COMUNE DI TREVENZUOLO

PROVINCIA DI VERONA

Regolamento per la protezione dell'informazione e dei dati

1 Introduzione e finalità del presente documento 2

1.1 Definizioni 3

1.2 Contesto normativo 7

1.3 Ambito di applicazione e Principi generali 8

2 Regole di comportamento 9

2.1 Accesso ai locali ove vengono custoditi dispositivi di archiviazione 9

2.2 Regole di utilizzo per una corretta gestione delle postazioni di lavoro 10

2.3 Credenziali e Password 14

2.4 Uso appropriato dei privilegi di amministratore anonimi 16

3 Utilizzo di posta elettronica, internet, notebook, tablets, smartphone, cellulari, stampanti 17

3.2 Notebook, Telefoni, cellulari, stampanti, fotocopiatrici, scanner e fax 17

3.3 Navigazione Internet e utilizzo della rete 18

3.4 Partecipazione ai social media 21

3.5 Posta elettronica 22

4 Manutenzione, modifiche, furto o smarrimento delle risorse ICT 25

5 Protezione Antivirus 25

6 Controlli 26

6.1 Modalità operative su Controlli per la tutela del patrimonio dell'Ente, nonché per la sicurezza e la salvaguardia del sistema informatico. Controlli per ulteriori motivi tecnici e/o manutentivi. 27

6.2 Controlli per esigenze produttive e di organizzazione 27

7 Conservazione 28

8 Violazioni 29.29

1 Introduzione e finalità del presente documento

La progressiva diffusione delle nuove tecnologie informatiche (riferendosi in particolar modo a dispositivi mobili quali notebook, tablet, smartphone nonché alla posta elettronica ed alle applicazioni di cui l'Amministrazione ammette l'uso) utilizzate sempre più frequentemente per lo svolgimento dell'attività lavorativa nonché l'utilizzo della rete internet espone l'Ente e gli utenti (dipendenti e collaboratori) a minacce che possono riguardare la sicurezza delle informazioni e in particolar modo il dato (inteso come dato personale ma anche come ogni informazione di cui l'amministrazione dispone). Esso può essere compromesso nelle sue tre caratteristiche: disponibilità, riservatezza, integrità. Nel caso in cui il dato venga perso (disponibilità), modificato (integrità) o divulgato a terzi (riservatezza) vi potrà essere un danno oltre che all'interessato (nel caso in cui si stia parlando di dato personale) anche all'Amministrazione in quanto si potrà creare un danno legale, materiale (economico), immateriale (danno all'immagine e al buon andamento dell'Amministrazione) od operativo (nel caso in cui si verifichi l'interruzione dei servizi da parte della Pubblica Amministrazione).

Al fine quindi di minimizzare tali rischi e consapevolizzare i soggetti che operano con tali strumenti sulle criticità che essi comportano, con il presente documento, si rende opportuno disciplinare le modalità di utilizzo degli strumenti informatici.

Il presente regolamento intende quindi fornire ai dipendenti e collaboratori, denominati anche incaricati o utenti, dell'Ente, indicazioni per una corretta e adeguata gestione delle informazioni, in particolare attraverso l'uso di sistemi, applicazioni e strumenti informatici.

È intenzione dell'Ente tutelare, anche attraverso il presente documento, il proprio patrimonio informativo ricomprendendo, in senso ampio, i dati (sia personali che di altro tipo) che la stessa Pubblica Amministrazione si trova a gestire ogni giorno. In particolare, si procederà ad effettuare una classificazione delle informazioni andando a suddividere quelle di dominio pubblico e quelle che invece dovranno rimanere private e, pertanto, tutelate attraverso l'adozione di apposite contromisure (intese quali misure tecniche-organizzative) che l'Amministrazione ha posto in essere o dovrà porre in essere.

Ogni dipendente e collaboratore è tenuto a rispettare il presente regolamento.

Si specifica che tutti gli strumenti utilizzati dal lavoratore, intendendo con ciò i PC, notebook, tablet, cellulari, e-mail ed altri strumenti con relativi software ed applicativi (di seguito più semplicemente "Strumenti"), sono messi a disposizione dall'Ente per rendere la prestazione lavorativa.

Gli strumenti, nonché le relative reti a cui è possibile accedere tramite gli stessi, sono patrimonio dell'Ente.

I dati personali e le altre informazioni dell'utente che sono registrati negli strumenti o che si possono eventualmente raccogliere tramite il loro uso, sono utilizzati per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio dell'organizzazione.

Per tutela del patrimonio dell'organizzazione si intende altresì la sicurezza informatica e la tutela del sistema informatico dell'Ente. Tali informazioni sono altresì utilizzabili per tutti i fini connessi al rapporto di lavoro, nel rispetto della normativa vigente e, comunque, nelle modalità indicate al successivo art. 6 del presente regolamento.

Si vogliono quindi fornire apposite prescrizioni per l'utilizzo delle risorse ICT dell'Ente in modo corretto, conforme alle finalità istituzionali e nel pieno rispetto delle norme di legge, promuovendo al contempo, in tutto il personale, una corretta cultura per la protezione dell'informazione con l'obiettivo di evitare il verificarsi di qualsiasi abuso o uso non conforme, muovendo dalla convinzione che la prevenzione dei problemi sia preferibile rispetto alla loro successiva correzione.

Infine, viene precisato che sui sistemi informatici in uso agli utenti non sono installati o configurati apparati hardware o strumenti software aventi come scopo il controllo a distanza dell'attività dei lavoratori.

1.1 Definizioni

Le risorse ICT messe a disposizione dall' Ente e le informazioni con esse trattate, oggetto di tutela descritte nel presente documento, sono:

- il patrimonio informativo: inteso come il complesso delle informazioni e dei dati gestiti a mezzo strumenti informatici/elettronici, siano essi banche dati memorizzate in database, aree documentali digitalizzate (documenti di vario tipo pdf, testi, fogli di calcolo…), archivi cartacei che in egual misura trattano dati personali, o anche non personali, che possono essere di natura riservata o non riservata e che costituiscono per l'appunto il complesso dei beni conoscitivi in possesso dell'Ente;
- i servizi informatici erogati dall'Amministrazione;
- le postazioni di lavoro (PC desktop e simili) e "mobili" (PC portatili, tablet e smartphone);
- i software di messaggistica (tipo "*messenger, hangouts*" e simili, se previsti);
- *i server*, e tutto il materiale *hardware* in generale.

Si riporta poi un piccolo glossario dei termini maggiormente usati in questo documento:

- *amministratore di sistema*: il soggetto che corrisponde a quanto indicato nel provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008, pubblicato nella G. U. n. 300 del 24 dicembre 2008, e successive modificazioni intervenute

con il Provvedimento del 25 giugno 2009, pubblicato nella G.U. n. 149 del 30 giugno 2009; ovverosia, colui che sovrintende alla gestione dell'infrastruttura informatica e che tratta i dati per finalità di sviluppo, gestione, implementazione, manutenzione dei componenti hardware e software di tale infrastruttura;

- *applicazione:* un programma software inserito in un sistema di telecomunicazioni (es. applicazioni di messaggistica quali *hangout* o *messenger*);
- *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;
- *controllo di sicurezza:* le tutele o contromisure prescritte per un sistema d'informazione o un'organizzazione per proteggere la confidenzialità, l'integrità e la disponibilità del sistema e delle sue informazioni;
- *dato anonimo*: il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;
- *dato identificativo*: dato personale che permette l'identificazione diretta dell'interessato;
- *dato personale:* ai sensi dell'art. 4 del Reg. EU 2016/679, è un "*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.
- *dati particolari:* ai sensi dell'art. 9 Reg. EU 2016/679, i dati che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché quelli genetici, biometrici (tesi a identificare in modo univoco una persona fisica), dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona;
- *dati di cui all' art. 10 del Reg. EU 2016/679, o*vverosia i dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza;
- *dato non personale ma riservato:* tutti quei dati collegati ad interessi giuridicamente rilevanti (come ad es. la proprietà individuale, il diritto d'autore e i segreti commerciali);
- *dato non personale e non riservato*: gli (open data) dato aperto, o (open access) ad accesso libero o (open use) di libero utilizzo;
- *disponibilità:* proprietà che rende l'informazione immediatamente accessibile ed utilizzabile, entro i termini stabiliti, su richiesta di un'entità autorizzata;

- *dispositivi mobili:* un dispositivo informatico portatile che ha una forma ridotta tale da essere trasportato facilmente da un singolo individuo; è disegnato affinché possa operare senza una connessione fisica (ad esempio trasmette in modalità wireless e riceve informazioni); possiede una memoria dati locale non removibile ed è acceso per lunghi periodi di tempo con una fonte di alimentazione autonoma. I dispositivi mobili possono anche includere capacità di comunicazione vocale, sensori che consentono al dispositivo di acquisire (es. fotografare, registrare video, determinare o registrare la posizione) informazioni nonché funzionalità integrate per sincronizzare dati locali con postazioni remote (es.: telefoni cellulari, smartphone, laptop, notebook, tablet, e-reader);
- *hardware:* i componenti fisici/materiali di un sistema;
- *integrità:* implica la garanzia che le informazioni non possano essere modificate o addirittura cancellate in seguito ad azioni non autorizzate, volontarie o involontarie, ma anche per danni o malfunzionamenti dei sistemi;
- *identificatore:* dati univoci utilizzati per rappresentare l'identità di una persona e associarne gli attributi (es.: il nome, il numero di carta); consistono in un'etichetta unica utilizzata dal sistema per identificare una specifica entità, oggetto o gruppo;
- *informazione:* visione della realtà derivante dall'elaborazione e interpretazione dei dati; il significato che associamo ai dati;
- *informazioni da proteggere*: si veda il patrimonio informativo così come definito all'inizio del presente articolo;
- *minaccia:* potenziale causa di un incidente non voluto che può comportare un danno al sistema o all'organizzazione complessivamente intesa*;*
- *riservatezza:* è la capacità dell'informazione di essere disponibile in un dato momento solo ad individui, ad entità o a processi autorizzati. In altri termini, questa proprietà assicura che le informazioni riservate non siano comunicate o addirittura divulgate a soggetti non legittimati ad accedervi;
- *sicurezza:* una condizione che risulta dalla creazione e dal mantenimento di misure protettive, che consente ad un'organizzazione di svolgere la sua missione o le sue funzioni principali nonostante i rischi rappresentati dalle minacce derivanti dall'uso dei propri sistemi;
- *sicurezza nell'informazione:* protezione dei sistemi informativi da accesso non autorizzato, uso, scoperta, interruzione, modifica o distruzione al fine di proteggere l'informazione nelle sue tre caratteristiche di disponibilità, integrità, riservatezza;
- *sistema:* un'associazione organizzata di risorse e procedure unite e regolate da un'interazione o interdipendenza per realizzare un set di specifiche funzioni. I sistemi

includono anche specifici sistemi come sistemi industriali di controllo, commutazioni telefoniche e sistemi di scambio di succursali private e sistemi di controllo ambientali. Una combinazione di elementi interconnessi organizzati ad uno o più scopi dichiarati. Ci sono molti tipi di sistemi. Esempi includono: sistemi di informazione per scopi generali e speciali; comandi, controlli e comunicazioni di sistema; moduli criptati; unità di elaborazione centrale e schede anagrafiche; sistema di controllo industriale; sistemi di controllo del volo;

- *software:* programmi per computer e dati associati che potrebbero essere dinamicamente scritti o modificati durante l'esecuzione;
- *spam:* l'abuso di sistemi di messagistica per inviare indiscriminatamente messaggi collettivi non richiesti;
- *spyware:* software nascosto installato all'interno di un sistema d'informazione per raccogliere informazioni su individui o organizzazioni a loro insaputa; un tipo di codice malevolo;
- *titolare del trattamento*: ai sensi dell'art. 4 Reg. Ue 2016/679 *"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";*
- *trattamento*: ai sensi dell'art. 4 Reg. Ue 2016/679 "qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione";
- *utente:* singolo, o processo del sistema che agisce per mezzo di un individuo, autorizzato ad accedere ad un sistema;
- *vulnerabilità*: carenze riguardanti un sistema di informazione, un sistema di procedure di sicurezza, controlli interni o implementazioni che potrebbero essere sfruttate o attivate da una fonte di minaccia.
-

2 Contesto normativo

Il presente documento fa riferimento al seguente quadro normativo:

- "*Regolamento (Ue) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE*", che sarà direttamente applicabile in tutti gli Stati dell'Unione europea a partire dal 25 maggio 2018 (d'ora in poi "GDPR");
- D.Lgs. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali"(d'ora in poi "Codice Privacy") integrato con le modifiche introdotte dal *D.Lgs 10 agosto 2018, n. 101, Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE(regolamento generale sulla protezione dei dati)*.
- Provvedimenti del Garante per la protezione dei dati personali in materia di "misure di sicurezza", in particolare con riguardo agli Amministratori di Sistema (Provvedimento generale del 27 novembre 2008 e successive modificazioni intervenute con il Provvedimento del 25 giugno 2009, pubblicato nella G.U. n. 149 del 30 giugno 2009)
- Garante della privacy "Linee guida per posta elettronica e internet" del 01.03.2007 pubblicato in Gazzetta Ufficiale n. 5 del 10 marzo 2007.
- Direttiva n. 2/2009 del Dipartimento Funzione Pubblica ad oggetto "Utilizzo di internet e della casella di posta elettronica istituzionale sul luogo di lavoro".
- Legge 20 maggio 1970, n. 300 "*Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro e norme sul collocamento*" (Statuto dei Lavoratori) modificata dall'articolo 23 D.lgs. 14 settembre 2015 n. 151 (così detto *"Decreto sulle semplificazioni"* attuativo della Legge delega 10.12.2014 n. 183, anche nota come *"legge di riforma del diritto del lavoro"* o *"Jobs Act"*).
- Vademecum del 17/03/2020 di AgID "**Le 11 raccomandazioni di AgID per uno Smart working sicuro".**
- **Normativa ISO/IEC 27001:2013.**

1.3 Ambito di applicazione e Principi generali

Le Pubbliche Amministrazioni sono tenute ad assicurare il corretto impiego degli strumenti di telefonia e ICT da parte dei propri operatori, definendone le modalità di utilizzo nell'organizzazione dell'attività lavorativa. Questo avviene nell'ottica di garantire la sicurezza, la disponibilità e l'integrità dei sistemi e di prevenire sprechi. Esiste quindi in capo agli operatori l'obbligo, sancito da norme di legge e di contratto, di adottare comportamenti conformi al corretto espletamento della prestazione lavorativa, e questo anche nell'utilizzo delle risorse dell'Organismo Amministrativo.

In funzione del proprio ruolo e delle esigenze organizzative e lavorative, il personale in servizio presso l'ente è dotato di personal computer, workstation, laptop, smartphone per lo svolgimento di attività connesse agli incarichi lavorativi, nel rispetto delle regole descritte nel presente documento.

In relazione all'utilizzo di Notebook, Telefoni, smartphone, stampanti, fotocopiatrici scanner e fax si rimanda a quanto indicato al successivo art. 3.2.

Il presente regolamento si applica a tutti i dipendenti, senza distinzioni di ruolo e/o di livello, nonché a tutti i collaboratori dell'Ente a prescindere dal rapporto contrattuale con lo stesso intrattenuto, che hanno necessità di usufruire delle risorse ICT dell'Ente.

Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche e telematiche, per "utente" deve intendersi ogni dipendente, collaboratore ed amministratore in possesso di specifiche credenziali di autenticazione. Tale figura potrà anche venir indicata come "incaricato del trattamento" o "autorizzata" o "dipendente/collaboratore".

Il presente documento e le prescrizioni ivi contenute si rivolgono a differenti categorie di soggetti essendo destinati a disciplinare sia il comportamento di Utenti "meri utilizzatori" (fruitori di PC desktop, smartphone, PC portatili, ecc.), sia il comportamento di Utenti che svolgono mansioni tecniche (Amministratori di Sistema, Amministratori di Rete, gestori di banche dati, gestori di servizi, ecc.).

Tutte le attività svolte in applicazione del presente regolamento devono conformarsi ai seguenti principi:

a) *principio di necessità/minimizzazione*, secondo cui i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzo di dati personali e di dati identificativi in relazione alle finalità perseguite e alle basi giuridiche che ne consentono il trattamento (art. 5 e 6 del Reg. UE 2016/679). Inoltre, i dati devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;

b) *principio di pertinenza e non eccedenza,* secondo i quali *i trattamenti devono essere effettuati per finalità determinate, esplicite e legittime* (art. 5 commi 1 e 2 Reg. UE 2016/679);
c) *principio di limitazione della conservazione:* i dati personali devono essere conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati;
d) *principio di integrità e riservatezza:* i dati personali devono essere trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali;
e) *Alle norme indicate al precedente art.* 1.2, nonché alle prescrizioni previste dall'Organizzazione all'interno di eventuali regolamenti/codici di condotta/linee guida/disciplinari/atti e documenti adottati dall'Ente a tutela delle informazioni trattate dalla stessa organizzazione, nonché alle istruzioni fornite dall'Ente al proprio personale.

2 Regole di comportamento

2.1 Accesso ai locali ove vengono custoditi dispositivi di archiviazione

L'accesso ai locali all'interno dei quali sono presenti dispositivi di archiviazione delle informazioni e quelli dai quali è possibile gestire l'infrastruttura informatica dell'Ente è consentito al solo personale autorizzato.

Gli utenti possono essere autorizzati all'accesso solo relativamente all'erogazione di servizi ed in presenza degli operatori dell'Ente. Gli operatori esterni che devono accedere ai locali (ad esempio per attività di manutenzione), devono essere espressamente autorizzati dal responsabile di riferimento dell'Ente. Gli operatori esterni, in ogni caso, devono operare in presenza e sotto la supervisione degli operatori dell'Ente.

Gli operatori esterni all'Ente sono tenuti a svolgere le proprie mansioni senza comprometterne la sicurezza delle risorse e delle informazioni a cui hanno accesso. Qualsiasi intervento, che possa anche minimamente compromettere la sicurezza, deve essere preventivamente comunicato al responsabile di riferimento che ne deve concedere autorizzazione scritta.

In assenza di operatori, tutti i locali all'interno dei quali sono presenti dispositivi di archiviazione delle informazioni e quelli dai quali è possibile gestire l'infrastruttura informatica dell'Ente, devono essere chiusi a chiave o protetti tramite sistema di controllo degli accessi, autorizzati solo al personale addetto. Gli operatori esterni all'Ente, per l'accesso ai locali ed agli

apparati, devono essere autorizzati dal responsabile di riferimento. Le autorizzazioni/revoche devono essere concesse per iscritto. L'accesso al personale esterno all'Ente, anche se autorizzato, è consentito esclusivamente alla presenza di addetti dell'Ente.

I responsabili possono controllare, attraverso visite ispettive ai locali, la corretta applicazione della presente procedura operativa di sicurezza degli accessi. Gli operatori dell'Ente devono provvedere alla chiusura dei locali.

Con riferimento alle **informazioni da proteggere**, contenute in **supporti cartacei** ed assegnate ai singoli operatori, al termine della giornata lavorativa o comunque quando i locali non sono presidiati, i suddetti supporti cartacei devono essere chiusi a chiave negli appositi armadi o cassettiere.

2.2 Regole di utilizzo per una corretta gestione delle postazioni di lavoro

L'utente nel rispetto di quanto esposto ai punti precedenti dovrà quindi osservare quanto segue:

- Evitare che su dischi fissi, supporti di archiviazione o sulla postazione siano presenti documenti/banche dati appartenenti al precedente utilizzatore. In caso si rilevi tale situazione deve essere immediatamente contattato il Responsabile di riferimento.
- L'accesso agli Strumenti dell'Ente è protetto da password; per l'accesso devono essere utilizzati Username e password assegnati, nel rispetto comunque di quanto indicato al successivi artt. 2.3 e 2.4.
- Il Personal Computer, notebook, tablet ed ogni altro hardware deve essere custodito con cura da parte degli assegnatari evitando ogni possibile forma di danneggiamento e segnalando tempestivamente al personale preposto ogni malfunzionamento e/o danneggiamento. Sui dispositivi portatili e dove è possibile, si consiglia la criptazione delle memoria di massa (bitlocker o altro) e l'attivazione della password d'accensione (BIOS/UEFI).
- L'utente è tenuto a scollegarsi dal sistema, o bloccare l'accesso, ogni qualvolta sia costretto ad assentarsi dal locale nel quale è ubicata la stazione di lavoro (PC) o nel caso ritenga di non essere in grado di presidiare l'accesso alla medesima: lasciare un PC incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso. L'ufficio dedicato alla gestione dei sistemi informativi può prevedere soluzioni tecniche atte alla sospensione momentanee del sistema.
- L'utente è tenuto a presidiare le risorse ICT al fine di evitare l'accesso a soggetti terzi non autorizzati. Qualora ciò non sia possibile, bloccare i dispositivi connessi alla rete.
- Le informazioni archiviate sul PC locale devono essere esclusivamente quelle necessarie all'attività lavorativa assegnata nel corso della giornata e pertanto ogni informazione deve essere riposta nella opportuna area del Server di archiviazione.

- Costituisce buona prassi effettuare con cadenza periodica (almeno una volta al mese) la pulizia degli archivi presenti sulla propria postazione e nelle cartelle di rete di propria competenza, con cancellazione dei file inutili o obsoleti. Si deve porre particolare attenzione ad evitare un'archiviazione ridondante con duplicazione dei dati.
- La gestione dei dati su PC è demandata all'utente utilizzatore che dovrà provvedere a memorizzare sulle condivisioni dell'Ente, dati che possono essere utilizzati anche da altri utenti, evitando di mantenere l'esclusività su di essi.
- Non è consentita l'installazione di programmi diversi da quelli autorizzati dall'ufficio deputato alla gestione dei sistemi informativi dell'Ente.
- Gli amministratori di sistema o l'ufficio preposto alla gestione dei sistemi informativi possono in qualunque momento procedere alla rimozione di ogni file o applicazione che riterranno essere pericolosi per la sicurezza dei PC, della rete locale e dei server dell'Ente, nonché tutte le impostazioni eventualmente configurate che possano interferire con il corretto funzionamento dei servizi informatici dell'Ente.
- La riproduzione o la duplicazione di programmi, può essere effettuata solo nel pieno rispetto della vigente normativa in materia di protezione della proprietà intellettuale.
- È vietato l'utilizzo di supporti di memoria (chiavi USB, CD, DVD o altri supporti) per il salvataggio di dati trattati tramite gli Strumenti Dell'Ente, salvo che il supporto utilizzato sia stato fornito dall'ufficio deputato alla gestione dei sistemi Informativi. In tale caso, il supporto fornito può essere utilizzato esclusivamente per finalità lavorative. Eventuali CD-ROM e DVD da eliminare vanno distrutti nel distruggi-documenti o rotti in più pezzi. Eventuali key-memory o hard disk esterni non funzionanti vanno immediatamente consegnati all'Amministratore del Sistema per lo smaltimento in sicurezza. La cancellazione dei dati avviene con modalità sicure tali da rendere irrecuperabile il dato ed impedirne la disponibilità ad alcun soggetto, anche mediante sovra-registrazione, così come indicato dal Garante per la Protezione dei Dati Personali con Provvedimento del 13 ottobre 2008 - "Rifiuti di apparecchiature elettriche ed elettroniche (Raee) e misure di sicurezza dei dati personali".
- È proibito duplicare documenti contenenti dati personali particolari su supporti removibili o su sistemi di rete non gestiti dal personale dell'Ente (ad es. su cloud) repository esterni (quali ad esempio Dropbox, GoogleDrive, OneDrive, etc.), se non espressamente consentito dall'Amministratore di Sistema.
- Nel caso in cui esista la necessità di elaborare banche dati in locale, ad esempio su fogli di calcolo o database personali, è necessario adottare le misure di sicurezza idonee a garantire il rispetto della normativa in materia di tutela dei dati personali.

- E' proibito trasportare le postazioni di lavoro "fisse" al di fuori delle sedi dell'Amministrazione, salvo specifica autorizzazione;
- E' opportuno procedere allo spegnimento delle postazioni di lavoro "fisse", al termine dell'orario di lavoro, salvo particolari esigenze di servizio autorizzate dal Direttore di struttura o di riferimento.

I log relativi all'utilizzo di Strumenti informatici, reperibili nella memoria in essi allocata, ovvero sui Server o sui router dell'Ente, nonché i file con essi trattati sono registrati e possono essere oggetto di controllo da parte del datore di lavoro (individuato all'interno della struttura organizzativa), attraverso l'ufficio deputato alla gestione dei sistemi informativi dell'Ente, per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio dell'Ente.

I controlli possono avvenire secondo le disposizioni previste al successivo art. 6 del presente Regolamento.

Le suddette norme comportamentali devono essere osservate anche nei casi di utilizzo di risorse informatiche non fornite direttamente dall' ufficio deputato alla gestione dei sistemi informativi dell'ente, ma acquisite a vario titolo nel corso del tempo.

Al solo fine di prestare assistenza tecnica informatica ai lavoratori, l'Ente utilizza alcuni software (teleassistenza) che permettono all'amministratore di sistema (previo consenso dell'utilizzatore finale) di vedere in tempo reale le attività svolte dal lavoratore all'interno della propria sessione di lavoro ed eventualmente di intervenire attivamente.

In ordine alla protezione delle informazioni, indipendentemente dallo strumento utilizzato, il dipendente deve attenersi alle seguenti regole di comportamento:

a) È vietato comunicare a soggetti non specificatamente autorizzati i dati personali (di qualunque tipo intesi), elementi e informazioni dell'Ente dei quali il dipendente / collaboratore viene a conoscenza nell'esercizio delle proprie funzioni e mansioni all'interno dell'Ente. In caso di dubbio, è necessario accertarsi che il soggetto cui devono essere comunicati i dati sia o meno autorizzato a riceverli, mediante richiesta preventiva al proprio Responsabile dell'area/funzione.
b) È vietato modificare, estrarre originali e/o copie cartacee ed informatiche per uso personale di documenti, manuali, fascicoli, lettere, data base e quant'altro, salvo esplicita autorizzazione da parte del Responsabile di riferimento.
c) È vietato alterare l'informazione.
d) È vietato lasciare incustoditi documenti, lettere, fascicoli, appunti e quant'altro possa contenere dati personali e/o informazioni dell'Ente quando il dipendente/collaboratore si

allontana dalla postazione di lavoro. È vietato lasciare sulla postazione di lavoro (scrivania, bancone etc.) materiali che non siano inerenti la pratica che si sta trattando in quel momento. Ciò vale soprattutto nel caso di personale con mansioni di front office.

e) E' vietato divulgare a familiari ed amici dettagli dell'attività svolta e della struttura informatica comunale.
f) E' vietato colloquiare con colleghi di attività d'ufficio, al telefono o di persona, in presenza di estranei.
g) E' vietato gettare atti e/o appunti d'ufficio nella spazzatura, se non dopo averli debitamente parcellizzati tramite i sistemi distruggi-documenti o altro idoneo sistema.
h) Per le riunioni e gli incontri con utenti, cittadini, Clienti, Fornitori, Consulenti e Collaboratori dell'Ente è necessario utilizzare le apposite Sale dedicate e/o le piattaforme informatiche di videoconferenza identificate dall'Ente.
i) Moderare il tono della voce ogni qualvolta si trattino argomenti inerenti dati personali.
j) Chiudere a chiave tutti i cassetti (se contenenti dati personali o sensibili), gli armadi (se contenenti dai personali o sensibili) e le porte, al termine dei propri orari di servizio.
k) I dispositivi hardware e software ed in generale tutti gli strumenti di lavoro disponibili sono utilizzabili esclusivamente per le attività finalizzate al compimento degli incarichi di lavoro assegnati; altri utilizzi al di fuori di quest'ultimo sono da considerarsi esclusi.
l) I soli dispositivi informatici utilizzabili durante l'attività di lavoro sono quelli consegnati al momento dell'assunzione o al cambio/modifica della propria attività di lavoro. Perciò non è consentito l'uso, anche temporaneo, di dispositivi informatici al di fuori di quelli autorizzati.
m) É sempre vietato l'utilizzo di apparecchiature hardware e software personali, salvo esplicita autorizzazione da parte del Responsabile di riferimento.

Va ricordato che la politica generale sull'accesso ai beni ed informazioni è quella basata sul "need to know", (pertinente e non eccedente) ovvero è consentito l'accesso a quel dato, quel bene, quel documento, quel PC, etc. se e solo se è indispensabile per lo svolgimento delle attività assegnate.

Quindi se si viene in possesso di un bene e/o un'informazione non necessaria (sia da una persona interna all'Ente, sia da un soggetto esterno, come ad esempio un utente), è necessario:

- informare subito il mittente che non si è autorizzati a tenere/accedere a tale bene/informazione;
- invitare il mittente a non consegnare/inviare più quel tipo bene/informazione;
- riconsegnare/eliminare prontamente il bene/informazione.

Nota bene: L'Ente si riserva la facoltà di effettuare controlli anche saltuari, in conformità a quanto previsto dalla normativa vigente e comunque in conformità a quanto previsto dall'art. 6 del presente regolamento, per verificare che quanto indicato nel presente documento sia rispettato.

Nel caso in cui l'utente venga autorizzato, da parte dell'Amministrazione, ad operare da remoto (smart-working/telelavoro), o abbia in dotazione dispositivi mobili che possono connettersi all'infrastruttura informatica dell'Ente, l'utente dovrà:

- seguire prioritariamente le policy e le raccomandazioni dettate dall'ufficio deputato alla gestione dei sistemi informativi dell'Ente;
- in ogni caso utilizzare i sistemi operativi per i quali è garantito il supporto, effettuare costantemente gli aggiornamenti di sicurezza del sistema operativo (se tale attività non risulta esperibile da remoto dall'ufficio deputato alla gestione dei sistemi informativi dell'Ente);
- assicurarsi che i software di protezione del sistema operativo (Firewall, Antivirus, ecc) siano abilitati e costantemente aggiornati;
- assicurarsi che gli accessi al sistema operativo siano protetti da una password sicura e comunque conforme alle password policy emanate dalla dall'ente;
- non installare software proveniente da fonti/repository non ufficiali;
- bloccare l'accesso al sistema e/o configurare la modalità di blocco automatico quando ci si allontana dalla postazione di lavoro;
- non cliccare su link o allegati contenuti in email sospette;
- utilizzare l'accesso a connessioni Wi-Fi adeguatamente protette;
- collegarsi a dispositivi mobili (pen-drive, hdd-esterno, etc) solo si conosce la provenienza (nuovi, già utilizzati, forniti dall' Amministrazione);
- effettuare sempre il log-out dai servizi/portali utilizzati dopo che si ha concluso la sessione lavorativa.

2.3 Credenziali e Password

Le credenziali (nome utente e password) di primo accesso ai servizi informatici vengono assegnate dall'ufficio deputato alla gestione dei sistemi informativi, previa richiesta del Responsabile dell'ufficio/area, nell'ambito del quale verrà inserito ed andrà ad operare il nuovo utente

Successivamente alla prima autenticazione ai servizi, spetterà all'utente provvedere alla sostituzione delle credenziali assegnate, secondo le prescrizioni indicate nel presente articolo.

La richiesta di attivazione delle credenziali dovrà essere completa di generalità dell'utente ed elenco dei sistemi informativi per i quali deve essere abilitato l'accesso e, se possibile e

necessario, del periodo preciso di validità delle credenziali. Ogni successiva variazione delle abilitazioni di accesso ai sistemi informativi dovrà essere richiesta formalmente agli Amministratori di sistema dal Responsabile di riferimento.

La creazione di un nuovo utente di dominio sarà presa in considerazione per tutti i collaboratori.

Il personale dell'ufficio deputato alla gestione dei sistemi informativi provvede inoltre a rigenerare password scadute o dimenticate ed a disattivare le utenze cessate (pensionamento, dimissioni ecc.) o a sospenderle in particolari casi.

Ogni utente dovrà:

- modificare alla prima connessione la password attribuita e comunicata dall' ufficio deputato alla gestione dei sistemi informativi, e successivamente almeno ogni sei mesi (o con frequenza maggiore). Nel caso in cui l'utente svolga mansioni che, in astratto, possano comportare il trattamento di dati personali sensibili, è obbligatorio il cambio password almeno ogni tre mesi.
- deve essere composta da minimo 8 caratteri alfanumerici, preferibilmente almeno un carattere numerico, almeno uno maiuscolo, almeno uno minuscolo e almeno uno speciale; non deve contenere riferimenti agevolmente riconducibili all'incaricato e non deve essere semplice o comune. La password non deve essere costruita applicando criteri e/o logiche che possono essere utilizzate per individuare la password in vigore (es: password vecchia: Mm01pwbt - password nuova: Mm02pwbt);
- mantenere le password riservate, non divulgarle a terzi: l'utente è responsabile di abusi o incidenti di sicurezza nel caso in cui non custodisca adeguatamente le proprie credenziali. L'utente deve essere consapevole del fatto che cedere le proprie credenziali, ovvero permettere a terzi l'accesso ai servizi dell'organizzazione, significa autorizzarli a proprio nome alla gestione degli stessi, con effetti potenzialmente gravissimi (ad es. visualizzazione di informazioni riservate, alterazione o distruzione di dati, uso della propria posta elettronica etc.);
- non trascriverle su supporti facilmente accessibili a terzi (ad es. foglietti, post-it etc.). Le password non devono per nessuna ragione essere conservate per iscritto o salvate su documenti conservati all'interno della propria postazione o documentale aziendale. Qualora ci sia anche il minimo dubbio che la propria password possa essere conosciuta da altri, questa deve essere immediatamente modificata. La password va OBBLIGATORIAMENTE modificata almeno ogni SEI mesi (o con frequenza maggiore) e non può essere uguale alle ultime SEI

precedenti password. Le "domande di riserva" che aiutano a ricordare le password non devono essere mai utilizzate.

- Non permettere ad altri utenti o colleghi di operare con le proprie credenziali.
- Comunicare tempestivamente, all'ufficio deputato alla gestione dei sistemi informativi, trasferimenti e cessazioni, in modo da consentire la disabilitazione dell'accesso ai servizi non strettamente necessari. Nel caso di cessazione del rapporto di lavoro con il dipendente/collaboratore, il Responsabile dell'Ufficio/area di riferimento dovrà comunicare formalmente e preventivamente all'Amministratore di sistema la data effettiva a partire dalla quale le credenziali saranno disabilitate.
- È vietato chiedere o raccogliere in qualsiasi modo le password degli utenti a cui l'Ente eroga servizi, compresi i dipendenti stessi.
- Se è necessario accedere alle procedure di un utente che dovesse richiedere assistenza, deve essere invitato a digitare lui stesso la password, sia che l'operazione avvenga presso la sede esterna dell'utente, che presso la sede dell'Ente o in remoto. Qualora durante l'attività di lavoro si venga a conoscenza di una password dell'utente a cui l'Ente eroga servizi, questi deve essere immediatamente informato ed invitato a modificare la stessa il prima possibile.

Va ricordato che le credenziali non utilizzate da almeno SEI mesi sono disabilitate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.

Laddove tecnicamente possibile è assolutamente consigliato provvedere ad utilizzare l'autenticazione a più fattori (metodo di autenticazione sicuro che chiede agli utenti di dimostrare la loro identità fornendo due o più prove, o fattori, quando eseguono l'accesso) per accedere ai servizi informatici dell'Ente.

2.4 Uso appropriato dei privilegi di amministratore anonimi

Le utenze amministrative anonime, quali "root" di UNIX o "Administrator" di Windows, devono essere utilizzate solo per le situazioni di emergenza e le relative credenziali debbono essere gestite in modo da assicurare l'imputabilità di chi ne fa uso:

a) Per situazioni di emergenza si intendono quelle situazioni in cui le credenziali di amministrazione nominative non siano sufficienti o non reperibili

b) Le credenziali di amministrazione anonime devono essere conservate in un luogo sicuro ma facilmente accessibile sia all'Amministratore di sistema che alla Direzione generale in caso di emergenza

c) L'uso delle credenziali amministrative anonime in caso di emergenza deve essere registrato in apposito documento.

3 Utilizzo di posta elettronica, internet, notebook, tablets, smartphone, cellulari, stampanti

3.1 Smartphone, tablets e relative applicazioni mobili (APP)

I terminali di nuova generazione applicati alla telefonia mobile (smartphone e tablet) e le relative applicazioni mobili software (note comunemente con l'abbreviazione "App"), sono in costante evoluzione e consentono, con crescente facilità, di utilizzare, registrare e trasmettere dati tramite diverse tecnologie di rete.

Fermo restando l'assoluto divieto di installazione e utilizzo di applicazioni diverse da quelle autorizzate dall'Ufficio deputato alla gestione dei sistemi informativi, si fa presente che sia tali dispositivi hardware che il software in essi installato, a seconda delle proprie particolarità, potenzialmente potrebbero essere utilizzati violando, anche involontariamente, i diritti delle persone interessate alla comunicazione, come pure di terzi inconsapevoli.

3.2 Notebook, Telefoni, cellulari, stampanti, fotocopiatrici, scanner e fax

Fermo quanto indicato al precedente art. 1.3, il dipendente è consapevole che gli Strumenti di stampa, così come anche il telefono, il cellulare e i notebook dell'Ente, sono di proprietà dell'Ente stesso e sono resi disponibili all'utente per rendere la prestazione lavorativa. Pertanto, ne viene concesso l'uso esclusivamente per tale fine.

Il telefono e il cellulare dell'Ente affidato all'utente sono strumenti di lavoro. Ne viene concesso l'uso esclusivamente per lo svolgimento dell'attività lavorativa e non sono quindi consentite comunicazioni a carattere personale e/o non strettamente inerenti all'attività lavorativa stessa. La ricezione o l'effettuazione di comunicazioni a carattere personale è consentito solo nel caso di comprovata necessità ed urgenza.

Qualora venisse assegnato un cellulare dell'Ente all'utente, quest'ultimo sarà responsabile del suo utilizzo e della sua custodia.

Per quanto concerne l'utilizzo delle stampanti gli utenti sono tenuti a stampare documenti solo se strettamente necessari per lo svolgimento delle proprie funzioni operative. Laddove possibile i dispositivi di stampa dell'Ente a disposizione dei dipendenti prevedono un sistema di autenticazione mediante pin/password della stampante, al fine di evitare la visualizzazione dei contenuti del documento, da parte di soggetti non autorizzati.

Nel caso in cui si rendesse necessaria la stampa di informazioni riservate l'utente dovrà presidiare il dispositivo di stampa per evitare la possibile perdita o divulgazione di tali informazioni a persone terze non autorizzate.

Le stesse attenzioni devono essere poste per le scansioni: il file della scansione va rinominato e rimosso dalla cartella di rete condivisa. La cartella 'scansioni" non è una cartella archivio soggetta a backup, pertanto quanto in essa contenuto, in caso di cancellazione, non sarà recuperabile se non dall'originale cartaceo.

È vietato:

- l'utilizzo dei fax per fini personali, tanto per spedire quanto per ricevere documentazione, salva diversa autorizzazione da parte del Responsabile dell'unità operativa.
- l'utilizzo delle fotocopiatrici per fini personali, salvo preventiva autorizzazione da parte del Responsabile dell'unità operativa.
- l'utilizzo di scanner per fini personali, salvo preventiva autorizzazione da parte del Responsabile dell'unità operativa.
- la memorizzazione di numeri telefonici relativi alla propria attività lavorativa presso l'Ente sui cellulari personali.
- l'utilizzo dei cellulari personali durante l'orario di lavoro, anche lasciandoli in vista sulla scrivania per l'utilizzo di messaggistica di vario tipo. Restano esclusi gli utilizzi delle apparecchiature per "emergenze" personali che però non possono diventare un'abitudine. Non è considerato sicuro alternare l'uso degli strumenti personali con quelli dell'Ente, per questo è opportuno tenere gli apparecchi personali in cassetto, borsa o tasche (non sulla scrivania).

Solo in caso di necessità e urgenza, gli Utenti possono utilizzare tali beni per motivi non attinenti all'attività lavorativa e, comunque, non in modo ripetuto o per periodi di tempo prolungati. Il controllo sul corretto utilizzo degli strumenti in parola è affidato al Responsabile della unità operativa a cui detti strumenti sono stati assegnati.

3.3 Navigazione Internet e utilizzo della rete

Il PC assegnato al singolo utente ed abilitato alla navigazione in Internet costituisce uno strumento dell'organizzazione utilizzabile esclusivamente per lo svolgimento della propria attività lavorativa. È quindi proibita la navigazione in Internet per motivi diversi da quelli legati all'attività lavorativa stessa. Ciascun dipendente/collaboratore si deve attenere alle seguenti regole di utilizzo della rete Internet e dei relativi servizi.

Al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa, l'Ente adotta uno specifico sistema di blocco o filtro automatico che prevenga determinate operazioni quali

l'upload o l'accesso a determinati siti inseriti in una “black list” o in relazione ai contenuti. L'Ente si attiverà nell'individuazione di categorie di siti considerati correlati con la prestazione lavorativa.

Gli eventuali controlli, compiuti dal personale incaricato dell’ufficio deputato alla gestione dei sistemi informativi, potranno avvenire mediante un sistema di controllo dei contenuti (Web Filtering) o mediante "file di log" della navigazione svolta, nel rispetto di quanto previsto al successivo art. 6 e della normativa vigente.

Si provvede ora ad indicare le seguenti regole di comportamento per la navigazione internet:

- È ammessa solo la navigazione in siti considerati correlati con la prestazione lavorativa. L’accesso è consentito dal proxy dell’Ente con le sue policy di sicurezza debitamente implementate e aggiornate, ad es. i siti istituzionali, i siti degli Enti locali, di fornitori e partner dell’Ente.
- È vietato compiere azioni che siano potenzialmente in grado di arrecare danno all’Ente, ad esempio, il download o l’upload di file audio e/o video e di qualunque tipo di software gratuito (freeware) o shareware prelevato da siti Internet (se non espressamente autorizzato dall’ufficio deputato alla gestione dei sistemi informativi dell’Ente), nonché l’uso di servizi di rete con finalità ludiche o, comunque, estranee all’attività lavorativa.
- L’Ente si riserva di bloccare l’accesso a siti “a rischio” attraverso l’utilizzo di blacklist pubbliche in continuo aggiornamento e di predisporre filtri, basati su sistemi euristici di valutazione del livello di sicurezza dei siti web remoti, tali da prevenire operazioni potenzialmente pericolose o comportamenti impropri. In caso di blocco accidentale di siti di interesse dell’Ente, contattare l’Ufficio Sistemi Informativi per uno sblocco selettivo.
- È vietata l’effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, salvo i casi direttamente autorizzati dalla Direzione Generale e dall’Ufficio Sistemi Informativi, con il rispetto delle normali procedure di acquisto.
- È vietato l’utilizzo di abbonamenti privati per effettuare la connessione a Internet tranne in casi del tutto eccezionali e previa autorizzazione degli Amministratori di Sistema e dei responsabili di riferimento previo parere tecnico dello stesso Amministratore di sistema.
- La rete “Wi-Fi”, se presente all’interno dell’Ente, consente l’accesso alle risorse e ad internet per i dispositivi non connessi alla rete LAN mediante cavo. L’accesso mediante rete Wi-Fi viene concesso a consulenti, professionisti, tecnici e fornitori che nell’ambito di un rapporto contrattuale con l’Ente per permettergli di accedere a determinate risorse informatiche. A tali figure devono essere fornite chiare istruzioni sulle modalità di utilizzo della rete. Viene concesso, altresì, a dipendenti e funzionari dell’Ente che necessitino di svolgere compiti

specifici che non possono essere svolti dalle postazioni fisse. L'impostazione della connessione Wi-Fi sarà effettuata dall'Amministratore di sistema.

L'ufficio deputato alla gestione dei sistemi informativi dell'Ente si riserva la facoltà di negare o interrompere l'accesso alla rete a dispositivi non adeguatamente protetti e/o aggiornati, che possano costituire una concreta minaccia per la sicurezza informatica dell'Ente.

Si informa che l'Ente, attraverso l'Amministratore di Sistema, non effettua la memorizzazione sistematica delle pagine web visualizzate dal singolo Utente, né controlla con sistemi automatici i dati di navigazione dello stesso.

Si avvisa che possono essere effettuati controlli secondo le modalità indicate al successivo art. 6.

In caso di necessità e urgenza gli Utenti possono navigare in Internet per motivi non attinenti all'attività lavorativa e, comunque, non in modo ripetuto o per periodi di tempo prolungati, previa autorizzazione del Dirigente responsabile della struttura, compatibilmente con le misure di sicurezza implementate a protezione del sistema informatico. Tale modalità non deve in ogni caso avvenire in misura eccedente e pregiudizievole rispetto agli obblighi di servizio che il dipendente ha nei confronti dell'Ente.

L'utente utilizzatore del personal computer verifica periodicamente lo stato di aggiornamento dell'antivirus dell'Organizzazione installato. A fronte di eventuali anomalie contatta l'Ufficio deputato alla gestione dei sistemi informativi.

L'Ente mette a disposizione dei propri utenti la possibilità di accedere alle proprie risorse informatiche anche dall'esterno dei confini dell'Organizzazione stessa, mediante per esempio rete VPN (Virtual Private Network), un canale privato e criptato verso la rete interna. L'accesso mediante VPN/RDP (Remote Desktop Protocol) viene concesso a consulenti, professionisti, tecnici e fornitori che nell'ambito di un rapporto contrattuale con l'Ente necessitino di accedere a determinate risorse informatiche. Viene concesso, altresì, a dipendenti e funzionari dell'Ente che necessitino di svolgere compiti specifici o siano in modalità di lavoro subordinato o *smart working*, pur non essendo presenti in sede.

Le richieste di abilitazione all'accesso mediante tali canali di comunicazione dovranno essere autorizzate dall'ufficio deputato alla gestione dei sistemi informativi dell'Ente. Qualora sia necessario l'accesso alla rete dell'Ente attraverso i suddetti strumenti e tecniche di collegamento è necessario prestare la massima attenzione nelle fasi di accesso, proteggendo da occhi o da telecamere presenti la fase di digitazione dell'utente e della password. Una volta aperta la connessione, questa deve rimanere attiva lo stretto necessario all'espletamento delle attività

richieste, quindi chiusa. In ogni caso, prima di abbandonare la postazione dalla quale è stata aperta la connessione è bene accertarsi dell'avvenuta chiusura della stessa, eliminando cronologia e file temporanei (ove possibile) ed eventuali altri dati di connessione che l'amministratore di rete potrà indicare all'utente in fase di consegna delle credenziali di accesso.

Le credenziali di accesso alle VPN non vanno salvate nel software di collegamento, nè tantomeno nel dispositivo utilizzato per il collegamento stesso.

L'Ente si riserva la facoltà di effettuare controlli anche saltuari, in conformità a quanto previsto dalla normativa vigente e comunque in conformità a quanto previsto dall'art. 6 del presente regolamento, per verificare che quanto indicato nel presente articolo sia rispettato.

3.4 Partecipazione ai social media

L'utilizzo a fini promozionali di Facebook, Twitter, Linkedin, etc… dei blog e dei forum, chat line, anche professionali (ed altri siti o social media), bacheche elettroniche etc… è gestito ed organizzato esclusivamente dal Titolare del trattamento, in persona del legale rappresentante pro-tempore, attraverso **specifiche direttive ed istruzioni operative (social policy) fornite al personale, a cui integralmente si rimanda, rimanendo escluse iniziative individuali da parte dei singoli dipendenti/collaboratori.**

Fermo restando il diritto della persona alla libertà di espressione, e richiamando interamente quanto indicato nelle istruzioni conferite dal titolare al personale preposto alla gestione dei canali social, l'Ente ritiene comunque opportuno indicare ai dipendenti/collaboratori, nel presente documento, alcune regole comportamentali, al fine di tutelare tanto la propria immagine ed il patrimonio, anche immateriale, quanto i propri collaboratori, i propri clienti e fornitori, gli altri partners, oltre che gli stessi dipendenti/collaboratori utilizzatori dei social media, fermo restando che è vietata la partecipazione agli stessi social media durante l'orario di lavoro.

Il presente articolo deve essere osservato dai dipendenti/collaboratori sia che utilizzino dispositivi messi a disposizione dall'Ente, sia che utilizzino propri dispositivi, sia che partecipino ai social media a titolo personale, sia che lo facciano per finalità professionali, come dipendenti/collaboratori dell'organizzazione.

La condivisione dei contenuti nei social media deve sempre rispettare e garantire la segretezza sulle informazioni istituzionali considerate dal Titolare riservate ed in genere, a titolo esemplificativo e non esaustivo, sulle informazioni inerenti attività, dati contabili, finanziari, progetti, procedimenti svolti o in svolgimento presso gli uffici. Inoltre, ogni comunicazione e divulgazione di contenuti dovrà essere effettuata nel pieno rispetto dei diritti di proprietà industriale e dei diritti d'autore, sia di terzi che dell'Ente. Il dipendente/collaboratore, nelle

proprie comunicazioni, non potrà quindi inserire il nominativo e il logo dell'Ente, né potrà pubblicare disegni, modelli od altro connesso ai citati diritti. Ogni deroga a quanto sopra disposto potrà peraltro avvenire solo previa specifica autorizzazione del Titolare.

3.5 Posta elettronica

La casella di posta elettronica assegnata all'utente è uno strumento di lavoro. Gli Utenti assegnatari delle caselle di Posta Elettronica sono responsabili del corretto utilizzo delle stesse e sono tenuti, in un'ottica di correttezza ed uso responsabile degli strumenti, a contribuire alla riduzione del fenomeno dello "spam" (*trasmissione su larga scala e in grandi volumi di e-mail non sollecitati*). La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti per evitare che raggiunga dimensioni eccessive.

È fatto divieto:

- utilizzare la casella di posta elettronica per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mailing-list salvo diversa ed esplicita autorizzazione. È buona norma evitare messaggi completamente estranei al rapporto di lavoro od alle relazioni tra colleghi.
- inviare/partecipare a catene telematiche via *e-mail*. In caso di ricezione di *e-mail* non attinenti alle attività di lavoro (spam), queste vanno immediatamente eliminate; non si deve in alcun modo attivare gli allegati di tali messaggi.
- trasmettere a chiunque a mezzo Posta Elettronica materiale pornografico/pedopornografico, materiale fraudolento/illegale, gioco d'azzardo, materiale blasfemo o molesto/osceno. Il predetto divieto riguarda tanto il contenuto quanto gli allegati dei messaggi di Posta.

Se l'*e-mail* ricevuta è destinata ad altre persone è necessario limitare il più possibile la lettura del documento, ovvero facendolo con il solo obiettivo di comprendere che non si tratta di documentazione propria (quindi senza né leggere il contenuto, né cercare di capire a chi appartiene), ma inviare un messaggio al mittente spiegando l'errore. L'*e-mail* ricevuta va immediatamente eliminata, anche dal cestino.

Per quanto riguarda la posta di interesse dell'Ente che erroneamente è pervenuta all'indirizzo individuale, i destinatari devono inoltrare lo stesso giorno tale corrispondenza all'indirizzo del protocollo, in modo da consentire all'incaricato di distribuire il documento a tutti i soggetti interessati. Inoltre, va comunicato al mittente che ha spedito la posta di interesse dell'Ente all'indirizzo personale, che il recapito corretto è quello istituzionale dell'ente.

È consigliato che ogni *e-mail* inviata contenga un debito disclaimer in riferimento alla protezione delle informazioni.

Si ricorda che la posta personale non è sottoposta a backup. Sul server di posta viene mantenuta traccia delle *mail* inviate su files di log. Periodici controlli di detti log vengono effettuati allo scopo di verificare la sicurezza e il corretto uso delle *e-mail*. Altri controlli possono essere effettuati, su richiesta, dall'autorità giudiziaria. **Si ricorda che la casella mail non è adibita come strumento per salvare propri file.**

L'Ente fornisce, altresì, delle caselle di posta elettronica associate a ciascuna unità organizzativa, ufficio o gruppo di lavoro il cui utilizzo è da preferire rispetto alle *e-mail* nominative qualora le comunicazioni siano di interesse collettivo: questo per evitare che degli utenti singoli mantengano l'esclusività su dati dell'Ente.
L'iscrizione a mailing-list o newsletter esterne, con il proprio indirizzo personale dell'Ente, è concessa esclusivamente per motivi professionali. Prima di iscriversi occorre verificare anticipatamente l'affidabilità del sito che offre il servizio.

È obbligatorio porre la massima attenzione nell'aprire i file attachments (allegati) di posta elettronica prima del loro utilizzo (non scaricare file eseguibili o documenti di ogni genere da siti Web o FTP non conosciuti). **Porre la massima attenzione laddove i file allegati presentino una delle seguenti estensioni ".exe, *.com, *.vbs, *.htm, *html, *.scr, *.bat, *.js e *.pif , *.zip criptati, *.docx, *.xlsx, *.pptx "**- Si tratta di estensioni di file che potrebbero mandare in esecuzione file eseguibili che, a loro volta, possono infettare il computer con un virus.

Si invita a prestare la massima attenzione anche qualora le mail contenenti le suddette tipologie di allegati, provenissero da mittenti conosciuti, specie se il destinatario non sta attendendo della specifica documentazione dal mittente.

Nel caso vi fosse incertezza in ordine alla credibilità del messaggio e/o alla sua provenienza il dipendente dovrà contattare immediatamente l'ufficio deputato alla gestione dei sistemi informativi dell'Ente o il personale preposto per una valutazione del singolo caso.

Nel caso in cui fosse necessario inviare a destinatari esterni messaggi contenenti allegati con dati personali o dati personali sensibili, è obbligatorio che questi allegati vengano preventivamente resi inintelligibili attraverso crittazione con apposito software (archiviazione e compressione con password). La password di crittazione deve essere comunicata al destinatario attraverso un canale diverso dalla *e-mail* (ad esempio per lettera o per telefono) e mai assieme ai

dati criptati. Tutte le informazioni dell'Ente, i dati personali e/o sensibili di competenza dell'Ente possono essere inviati soltanto a destinatari - persone o Enti – qualificati e competenti.

Al fine di garantire la funzionalità del servizio di posta elettronica dell'Ente e di ridurre al minimo l'accesso ai dati, nel rispetto del principio di necessità e di proporzionalità, il sistema, in caso di assenze programmate (ad es. per ferie o attività di lavoro fuori sede dell'assegnatario della casella) invierà automaticamente messaggi di risposta contenenti le "coordinate" di posta elettronica di un altro soggetto o altre utili modalità di contatto della struttura / servizio. In tal caso, la funzionalità deve essere attivata dall'utente.

In caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, qualora non fosse possibile attivare la funzione autoreply o l'inoltro automatico su altre caselle dell'Ente e si debba conoscere il contenuto dei messaggi di posta elettronica, il titolare della casella di posta ha la facoltà di delegare un altro dipendente (fiduciario) per verificare il contenuto di messaggi e per inoltrare al titolare del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. Sarà compito del Dirigente responsabile assicurarsi che sia redatto un verbale attestante quanto avvenuto e che sia informato il lavoratore interessato alla prima occasione utile;

<u>Si informa:</u>

- che le comunicazioni anche elettroniche ed i documenti elettronici allegati possono avere rilevanza procedimentale e pertanto devono essere conservate per la durata prevista dalla normativa vigente.
- che l'Ente, per il tramite dell'ufficio deputato alla gestione dei sistemi informativi dell'Ente, non controlla sistematicamente il flusso di comunicazioni *e-mail* né è dotato di sistemi per la lettura o analisi sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio *e-mail*.
- che nel caso di cessazione dell'attività lavorativa dell'utente della casella di posta elettronica, sia nel caso di indirizzo nominale che di funzione (ad es. presidente, sindaco, segretario…), dev'essere bloccato l'accesso dal giorno successivo/settimana e il contenuto dev'essere cancellato entro un congruo termine dando previamente la possibilità di recuperare le informazioni strettamente personali. Tempi maggiori di conservazione possono essere autorizzati dal Segretario/Direttore generale per motivi di necessità opportunamente giustificati.

  Contestualmente, devono essere implementati sistemi automatici volti ad informare i terzi e a fornire indirizzi alternativi, oltre ad una policy informativa di avviso della scadenza a tempo

della casella per l'utilizzatore.
Nel caso invece di caselle e-mail condivise per servizio/ufficio e non riconducibili ad un unico soggetto (ad es. segreteria, anagrafe, info…) non è prevista la chiusura e la cancellazione della casella e dei dati in essa contenuti.

4 Manutenzione, modifiche, furto o smarrimento delle risorse ICT

Il sistema operativo ed il software di base del proprio PC è preimpostato, ed è definito dall'Ente stesso. Non è consentita l'installazione di nessun altro software oltre a quello definito, è vietata la modifica dei parametri di configurazione dei dispositivi assegnati. Eventuali modifiche alla configurazione possono essere apportate solo a seguito di autorizzazione del responsabile d'area/servizio dell'utente che ne fa richiesta e comunque a seguito di verifica tecnica effettuata dall'ufficio deputato alla gestione dei sistemi informativi dell'Ente, sulle implicazioni di sicurezza che la modifica comporta.

Non è permesso intervenire sul dispositivo togliendo o sostituendo componenti hardware o aggiungendo alla rete locale qualsiasi dispositivo ICT (PC esterni, router, switch…) che possa inficiare il corretto funzionamento degli apparati.

In caso di malfunzionamenti deve essere immediatamente avvertito il personale preposto, ogni eventuale modifica deve essere concordata e autorizzata da parte dell'Amministratore di Sistema.

In caso di smarrimento o furto di dispositivi informatici, oltre a sporgere regolare denuncia all'autorità competente, si dovrà informare tempestivamente l'ufficio deputato alla gestione dei sistemi informativi comunicando quali dati erano contenuti all'interno.

5 Protezione Antivirus

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

Nel caso il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente sospendere ogni elaborazione in corso, senza spegnere il computer, scollegarlo dalla rete informatica, nonché segnalare prontamente all'ufficio deputato alla gestione dei sistemi informativi dell'Ente.

Ogni dispositivo di provenienza esterna all'Ente dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato codice malevolo, dovrà essere prontamente consegnato al personale preposto.

6 Controlli

Fermo da parte dell'Ente il rispetto di quanto previsto dall'art. 4 Legge 300/1970 (Statuto dei lavoratori), poiché in caso di violazioni contrattuali e giuridiche, sia l'Ente, sia il singolo lavoratore sono potenzialmente perseguibili con sanzioni, anche di natura penale, l'Ente verificherà, nei limiti consentiti dalle norme di legge e contrattuali, il rispetto delle regole e l'integrità del proprio sistema informatico.

I controlli devono essere effettuati nel rispetto del presente Regolamento e dei seguenti principi:

- 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.
- Trasparenza: l'adozione del presente Regolamento ha l'obiettivo di informare gli utenti sui diritti ed i doveri di entrambe le parti.
- Pertinenza e non eccedenza: ovvero evitando un'interferenza ingiustificata sui diritti e sulle libertà fondamentali dei lavoratori, così come la possibilità di controlli prolungati, costanti o indiscriminati.

L'uso degli Strumenti Informatici dell'Ente può lasciare traccia delle informazioni sul relativo uso, come analiticamente spiegato nei punti precedenti del presente Regolamento. Tali informazioni, che possono contenere dati personali dell'Utente, possono essere oggetto di controlli da parte dell'Ente , per il tramite dell'ufficio deputato alla gestione dei sistemi informativi dell'Ente, volti a garantire esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio dell'Ente, nonché per la sicurezza e la salvaguardia del sistema informatico, per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento – sostituzione - implementazione di programmi, manutenzione hardware, etc.). Gli interventi di controllo possono permettere all'Ente di avere indirettamente cognizione dell'attività svolta con gli strumenti.

6.1 Modalità operative su Controlli per la tutela del patrimonio dell'Ente, nonché per la sicurezza e la salvaguardia del sistema informatico. Controlli per ulteriori motivi tecnici e/o manutentivi.

Qualora per le finalità qui sopra descritte risulti necessario l'accesso agli Strumenti e alle risorse informatiche e relative informazioni descritte ai punti del presente Regolamento, il Titolare del trattamento dei dati personali per il tramite dell'Amministratore di Sistema, si atterrà al processo descritto qui di seguito (se e in quanto compatibile con lo Strumento oggetto di controllo).

1. Avviso generico a tutti i dipendenti della presenza di comportamenti anomali che possono mettere a rischio la sicurezza del sistema informativo e richiamo all'esigenza di attenersi al rispetto del presente Regolamento.
2. Se il comportamento anomalo persiste, l'Ente potrà accedere alle informazioni necessarie con possibilità di rilevare files trattati, siti web visitati, software installati, documenti scaricati, statistiche sull'uso di risorse ecc. nel corso dell'attività lavorativa. Tale attività potrà essere effettuata in forma anonima ovvero tramite controllo del numero IP dell'Utente e con l'identificazione del soggetto che non si attiene alle istruzioni impartite.
3. Qualora il rischio di compromissione del sistema informatico dell'Ente sia imminente e grave a tal punto da non permettere l'attesa dei tempi necessari per i passaggi procedimentali descritti ai punti 1 e 2, il Titolare del Trattamento, unitamente all'amministratore di sistema, può intervenire senza indugio sullo strumento da cui proviene la potenziale minaccia.

6.2 Controlli per esigenze produttive e di organizzazione

Qualora risulti necessario l'accesso alle risorse informatiche (ivi comprese quelle disciplinate al precedente art. 3) e alle relative informazioni, il Titolare del trattamento dei dati personali, per il tramite dell'Amministratore di Sistema, si atterrà alla procedura descritta qui di seguito (se e in quanto compatibile con lo Strumento oggetto di controllo).

1. Redazione di un atto da parte del Direttore e/o Capo Area che comprovi le necessità produttive e di organizzazione che richiedano l'accesso allo Strumento.
2. Incarico all'Amministratore di sistema di accedere alla risorsa con credenziali di Amministratore ovvero tramite l'azzeramento e la contestuale creazione di nuove credenziali di autenticazione dell'Utente interessato, con avviso che al primo accesso alla risorsa, lo stesso dovrà inserire nuove credenziali.
3. Redazione di un verbale che riassuma i passaggi precedenti.
4. In ogni caso l'accesso ai documenti presenti nella risorsa è limitato a quanto strettamente indispensabile alle finalità produttive e di organizzazione del lavoro.

Dell'attività sopra descritta viene redatto verbale, sottoscritto dal Titolare del Trattamento e dall'Amministratore di Sistema che ha svolto l'attività.

Qualora indirettamente si riscontrino file o informazioni anche personali, esse potranno essere altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, considerato che il presente Regolamento costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli.

Al fine delle verifiche di cui al presente regolamento, si informa che l'Ente, per il tramite degli Amministratori di Sistema, non effettua la memorizzazione sistematica delle pagine web visualizzate dal singolo Utente, né controlla con sistemi automatici i dati di navigazione dello stesso o la casella email ad esso assegnata.

Si informa tuttavia che al fine di garantire il servizio Internet e la sicurezza dei sistemi informativi, nonché per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio, il Titolare, per il tramite del Responsabile esterno all'uopo incaricato, può conservare i dati di navigazione (file di log riferiti al traffico web) con modalità inizialmente volte a precludere l'immediata e diretta identificazione di Utenti, mediante opportune aggregazioni. La conservazione non può essere superiore a trenta.

Solo in casi eccezionali e di comprovata urgenza rispetto alle finalità sopra descritte, il Titolare può trattare i dati di navigazione riferendoli specificatamente ad un singolo nome utente.

Le informazioni così raccolte sono altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, compresa la verifica del rispetto del presente Regolamento.

7 Conservazione

I dati personali relativi agli accessi ad Internet ed al traffico telematico ai log di sistema, la cui conservazione non sia necessaria, saranno periodicamente cancellati in modo automatico mediante procedure tecniche adottate dall'ufficio deputato alla gestione dei sistemi Informativi, che provvederà a configurare i sistemi in modo che ciò avvenga, nel rispetto anche di quanto indicato dal Garante per la Protezione dei dati personali con provvedimento del *"13 ottobre 2008* ***-Rifiuti di apparecchiature elettriche ed elettroniche (Raee) e misure di sicurezza dei dati personali".***

L'eventuale prolungamento dei tempi di conservazione va valutato come eccezionale e può aver luogo solo in relazione ad esigenze tecniche o di sicurezza del tutto particolari; all'indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;

all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria.

In questi casi, il trattamento dei dati personali deve essere limitato alle sole informazioni indispensabili per perseguire finalità specifiche, comprovate e limitate al tempo necessario - e predeterminato - a raggiungerla.

L'Ente si impegna ad assumere le misure di sicurezza nel trattamento e nella conservazione di tale tipologia di dati alla luce di quanto stabilito dal Legislatore.

In riferimento agli articoli 5 e 6 del Reg. UE n. 2016/679 e in applicazione ai principi di diritto di accesso, legittimità, proporzionalità, sicurezza ed accuratezza e conservazione dei dati, le informazioni relative all'accesso ad Internet e dal traffico telematico (log di sistema e del server proxy), la cui conservazione non sia necessaria), verranno cancellati nel rispetto dei termini previsti dalle normative vigenti.

In casi eccezionali – ad esempio: per esigenze tecniche o di sicurezza; o per l'indispensabilità dei dati rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria o, infine, all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria – è consentito il prolungamento dei tempi di conservazione limitatamente al soddisfacimento delle esigenze sopra esplicitate.

Il Titolare si impegna ad assumere le misure di sicurezza nel trattamento e nella conservazione di tale tipologia di dati alla luce di quanto stabilito dal Legislatore.

8 Violazioni

Qualora si ravvisassero violazioni di una o più delle prescrizioni definite nel presente regolamento, possono essere avviate procedure per l'attribuzione di sanzioni in ogni sede ritenuta competente.