2016/679 (GDPR) in materia di archiviazione, gestione, trattamento e trasmissione di dati particolari, è fatto divieto di applicare sistemi di crittografia dati, se non espressamente richiesto e/o autorizzato dal Responsabile di struttura.

Art. 19 - Utilizzo e conservazione dei supporti rimovibili

I supporti rimovibili (hard disk esterni, CD e DVD riscrivibili, supporti USB, ecc.) non costituiscono un sistema di archiviazione dei dati. Di conseguenza i Sistemi Informativi o chi ne fa funzione non avvieranno nessuna operazione di recupero di dati salvati su di essi.

I supporti rimovibili dovranno essere utilizzati per il trasferimento di dati solo quando altri meccanismi non siano disponibili.

Va evitato, tranne che per casi particolari adeguatamente motivati, di utilizzare supporti rimovibili per la memorizzazione di dati sensibili nonché informazioni costituenti know-how aziendale. In caso sia necessario, il dispositivo va cifrato. Per la cifratura chiedere supporto ai Sistemi Informativi o all'azienda che dà supporto informatico.

Se ciò dovesse avvenire, tali supporti dovranno essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto o recuperato successivamente alla cancellazione.

In ogni caso, i supporti contenenti dati sensibili devono essere adeguatamente custoditi, possibilmente in cassetti e armadi provvisti di chiusura.

A tal proposito si ricorda che l'utente è responsabile non solo della custodia dei supporti ma anche dei dati aziendali in essi contenuti.

Nel caso di utilizzo condiviso dei medesimi supporti da parte di più utenti, occorre provvedere alla cancellazione delle informazioni ivi contenute mediante opportuni programmi (es. CLEANER in modalità sovrascrittura avanzata).

Nel caso di smaltimento, i supporti dovranno essere prima distrutti mediante punzonatura o deformazione meccanica o distruzione fisica o demagnetizzazione.

Art. 20 - Protezione antivirus

Il sistema informatico ed i PC collegati alla rete dell'ente sono protetti da software antivirus aggiornati quotidianamente.

Ogni Utente è comunque tenuto a comportarsi in modo tale da ridurre il rischio di attacco al sistema informatico aziendale da parte di virus o attraverso qualsiasi altro software "aggressivo".

Le stesse regole dovranno essere rispettate da parte di Soggetti terzi fornitori/gestori di apparecchiature e servizi informatici che vengono utilizzati a qualsiasi titolo all'interno della rete aziendale.

Art. 21 - Scanner di rete e fax

Deve essere privilegiato l'utilizzo dello scanner di rete alle fotocopie tradizionali.

Il Responsabile della Struttura deve individuare formalmente i dipendenti che devono dismettere l'utilizzo del fax progressivamente e comunque presidiarvi i contenuti in caso arrivino.

Non è consentito installare apparati fax tradizionali o software di gestione fax diversi da quelli forniti dall'ente previa autorizzazione e supporto da parte di questa.

Si raccomanda di non lasciare documenti incustoditi negli apparati tradizionali (fax, fotocopiatrici, scanner e stampanti di rete).

Art. 22 - Teleassistenza

Per lo svolgimento di normali attività di manutenzione su personal computer connessi alla rete, il personale del Servizio Sistemi Informativi o facente funzione e di fornitori potrà utilizzare specifici software di connessione remota.

Tali programmi sono necessari per compiere interventi di assistenza informatica e manutenzione su applicativi ed hardware in uso presso l'Utente.

L'attività da remoto di assistenza e manutenzione avviene previa autorizzazione da parte dell'utente interessato e possibilmente mediante visualizzazione di un indicatore visivo sul monitor dell'utente che segnala la connessione in remoto del tecnico e l'accesso al dato dell'operatore che si collega da remoto.

L’accesso al dato da remoto è infatti possibile mediante teleassistenza a va monitorato.

Art. 23 - Monitoraggio e controlli

L’ente adotterà ogni accorgimento tecnico necessario a tutelarsi da eventuali comportamenti non consentiti, salvaguardando il rispetto della libertà e della dignità dei lavoratori; gli eventuali trattamenti effettuati saranno ispirati a canoni di trasparenza e rispetteranno il principio di pertinenza e non eccedenza.

Art. 23.1 - Monitoraggio

Il Servizio Sistemi Informativi o facente funzione effettua monitoraggi periodici su dati anonimi allo scopo di verificare l’attuazione del presente Regolamento, i possibili rischi alla sicurezza informatica e le possibili problematiche inerenti l’utilizzo degli strumenti informatici.

Questi monitoraggi si possono classificare in:

- analisi del traffico di rete, effettuate attraverso specifici log dei dispositivi di rete;
- analisi del traffico Internet, effettuate attraverso specifici log dei dispositivi di connessione ad Internet;
- inventario Hardware e Software, effettuati attraverso procedure prevalentemente automatiche per le apparecchiature collegate in rete ed in maniera semiautomatica per le altre macchine.

Il monitoraggio delle risorse hardware e software non coinvolge in alcun modo i dati personali ed i documenti presenti sulle singole postazioni di lavoro né si configura come attività di controllo del lavoro del dipendente, e viene effettuato per finalità organizzative e gestionali.

I dati del traffico telematico saranno gestiti secondo le modalità e le tempistiche previste dalla normativa vigente in materia di sicurezza dei dati del traffico telefonico e telematico.

L’ente si riserva la facoltà di procedere alla rimozione di ogni file o applicazione che riterrà pericolosa per la sicurezza del sistema informatico ovvero acquisita o installata in violazione del presente Regolamento.

Art. 23.2 - Controlli

L’ente si riserva di effettuare controlli per verificare il rispetto del Regolamento.

Riguardo a tali controlli il presente Regolamento costituisce preventiva e completa informazione nei confronti dei dipendenti.

In base al principio di correttezza l'eventuale trattamento deve essere ispirato ad un canone di trasparenza, come prevede anche la disciplina di settore (Art. 4, secondo comma, Statuto dei lavoratori).

I dati devono essere gestiti soltanto dai soggetti preventivamente designate in qualità di persona autorizzata al trattamento, come precisano gli art. 29 e 32 del GDPR.

Nel caso in cui emerga un evento dannoso, una situazione di pericolo o utilizzi non aderenti al presente Regolamento, che non siano stati impediti con preventivi accorgimenti tecnici o rilevati durante i monitoraggi o da attività di gestione degli strumenti informatici, la Direzione Generale, attraverso il Servizio Sistemi Informativi o facente funzione, potrà adottare le eventuali misure che consentano la verifica di tali comportamenti preferendo, per quanto possibile, un controllo preliminare su dati aggregati riferiti all'intera Struttura organizzativa o a sue articolazioni.

Il controllo su dati anonimi si terminerà in una comunicazione al Responsabile della Struttura analizzata che si preoccuperà di inviare un avviso generalizzato relativo a un utilizzo non corretto degli strumenti aziendali, invitando i destinatari ad attenersi scrupolosamente al presente Regolamento.

Qualora le anomalie e irregolarità dovessero persistere, si procederà circoscrivendo l’invito al personale afferente alla Struttura in cui è stata rilevata l’anomalia.
In caso di reiterate anomalie o irregolarità, saranno effettuati controlli su base individuale.

In nessun caso, a eccezione di specifica richiesta da parte dell’Autorità Giudiziaria, verranno poste in essere azioni sistematiche quali:
- la lettura e la registrazione dei messaggi di posta elettronica (al di là di quanto tecnicamente necessario per lo svolgimento del servizio di gestione e manutenzione della posta elettronica);
- la riproduzione ed eventuale memorizzazione delle pagine web visualizzate dal lavoratore;
- la memorizzazione di quanto visualizzato sul monitor.

Oltre a ciò l’ente si riserva di effettuare specifici controlli sui software caricati sui personal computer utilizzati dai dipendenti al fine di verificarne la regolarità sotto il profilo delle autorizzazioni e delle licenze, nonché, in generale, la conformità degli stessi

alla normativa vigente e, in particolare, alle disposizioni in materia di proprietà intellettuale.

Oltre a tali controlli di carattere generale, l'ente si riserva comunque le facoltà previste dalla normativa vigente di effettuare specifici controlli ad hoc nel caso di segnalazioni di attività che hanno causato danno all'ente stesso, che ledono diritti di terzi o che, comunque, sono illegittime.

Art. 24 - Sanzioni

È fatto obbligo a tutti gli utenti di osservare le disposizioni contenute nel presente Regolamento.

Il mancato rispetto o la violazione delle indicazioni ivi contenute è perseguibile nei confronti del personale dipendente con provvedimenti disciplinari e risarcitori previsti dai vigenti CCNL, nonché con le azioni civili e penali conseguenti previste dalla normativa vigente in materia.

Ogni dipendente dovrà assumersi la piena responsabilità per le proprie azioni e dovrà farsi garante per l'ente e tenerlo indenne da responsabilità e richieste di rimborsi di danni, avanzate da soggetti terzi.

Art. 25 - Applicabilità a soggetti diversi dai dipendenti

Con riferimento ai collaboratori e/o prestatori d'opera (consulenti, stagisti, etc.), qualora questi per l'espletamento del loro incarico si servissero degli strumenti e servizi informatici dell'ente, deve essere previsto nell'ambito del contratto l'obbligo di rispettare il presente Regolamento, con diritto dell'ente stesso, nei casi di violazione di particolare gravità, di risolvere il contratto stesso.

Riferimenti Normativi

General Protection Data Rule

General Protection Data Rule