



UNIONE DEI COMUNI "ELIMO ERICINI"

Cod. Fisc. Part. IVA 93045120818

Buseto Palizzolo – Custonaci – Erice - Paceco - San Vito Lo Capo – Valderice

**DISCIPLINARE INTERNO PER L'UTILIZZO DELLA RETE
INFORMATICA, DEI DISPOSITIVI E DEI SERVIZI
INFORMATICI**

2019

Approvato con deliberazione della Giunta dell'Unione n. 8 del 27 marzo 2019

SOMMARIO

1. Premessa	3
2. Campo di applicazione	4
3. Riferimenti normativi	5
4. Tutela del dipendente	6
5. Riservatezza delle informazioni	6
6. Utilizzo del personal computer	7
7. Hardware e Software	9
8. Computer portatili, tablet e smartphone	10
9. Stampanti, Fotocopiatori, Scanner, Fax e Telefoni	10
10. Credenziali di accesso	11
11. Utilizzo della rete e accessi da remoto	12
12. Credenziali di accesso ai programmi gestionali	13
13. Supporti rimovibili	14
14. Posta elettronica	14
15. Navigazione internet	16
16. Protezione da virus	17
17. Salvataggio dati	18
18. Tele-assistenza	18
19. Monitoraggio	19
20. Controlli	19
21. Conservazione dei dati	21
22. Social Media	21
23. Sanzioni	22
24. Aggiornamento e revisione	22

1. Premessa

Il presente disciplinare intende fornire al personale ai dipendenti e collaboratori, denominati anche utenti o persone autorizzate al trattamento dei dati personali, dell'Unione dei Comuni Elimo Ericini le indicazioni per una corretta e adeguata gestione delle informazioni personali, in particolare attraverso l'uso di sistemi, applicazioni e strumenti informatici dell'Ente. Si specifica che tutti gli strumenti con relativi software e applicativi (di seguito più semplicemente "Strumenti"), sono messi a disposizione dall'Unione dei Comuni Elimo Ericini per rendere la prestazione lavorativa. Gli Strumenti, nonché le relative reti informatiche dell'Ente a cui è possibile accedere tramite gli stessi, rappresentano il domicilio informatico dell'Unione dei Comuni Elimo Ericini. 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 finalità istituzionali, per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio dell'Ente. Per tutela del patrimonio dell'Ente si intende altresì la sicurezza informatica e la tutela del sistema informatico dell'Ente. Tali informazioni sono altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, considerato che il presente disciplinare costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli, sempre nel rispetto di quanto disposto dal Regolamento Europeo n. 2016/679 sulla protezione dei dati personali. Viene, infine, precisato che non sono installati o configurati sui sistemi informatici in uso agli utenti apparati hardware o strumenti software aventi come scopo il controllo a distanza dell'attività dei lavoratori, nel rispetto della disciplina lavoristica ex L. 300/70 e D.lgs 151/2015 (Jobs Act).

L'utilizzo delle risorse informatiche e telematiche deve sempre ispirarsi, in applicazione di quanto disposto dagli artt. 2104 e 2105 c.c., al **principio della diligenza, fedeltà e correttezza, comportamenti che normalmente si adottano nell'ambito dei rapporti di lavoro**, adottando, quindi, tutte le cautele e le precauzioni necessarie per evitare le possibili conseguenze dannose alle quali un utilizzo non avveduto di tali strumenti può produrre, anche in considerazione della difficoltà di tracciare una netta linea di confine tra l'attività lavorativa e la sfera personale e la vita privata del lavoratore e di terzi che interagiscono con quest'ultimo. In tale contesto, l'Autorità Garante per la protezione dei dati personali ha emanato la deliberazione n. 13 del 1° marzo 2007 "Lavoro: Le linee guida del Garante per posta elettronica e internet" con la quale ha inteso **prescrivere ai datori di lavoro alcune misure per conformare alle disposizioni vigenti il trattamento di dati personali effettuato** per verificare il corretto utilizzo, nello svolgimento del rapporto di lavoro, della posta elettronica e della rete internet. La progressiva diffusione delle nuove tecnologie informatiche, le maggiori possibilità di interconnessione tra computer e l'aumento di informazioni trattate con strumenti elettronici aumentano infatti i rischi legati alla sicurezza e all'integrità delle informazioni oltre alle conseguenti responsabilità previste dalla normativa vigente in materia.

L'Unione dei Comuni Elimo Ericini con il presente atto adotta un Disciplinare interno diretto ad evitare che comportamenti inconsapevoli possano innescare problemi alla gestione della Rete informatica e/o minacce alla sicurezza nel trattamento dei dati personali di qualsivoglia tipo (personale, sensibile e giudiziario) e per richiamare le indicazioni e le misure

necessarie ed opportune per il corretto utilizzo, nel rapporto di lavoro, dei personal computer (fissi e portatili), dei dispositivi elettronici in genere, della posta elettronica e di internet, **definendone le modalità di utilizzo nell'ambito dell'attività lavorativa.**

Le prescrizioni di seguito previste si aggiungono ed integrano le specifiche istruzioni già fornite a tutti i dipendenti dell'Unione dei Comuni Elimo Ericini, in attuazione del Codice Privacy e del Regolamento Generale sulla protezione dei dati personali (Regolamento UE 2016/679).

L'Unione dei Comuni Elimo Ericini (D'ORA IN AVANTI ANCHE "ENTE") deve provvedere a garantire un servizio continuativo, nel suo stesso interesse, ed assicurare la riservatezza delle informazioni e dei dati, in maniera tale da evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla sicurezza nel trattamento dei dati o diminuire l'efficienza delle risorse informatiche. L'Ente riconosce il valore fondamentale dell'utilizzo di strumenti di comunicazione sia nella comunicazione interna che con l'utenza esterna, anche al fine di ridurre i tempi di risposta e di migliorare pertanto l'efficienza del proprio operato istituzionale.

2. Campo di applicazione

Il presente Disciplinare **si applica a tutto il personale, ai dipendenti, senza distinzione di ruolo o livello, nonché a tutti i collaboratori dell'Unione dei Comuni Elimo Ericini** a prescindere dal rapporto contrattuale con lo stesso intrattenuto (consulenti, tirocinanti, borsisti, volontari, ditte esterne autorizzate, ecc.). Inoltre, il presente Disciplinare regola l'utilizzo di tutti i dispositivi collegati alla rete informatica e quindi direttamente gestibili e controllabili a norma di legge, attraverso gli opportuni strumenti, dal personale autorizzato.

Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche e telematiche, per "utente" deve intendersi ogni soggetto, in possesso di specifiche credenziali di autenticazione, operante su computer in rete informatica. Tale figura si configura quale "persona autorizzata" ai sensi del Regolamento Generale sulla protezione dei dati personali.

Il presente Disciplinare contiene le disposizioni relative alle corrette modalità di utilizzo della rete informatica e di tutte le risorse, in conformità e nel rispetto di quanto previsto dalla specifica normativa di settore e dalle ulteriori disposizioni emanate dall'Ente.

Gli strumenti informatici oggetto del presente Disciplinare sono di proprietà dell'Ente e sono messi a disposizione degli Utenti al fine di permettere il quotidiano svolgimento delle proprie prestazioni lavorative. Essi sono essenzialmente individuabili nei computer, negli apparati removibili, nei sistemi di identificazione e di autenticazione informatica, Internet e negli strumenti di scambio di comunicazioni e file, nella posta elettronica e in qualsiasi altro programma e apparecchiatura informatica destinata a memorizzare o a trasmettere dati e informazioni.

E' responsabilità di tutti i soggetti che utilizzano gli strumenti informatici messi a disposizione, di applicare e rispettare puntualmente le disposizioni del presente Disciplinare.

Sono esentati dall'applicazione del presente Disciplinare, e limitatamente a quanto necessario per il corretto svolgimento delle proprie funzioni, gli Amministratori di Sistema formalmente nominati.

Per qualsiasi dubbio relativo all'applicazione pratica ed all'interpretazione autentica delle disposizioni contenute nel presente Disciplinare, è possibile rivolgersi al Segretario Generale dell'Unione dei Comuni Elimo Ericini.

Per Amministratore di Sistema si intende il soggetto cui è conferito il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di base dati e di consentirne l'utilizzazione.

Devono essere nominati Amministratori di Sistema tutti coloro che, nell'espletamento delle loro consuete attività tecniche, sono "responsabili" di fasi lavorative che possono comportare elevate criticità rispetto alla protezione dei dati, quali:

- gestione dei sistemi di autenticazione e di autorizzazione;
- custodia delle credenziali di autenticazione e di autorizzazione;
- salvataggio dei dati (backup/recovery);
- organizzazione dei flussi di rete;
- gestione dei supporti di memorizzazione;
- manutenzione hardware.

Possono dunque qualificarsi quale Amministratori di sistema i seguenti soggetti:

- amministratori di sistemi di autenticazione e di autorizzazione;
- amministratori di server e pc;
- amministratori di apparati rete;
- amministratori di base di dati;
- amministratori di apparati di sicurezza;
- amministratori di applicazioni.

Nel caso di servizi di amministrazione di sistemi affidati in outsourcing, ove il fornitore si configura quale Responsabile esterno del trattamento ai sensi dell'art. 28 del Regolamento UE 2016/679, l'Ente si impegna a conservare direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema. Qualora l'attività degli amministratori di sistema riguardi servizi o sistemi che trattano informazioni di carattere personale di dipendenti, l'Ente è tenuto a rendere nota o conoscibile l'identità degli amministratori di sistema nell'ambito della propria organizzazione.

3. Riferimenti normativi

Il presente disciplinare è redatto:

- alla luce della Legge 20.5.1970, n. 300, recante "Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro e norme sul collocamento";

- in attuazione del Regolamento Europeo n. 2016/679 sulla protezione dei dati personali (d'ora in avanti Regolamento 2016/679 o RGPD);
- ai sensi delle "Linee guida del Garante per posta elettronica e internet" in Gazzetta Ufficiale n. 58 del 10 marzo 2007;
- alla luce dell'articolo 23 del D.Lgs. n. 151/2015 (c.d. Jobs Act) che modifica e rimodula la fattispecie integrante il divieto dei controlli a distanza, nella consapevolezza di dover tener conto, nell'attuale contesto produttivo, oltre agli impianti audiovisivi, anche degli altri strumenti «dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori» e di quelli «utilizzati dal lavoratore per rendere la prestazione lavorativa».

La finalità è quella di promuovere in tutto il personale dell'Ente una corretta "cultura informatica" affinché l'utilizzo degli Strumenti informatici e telematici forniti dall'Ente, quali la posta elettronica, internet e i personal computer con i relativi software, sia conforme alle finalità dell'Ente e nel pieno rispetto della legge. Si vuole fornire a tutto il personale le indicazioni necessarie con l'obiettivo principale 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.

4. Tutela del dipendente

Alla luce dell'art. 4, comma 1, L. n. 300/1970 e s.m.i., la regolamentazione della materia indicata nel presente Disciplinare non è finalizzata all'esercizio di un controllo a distanza dei lavoratori da parte del datore di lavoro ma solo a permettere a quest'ultimo di utilizzare i servizi informatici per fare fronte ad esigenze produttive od organizzative e di sicurezza nel trattamento dei dati personali.

È sempre garantito al singolo lavoratore il controllo sui propri dati personali secondo quanto previsto dagli articoli 15-16-17-18-20-21-78 del Regolamento UE 2016/679.

5. Riservatezza delle informazioni

I principi che sono a fondamento del presente disciplinare sono gli stessi espressi nel Regolamento UE 2016/679 e, precisamente:

- a. il principio di necessità, secondo cui i sistemi informatici e 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 del Reg. 679/16);
- b. il principio di correttezza, secondo cui le caratteristiche essenziali dei trattamenti devono essere rese note ai lavoratori. Le tecnologie dell'informazione permettono di svolgere trattamenti ulteriori rispetto a quelli connessi ordinariamente all'attività lavorativa. Ciò, all'insaputa o senza la piena consapevolezza dei lavoratori, considerate anche le potenziali applicazioni di regola non adeguatamente conosciute dagli interessati;
- c. i trattamenti devono essere effettuati per finalità determinate, esplicite e legittime (art.5 commi 1 e 2), 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".

Il dipendente si attiene alle seguenti regole di trattamento:

- È vietato comunicare a soggetti non specificatamente autorizzati i dati personali comuni, sensibili, giudiziari, sanitari o altri dati, 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 di Settore;
- È vietata l'estrazione di originali e/o copie cartacee ed informatiche per uso personale di documenti, manuali, fascicoli, lettere, data base e quant'altro;
- 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, per più di 15 minuti. È vietato lasciare sulla postazione di lavoro (scrivania, bancone ecc.) materiali che non siano inerenti la pratica che si sta trattando in quel momento. Ciò vale soprattutto nel caso di lavoratori con mansioni di front office.
- Per le riunioni e gli incontri con Utenti, Cittadini, Clienti, Fornitori, Consulenti e Collaboratori dell'Ente è necessario utilizzare le apposite Sale dedicate o uffici dell'Ente.

6. Utilizzo del personal computer

Il personal computer affidato all'Utente è uno strumento di lavoro. Ogni utilizzo non inerente all'attività lavorativa è vietato perché può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. Il Pc deve essere custodito con cura evitando ogni possibile forma di danneggiamento.

Il personal computer dato in affidamento all'Utente permette l'accesso alla rete informatica solo attraverso specifiche credenziali di accesso ed autenticazione.

L'Ente rende noto che il personale incaricato in qualità di Amministratore di Sistema, è autorizzato a compiere interventi nel sistema informatico, diretti a garantire la sicurezza e la salvaguardia del sistema stesso, nonché per ulteriori motivi tecnici e/o manutentivi. Detti interventi potranno anche comportare l'accesso in qualunque momento, ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica, nonché alla verifica sui siti internet acceduti dagli utenti abilitati. La stessa facoltà, sempre ai fini della sicurezza del sistema e per garantire la normale operatività dell'Ente, si applica anche in caso di assenza prolungata od impedimento del dipendente.

Il personale autorizzato ha la facoltà di collegarsi, previa autorizzazione dell'Utente, e visualizzare in remoto il desktop delle singole postazioni PC al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza contro virus e malware in genere. L'intervento viene effettuato esclusivamente su chiamata dell'Utente o, in caso di oggettiva necessità, a seguito

della rilevazione tecnica di problemi nel sistema informatico e telematico. In quest'ultimo caso, e sempre che non si pregiudichi la necessaria tempestività ed efficacia dell'intervento, verrà data formale comunicazione della necessità dell'intervento stesso.

Il personal computer viene 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 richieste all'Amministratore di sistema, che provvederà ad effettuarle.

L'utente non può modificare le impostazioni del Pc autonomamente.

Di conseguenza:

- non verranno forniti privilegi di "amministratore" ad eccezione di specifiche e motivate esigenze avanzate formalmente da parte del Responsabile dell'Area interessato e dietro specifica autorizzazione rilasciata dall'Amministratore di sistema, sentito il **Responsabile del Servizio Informatico dell'Ente**;
- non è consentita l'installazione di mezzi di comunicazione personali (come ad esempio modem e dispositivi bluetooth, smartphone, chiavette per l'accesso ad internet etc.);
- non è consentito utilizzare strumenti software e/o hardware atti a 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 deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio o in caso di suo inutilizzo;
- qualora ci si allontani dalla propria postazione, occorre spegnere o "bloccare" il computer o disconnettersi (per il sistema operativo windows premendo contemporaneamente i tasti Alt+Ctrl+Canc e cliccando su blocca computer o in alternativa attivando la protezione sul proprio screen saver); lasciare un elaboratore 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.
- non è consentito utilizzare strumenti potenzialmente in grado di consentire accessi non autorizzati alle risorse informatiche (es.: programmi di condivisione quali IRC, ICQ, AudioGalaxy o software di monitoraggio della rete in genere);
- non è consentito configurare o utilizzare servizi diversi da quelli messi a disposizione da parte dell'Ente (quali DNS, DHCP, server internet Web, FTP,);
- non è consentito intercettare pacchetti sulla rete (sniffer) o software dedicati a carpire, in maniera invisibile, dati personali, password e ID dell'utente oppure a controllare ogni attività, ivi inclusa la corrispondenza e i dati personali;
- non è consentito impostare password nel bios;
- non è consentito disassemblare il computer, asportare qualsiasi apparecchiatura in dotazione all'Utente;
- non è consentito avviare il personal computer con sistemi operativi diversi da quello installato dal personale tecnico specializzato per conto dell'Ente;
- non è consentito utilizzare connessioni in remoto per l'accesso alle risorse informatiche, al di fuori del perimetro dell'Ente e fatte salve le connessioni

realizzate e autorizzate da parte dell'Amministratore di sistema, sentito il **Responsabile del Servizio Informatico dell'Ente**;

- salvo preventiva espressa formale autorizzazione dell'Amministratore di sistema, sentito il **Responsabile del Servizio Informatico dell'Ente**, non è consentito l'uso di programmi diversi da quelli ufficialmente installati dal personale tecnico per conto dell'Ente, né viene consentito agli utenti di installare autonomamente programmi provenienti dall'esterno, sussistendo infatti il grave pericolo di introdurre virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti. L'inosservanza della presente disposizione espone l'Ente a gravi responsabilità civili; si evidenzia inoltre, che le violazioni della normativa a tutela dei diritti d'autore sul software, che impone la presenza nel sistema di software regolarmente licenziato o comunque libero e quindi non protetto dal diritto d'autore, saranno sanzionate anche penalmente;
- ogni Utente deve prestare la massima attenzione ai supporti di origine esterna, sottoponendoli sempre a scansione antivirus ed avvertendo immediatamente il personale tecnico preposto nel caso in cui siano rilevati virus di qualsivoglia natura;
- Non è consentito collegare alla rete informatica Personal Computer o Pc Portatili e, più in generale, qualsiasi dispositivo hardware senza la formale autorizzazione dell'Amministratore di sistema, sentito il **Responsabile del Servizio Informatico dell'Ente**.

7. Hardware e Software

Tutto l'hardware ed il software potrà essere acquistato solo previa richiesta di parere tecnico favorevole da parte dell'Amministratore di sistema, sentito il **Responsabile del Servizio Informatico dell'Ente**, che controllerà le richieste di acquisto al fine di valutarne la compatibilità e programmare l'applicazione delle misure di sicurezza informatica.

A tal fine le richieste di acquisto dell'hardware e del software dovranno essere indirizzate all'Amministratore di sistema per la verifica tecnica di compatibilità o per la eventuale proposizione di soluzioni alternative. I supporti originali dei software acquistati e le relative licenze devono essere conservati presso il **Servizio Informatico dell'Ente**, così da consentire le operazioni di verifica della disponibilità di licenze e l'eventuale reinstallazione delle procedure.

Il personale non può utilizzare eventuale software di proprietà personale. Tutto ciò comprende anche le applicazioni regolarmente acquistate e registrate, programmi shareware e/o freeware, eventuale software scaricato da Internet o proveniente da CD/DVD allegati a riviste e/o giornali o altro software posseduto a qualsiasi titolo. Qualora fosse necessario per fini strettamente collegati all'attività lavorativa, l'utilizzo di software di proprietà personale, potrà essere installato solo previa richiesta di parere tecnico favorevole dell'Amministratore di sistema, sentito il **Responsabile del Servizio Informatico dell'Ente**, che controllerà la compatibilità con le misure di sicurezza informatica dell'Ente.

Nell'ipotesi di utilizzo di software realizzato direttamente dall'utente finale potrà essere installato solo previa richiesta di parere tecnico favorevole da parte dell'Amministratore di sistema, sentito il **Responsabile del Servizio Informatico**

dell'Ente, che controllerà la compatibilità con le misure di sicurezza informatica e qualora vengano trattati dati sensibili, darne comunicazione anche al Responsabile della Protezione dei Dati personali dell'Ente.

Il software per elaboratori è considerato opera di ingegno e come tale è tutelato dalle Leggi sul diritto di autore. L'utilizzo del software è regolamentato da licenze d'uso che devono essere assolutamente rispettate da tutti. (Dlgs. 518/92 sulla tutela giuridica del software e L. 248/2000 "nuove norme di tutela del diritto d'autore").

E' vietato provare ad installare arbitrariamente il software scaricato da Internet o contenuto nei vari supporti distribuiti con le riviste, con i libri e con i quotidiani anche se si tratta di software allegato a riviste dell'Area. Prima di installare questi programmi, qualora l'uso fosse collegato ad esigenze lavorative, sarà necessario il benestare da parte dell'Amministratore di sistema, sentito il **Responsabile del Servizio Informatico dell'Ente**.

8. Computer portatili, tablet e smartphone

L' Utente è responsabile dell'integrità dei computer portatili, tablet e smartphone affidati dall'Ente e dei dati ivi contenuti. L'Utente è tenuto a custodirlo con diligenza sia durante l'utilizzo nel luogo di lavoro sia durante i suoi spostamenti. A tali dispositivi si applicano le regole di utilizzo previste per i personal computer. Nel caso di utilizzo condiviso con altri Utenti, prima della riconsegna occorre provvedere alla rimozione definitiva di eventuali file elaborati. I dischi rigidi, se contenenti dati sensibili, dovranno essere criptati 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. Tutti i dispositivi portatili dovranno essere resi noti all'Amministratore di sistema, che provvederà all'applicazione di tutte le misure di sicurezza previste da disciplinare interno e dalla normativa vigente.

9. Stampanti, Fotocopiatori, Scanner, Fax e Telefoni

Il dipendente è consapevole che gli Strumenti di stampa, così come anche il telefono dell'Ente, sono di proprietà dell'Unione dei Comuni Erimo Ericini e sono resi disponibili all'utente per rendere la prestazione lavorativa. Pertanto ne viene concesso l'uso esclusivamente per tale fine.

Il telefono dell'Ente eventualmente affidato all'utente è uno strumento 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 l'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. Ai cellulari e smartphone dell'Ente si applicano le medesime regole sopra previste per gli altri dispositivi informatici per quanto riguarda il mantenimento di un adeguato livello di sicurezza informatica. In particolare si raccomanda il rispetto delle regole per una corretta navigazione in Internet, se consentita.

Per gli smartphone dell'Ente è vietata l'installazione e l'utilizzo di applicazioni (o altresì denominate "app" nel contesto degli smartphone) diverse da quelle autorizzate dal Servizio CED dell'Ente.

È vietato l'utilizzo delle fotocopiatrici dell'Ente per fini personali, salvo preventiva ed esplicita autorizzazione da parte del Responsabile dell'Area.

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

- stampare documenti solo se strettamente necessari per lo svolgimento delle proprie funzioni operative;
- prediligere le stampanti di rete condivise, rispetto a quelle locali/personali, per ridurre l'utilizzo di materiali di consumo (toner ed altri consumabili);
- prediligere la stampa in bianco/nero e fronte/retro al fine di ridurre i costi, se possibile.

Le stampanti e le fotocopiatrici dell'Ente devono essere spente ogni sera prima di lasciare gli uffici o in caso di inutilizzo prolungato.

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 e persone terze non autorizzate.

10. Credenziali di accesso

I sistemi di controllo degli accessi assolvono il compito di prevenire che persone non autorizzate possano accedere a un sistema informatico ed alle relative applicazioni. Lo scopo è di cautelare l'Ente e 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.

Le credenziali di autenticazione nell'intranet (accesso rete informatica), vengono inizialmente assegnate dall'Amministratore di sistema e successivamente obbligatoriamente reimpostate dal dipendente stesso secondo criteri prestabiliti dalla normativa vigente e con modalità operative di seguito meglio specificate.

Non sono ammesse impostazioni autonome della password al Bios del computer onde evitare impedimenti all'accesso in caso di prolungata assenza o impedimento dell'incaricato e considerata la necessità di questo Ente di garantire in ogni caso la continuità dei servizi istituzionali.

Le credenziali di autenticazione per l'accesso alla rete e per l'utilizzo del servizio di posta elettronica istituzionale vengono assegnate dal personale **del Servizio CED dell'Ente** previa formale richiesta da effettuarsi attraverso la compilazione dell'apposito modulo in allegato "mod-utenze-rete-email", sottoscritta dal Responsabile dell'Area presso il quale l'Utente dovrà operare.

La credenziale di autenticazione (login) consiste in un codice per l'identificazione dell'Utente (user id), assegnato dal personale tecnico **del Servizio CED dell'Ente** ed associato ad una parola chiave (password) riservata e modificata dall'Utente al primo accesso. Essa dovrà essere memorizzata, custodita con la massima

diligenza e non divulgata (ad es.: non scrivere la password su carta o post-it lasciandoli sulla scrivania o attaccati al monitor; non comunicare o condividere con altri colleghi 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 otto caratteri e deve essere "robusta". Una password si dice robusta quando è difficile ricostruirla e cioè quando risponde ad alcuni principi quali:

- all'aumentare della sua lunghezza, aumenta la difficoltà a carpirla;
- include cifre, lettere e caratteri speciali;
- non contiene il proprio nome o cognome, il soprannome, la data di nascita, il nome di persone familiari, parole comuni, nomi di paesi, animali e così via;
- non contiene parole che si trovano nei dizionari di qualsiasi lingua, anche se digitate al contrario, in quanto esistono software in grado di individuarle;
- non sono composte da semplici sequenze di tasti, come ad esempio "qwerty", o da ripetizioni del proprio nome utente (ad es. se il proprio utente è rossi; la password "rossi rossi" sarebbe inopportuna);
- è composta con più parole contenenti errori ortografici o con sillabe combinate costituite da parole non correlate tra loro.

La password di accesso di ciascun Utente di rete dovrà essere reimpostata ogni 90 giorni. In base a tale procedura automatica, l'Utente dovrà inserire una nuova password, diversa dalla precedente. **E' vietato condividere le credenziali di accesso al computer tra colleghi anche se appartenenti allo stesso Servizio o Ufficio.**

L'Utente potrà richiedere la modifica della password al personale tecnico **del Servizio CED dell'Ente** per decorrenza del termine sopra previsto in via eccezionale e/o in via ordinaria in caso questi ravveda una perdita della riservatezza. Qualsiasi azione svolta sotto l'autorizzazione offerta dalla coppia userid e password sarà attribuita in termini di responsabilità all'utente titolare del codice userid, salvo che l'utente dia prova di illecito utilizzo della sua autorizzazione da parte di terzi.

11. Utilizzo della rete e accessi da remoto

Per l'accesso alla Rete dell'Ente ciascun Utente deve essere in possesso delle specifiche credenziali sopra descritte.

E' assolutamente vietato accedere alla rete informatica e/o nei programmi con un codice d'identificazione Utente di un altro operatore.

La presenza di eventuali cartelle di rete condivise sono da considerarsi strumento di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi.

Si ricorda che tutti i dischi rigidi o altre unità di memorizzazione locali (es. dischi fissi interni o esterni al PC) non sono soggette a salvataggio da parte del personale incaricato **del Servizio CED dell'Ente**. La responsabilità del salvataggio dei dati ivi contenuti è pertanto a carico del singolo Utente.

All'interno delle sedi dell'Ente può essere resa disponibile anche una rete senza fili, c.d. "Wi-Fi". Tali reti consentono l'accesso alle risorse dell'Ente 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 il Unione dei Comuni Elimo Ericini necessitano di accedere a determinate risorse informatiche. Viene concesso, altresì, a dipendenti e funzionari dell'Ente che necessitano di svolgere compiti specifici che non possono essere svolti dalle postazioni fisse. L'impostazione della connessione Wi-Fi sarà effettuata da personale del Servizio CED dell'Ente.

Il personale tecnico **del Servizio CED dell'Ente** può in qualunque momento, senza preavviso, procedere alla rimozione dai computer in rete di ogni file e/o applicazione che riterrà essere pericolosi per la sicurezza dei dati e della rete.

Il **Servizio CED dell'Ente** si riserva la facoltà di negare o interrompere l'accesso alla rete informatica comunale mediante dispositivi non adeguatamente protetti e/o aggiornati, che possano costituire una concreta minaccia per la sicurezza informatica dell'Ente.

Non è consentito collegare alle prese di rete apparecchiature non autorizzate da parte dell'Amministratore di sistema, quali: hub, switch, access point o similari. Non è inoltre consentito installare o utilizzare qualsiasi altra apparecchiatura atta a gestire comunicazioni, salvo specifica autorizzazione rilasciata dall'Amministratore di sistema, sentito il **Responsabile del Servizio Informatico dell'Ente**, quali a titolo esemplificativo: modem, router, Internet key.

I tecnici delle ditte esterne (fornitori applicativi, sistemisti etc.) dovranno richiedere l'autorizzazione dell'Amministratore di sistema, sentito il **Responsabile del Servizio Informatico dell'Ente**, prima di collegarsi fisicamente alla rete informatica con dispositivi personali. Quest'ultimi saranno sottoposti alle politiche di sicurezza di questo Ente, al fine di garantire la sicurezza generale della rete informatica.

Gli accessi da remoto verso la rete informatica dell'Ente potranno essere effettuati solo previa autorizzazione dell'Amministratore di sistema, sentito il **Responsabile del Servizio Informatico dell'Ente**, che rilascerà apposite credenziali per l'autenticazione sicura. Tutti gli accessi saranno monitorati e registrati. Non sono ammessi accessi di tipologia differente da quella VPN (Ipsec o SSL) gestita dall'Amministratore di sistema. **Ai fini della richiesta di autorizzazione all'accesso da remoto in VPN è necessario compilare il modulo in allegato "mod-vpn-ditte" da indirizzare all'Amministratore di sistema.**

12. Credenziali di accesso ai programmi gestionali

E' possibile ottenere l'assegnazione di specifiche credenziali di autenticazione a programmi gestionali specifici, attraverso la compilazione dell'apposito **modulo in allegato "mod-utenze-gestionali"** sottoscritta dal Dirigente Responsabile dell'Area presso il quale l'Utente dovrà operare.

Il sopraindicato modulo dovrà essere compilato a cura del Dirigente Responsabile dell'Area anche in caso di trasferimento del dipendente ad altro Settore o eventuale cessazione del rapporto di lavoro con l'Ente, per la conseguente comunicazione di disattivazione dei profili di accesso.

13. Supporti rimovibili

Eventuali supporti magnetici contenenti dati sensibili devono essere adeguatamente custoditi dall'Utente in armadi o cassette chiudibili a chiave. E' vietato l'utilizzo di supporti rimovibili personali (dischi rigidi e penne USB) compreso qualsiasi altro punto di memorizzazione tramite internet (c.d. "remote storage" quali Dropbox, GoogleDrive, OneDrive, etc.) nel caso si voglia trattare dati personali, sensibili e/o giudiziari. In caso di trasferimento di dati sensibili tra computer in rete, si devono necessariamente utilizzare "cartelle di lavoro condivise" e protette da password note solo agli utenti a ciò interessati. L'Utente è responsabile della custodia dei supporti e dei dati in essi contenuti.

14. Posta elettronica

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

La casella di posta elettronica istituzionale assegnata all'Utente è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica istituzionale sono responsabili del corretto utilizzo delle stesse.

E' fatto divieto di utilizzare le caselle di posta elettronica per motivi diversi da quelli strettamente legati all'attività lavorativa. In questo senso, a titolo puramente esemplificativo, l'Utente non potrà utilizzare la posta elettronica ordinaria e certificata per:

- l'invio e/o il ricevimento di allegati contenenti filmati o brani musicali (es. mp3) non legati all'attività lavorativa;
- l'invio e/o il ricevimento di messaggi personali o per la partecipazione a dibattiti, sondaggi e aste on-line;
- la partecipazione a catene di Sant'Antonio; non si dovrà in alcun caso procedere all'apertura degli allegati a tali messaggi.

La casella di posta elettronica deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti (in termini di centinaia di MB e, ancor più di GB).

E' obbligatorio porre la massima attenzione nell'aprire i file allegati alle e-mail prima del loro utilizzo. In linea di massima non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti, altrimenti, se obbligati sottoporre necessariamente detti file ad una "scansione approfondita" dell'antivirus prima del loro utilizzo.

L'Utente assegnatario della casella di posta elettronica istituzionale è il diretto responsabile del corretto utilizzo della stessa e risponde personalmente dei contenuti trasmessi. In particolare l'Utente è tenuto a rispettare quanto segue:

- non utilizzare il servizio per scopi illegali o non conformi al presente Regolamento o in maniera tale da recar danno o pregiudizio all'Ente o a terzi;
- non utilizzare il servizio in modo da danneggiare, disattivare, sovraccaricare, pregiudicare o interferire con la fruibilità del servizio da parte degli altri utenti;
- 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;

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 (C.D. catene di Sant' Antonio) anche quando il contenuto sia volto a segnalare presunti o veri allarmi (esempio: segnalazioni di virus).

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 dell'Area/Servizio 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 istituzionale 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 e inoltrare al responsabile dell'Area in cui lavora, quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa.

Di tale attività deve essere redatto apposito verbale e 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 istituzionale 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 dell'Area cui afferisce il dipendente può chiedere all'Amministratore di sistema, sentito il **Responsabile del Servizio Informatico dell'Ente**, di accedere alla postazione e/o alla casella di posta elettronica istituzionale del dipendente assente mediante apposito **modulo in allegato "mod-password-urgenza"** in cui si evinca la richiesta.

Sarà onere del Responsabile dell'Area informare celermente il dipendente al suo rientro, fornendo adeguata spiegazione e redigendo apposito verbale.

Le caselle di posta elettronica istituzionale nominative hanno validità pari alla durata della permanenza in servizio del dipendente, fatte salve eventuali situazioni di congedo, distacco e comando. Nel caso il cui il dipendente non presti più la sua attività lavorativa presso questo Ente, la casella di posta elettronica sarà prontamente disattivata. **Su richiesta dell'interessato la casella di posta potrà restare attiva per ulteriori tre mesi dalla data di cessazione del rapporto di lavoro, durante il quale l'interessato provvederà ad inserire inserita una risposta automatica d'ufficio.**

15. Navigazione internet

Il Personal computer assegnato all'Utente ed abilitato alla navigazione in Internet costituisce uno strumento utilizzabile esclusivamente per lo svolgimento della propria attività lavorativa. È quindi assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa, all'interno dell'Ente.

In questo senso, a titolo puramente esemplificativo, l'Utente non potrà utilizzare Internet per:

- l'upload o il download di software gratuiti se non espressamente autorizzati dall'Amministratore di sistema;
- l'utilizzo di documenti (filmati e musica) provenienti da siti web o http, se non strettamente attinenti all'attività lavorativa;
- l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, fatti salvi i casi autorizzati e comunque nel rispetto delle normali procedure di acquisto;
- ogni forma di registrazione a siti i cui contenuti non siano strettamente legati all'attività lavorativa;
- la partecipazione a forum non professionali, a giochi on-line, l'utilizzo di chat line, di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames).

Al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa, l'Ente con logica preventiva, adotta uno specifico sistema di filtro automatico che impedisce determinate operazioni quali l'upload, download (illeciti o illegali) o l'accesso a determinati siti ludici (black-list). 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; peer to peer; malware, spyware, hacking, proxy anonimi, bypass proxy, phishing.

Qualsiasi altra tipologia di contenuti o siti che l'Amministratore di sistema, sentito il **Responsabile del Servizio Informatico dell'Ente**, riterrà di non dover rendere accessibile dalla rete informatica, verrà preventivamente comunicata agli utenti e al Segretario Generale. La navigazione, ovvero l'accesso ai siti Internet, potrebbe avvenire previa autenticazione dell'Utente su di un Proxy Server.

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.

Si informa che l'Ente, per il tramite del Servizio CED, non effettua la memorizzazione sistematica delle pagine web visualizzate dal singolo Utente, né controlla con sistemi automatici i dati di navigazione dello stesso.

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 dell'Ente, il Unione dei Comuni Elimo Ericini registra 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. Solo in casi eccezionali e di comprovata urgenza rispetto alle finalità sopra descritte, l'Ente può trattare i dati di navigazione riferendoli specificatamente ad un singolo nome utente.

Gli eventuali controlli per motivi di sicurezza informatica, compiuti dal personale tecnico **del Servizio CED dell'Ente**, potranno avvenire mediante un sistema di controllo dinamico dei contenuti o mediante "file di log" della navigazione svolta. Il controllo sui log, i quali sono cancellati periodicamente ed automaticamente, non è sistematico e le informazioni vengono conservate temporaneamente per finalità di sicurezza di questo Ente. Il prolungamento dei tempi di conservazione dei log potrà aver luogo solo nei seguenti casi:

- Esigenze tecniche o di sicurezza del tutto particolari;
- Indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;
- Su specifica richiesta dell'autorità giudiziaria

16. Protezione da virus

Le postazioni di lavoro collegate alla rete informatica dell'Ente sono protette da uno stesso software antivirus che viene aggiornato automaticamente grazie ad una gestione centralizzata per mezzo di un Server antivirus dedicato. **Non è ammesso l'utilizzo di sistemi antivirus differenti da quello fornito dall'Ente.**

Ogni Utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico. Questa fattispecie può accadere mediante virus o malware, proveniente da dati e/o software importati/installati dall'Utente, che si

auto-installano, all'insaputa dell'Utente, all'interno del Pc, infettandolo e diffondendosi nella rete informatica dell'Ente.

Nel caso in cui il software antivirus rilevi e non disinfezioni la presenza di un virus, l'Utente dovrà immediatamente sospendere ogni elaborazione in corso e segnalare l'accaduto all'**Amministratore di Sistema**.

Ogni dispositivo di memorizzazione esterna dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, dovrà essere prontamente consegnato al personale tecnico autorizzato che provvederà ad effettuare le dovute operazioni di disinfezione.

17. Salvataggio dati

Ogni Utente è responsabile della corretta conservazione dei dati e dei documenti elettronici che utilizza sul Pc per motivi lavorativi, di qualsiasi tipo, formato e natura essi siano. Per questo motivo la tutela della gestione dei dati sulle postazioni di lavoro (Personal computer e Pc portatili) è demandata all'Utente finale, che avrà l'obbligo di effettuare il salvataggio dei dati memorizzati sui computer in dotazione, con frequenza almeno settimanale e la conservazione degli stessi in luogo idoneo.

Costituisce buona regola la pulizia periodica (almeno ogni sei mesi) degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. E' infatti assolutamente da evitare un'archiviazione ridondante.

18. Tele-assistenza

Per lo svolgimento di normali attività di assistenza e manutenzione su personal computer connessi alla rete, l'**Amministratore di Sistema** potrà utilizzare specifici software di connessione remota. Tali programmi sono utilizzati per assistere l'Utente al fine di effettuare interventi di assistenza informatica e di manutenzione su applicativi e hardware in uso. L'attività di assistenza e manutenzione avviene previa autorizzazione da parte dell'Utente e mediante visualizzazione di un indicatore visivo sul monitor che segnala la connessione in remoto del tecnico informatico.

Gli Amministratori di Sistema (interni ed esterni) possono accedere ai dispositivi informatici dell'Ente sia direttamente, sia mediante software sicuro di accesso remoto, per i seguenti scopi:

- verifica e risoluzione di problemi sistemistici ed applicativi, su segnalazione dell'utente finale.
- verifica del corretto funzionamento dei singoli dispositivi in caso di problemi rilevati nella rete.
- richieste di aggiornamento software e manutenzione preventiva hardware e software.

Gli interventi tecnici possono avvenire previo consenso dell'utente, quando l'intervento stesso richiede l'accesso ad aree personali dell'utente stesso. Qualora l'intervento tecnico in loco o in remoto non necessiti di accedere mediante

credenziali utente, gli Amministratori di sistema sono autorizzati ad effettuare gli interventi senza il consenso dell'utente cui la risorsa è assegnata.

L'accesso in teleassistenza sui computer della rete informatica dell'Ente richiesto da terzi (fornitori e consulenti) deve essere autorizzato dall'Amministratore di Sistema, per le verifiche delle modalità di intervento per il primo accesso. Le richieste successive, se effettuate con la medesima modalità, possono essere gestite autonomamente dall'utente finale.

19. Monitoraggio

L'Amministratore di sistema potrà effettuare monitoraggi periodici su dati anonimi allo scopo di verificare l'attuazione del presente Disciplinare, 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: effettuati attraverso specifici log dei dispositivi di rete.
- analisi del traffico Internet: effettuati attraverso specifici log dei dispositivi di connessione ad Internet;
- inventario Hardware e Software: effettuati attraverso procedure prevalentemente automatiche per le apparecchiature collegate in rete e in maniera semiautomatica per le macchine non appartenenti al dominio.

Il monitoraggio delle risorse hardware e software non coinvolge in alcun modo i dati personali e i documenti presenti sulle singole postazioni di lavoro e viene effettuato per finalità organizzative e gestionali.

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

20. Controlli

L'Ente si riserva di effettuare controlli per verificare il rispetto del presente Disciplinare che costituisce preventiva e completa informativa 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.

I controlli sono effettuati nel rispetto 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 Disciplinare 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.

Nel caso in cui emerga un evento dannoso, una situazione di pericolo o utilizzi non aderenti al presente Disciplinare, che non siano stati impediti con preventivi accorgimenti tecnici o rilevati durante i monitoraggi o da attività di gestione degli strumenti informatici, l'Amministratore di sistema, sentito il **Responsabile del Servizio Informatico dell'Ente e con il supporto del Responsabile della Protezione dei dati**, potrà adottare le eventuali misure che consentano la verifica di tali comportamenti preferendo, per quanto possibile, un controllo preliminare su dati aggregati riferiti all'intero Settore o a sue articolazioni.

Il controllo su dati anonimi si concluderà con una comunicazione al Responsabile dell'Area analizzato che si preoccuperà di inviare un avviso generalizzato relativo a un utilizzo non corretto degli strumenti informatici, invitando i destinatari ad attenersi scrupolosamente al presente Disciplinare.

Qualora le anomalie e irregolarità dovessero persistere, si procederà circoscrivendo l'invito al personale afferente al Settore 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, questo 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, che ledono diritti di terzi o che, comunque, sono illegittime.

Qualora risulti necessario l'accesso alle risorse informatiche e relative informazioni su risorse informatiche di un Utente (quali file salvati, posta elettronica, pec etc..) che non sia reperibile, in quanto ad esempio assente, temporaneamente irreperibile ovvero cessato, il Responsabile dell'Area, per il tramite dell'Amministratore di Sistema dell'Ente, si atterrà alla procedura descritta qui di seguito:

- a) Redazione di un atto da parte del Responsabile dell'Area che comprovi le necessità produttive e di organizzazione che richiedano l'accesso allo Strumento;
- b) 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;
- c) Redazione di un verbale che riassume i passaggi precedenti;
- d) In ogni caso l'accesso ai documenti presenti nella risorsa è limitato a quanto strettamente indispensabile alle finalità produttive e di organizzazione del lavoro;
- e) 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, sempre nel rispetto di quanto disposto dal Regolamento Europeo 2016/679.

21. Conservazione dei dati

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, saranno cancellati entro i termini indicati nel presente Regolamento, comunque per un massimo di 12 mesi, salvo esigenze ulteriori 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.

22. Social Media

L'eventuale utilizzo a fini promozionali di Facebook, Twitter, LinkedIn, Whatsup, dei blog e dei forum, anche professionali (ed altri siti o social media) è gestito ed organizzato esclusivamente dall'Ente attraverso specifiche direttive ed istruzioni operative al personale a ciò espressamente addetto, rimanendo escluse iniziative individuali da parte dei singoli utenti o collaboratori.

Fermo restando il diritto della persona alla libertà di espressione, l'Ente ritiene comunque opportuno indicare agli utenti alcune regole comportamentali, al fine di tutelare tanto la propria immagine ed il patrimonio dell'Ente, anche immateriale, quanto i propri dipendenti, i propri fornitori oltre che gli stessi cittadini 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 dall'Utente sia che utilizzi dispositivi messi a disposizione dall'Ente, sia che utilizzi propri dispositivi, sia che partecipi ai social media a titolo personale, sia che lo faccia per finalità professionali, come dipendente dell'Ente.

La condivisione dei contenuti nei social media deve sempre rispettare e garantire la segretezza sulle informazioni dell'Ente, nel rispetto del segreto d'ufficio, segreto professionale e della protezione dei dati.

E' vietato l'utilizzo di strumenti di condivisione quali Whatsup, Telegram etc.. per la trasmissione tra colleghi di documenti istituzionali attraverso dispositivi di proprietà personale.

23. Sanzioni

È fatto obbligo a tutti i dipendenti ed utenti del sistema informativo/informatico dell'Ente di osservare le disposizioni portate a conoscenza con il presente Disciplinare. Il mancato rispetto o la violazione delle regole sopra ricordate è perseguibile con provvedimenti disciplinari e/o risarcitori previsti dalla vigente normativa, nonché con tutte le azioni civili e penali consentite.

24. Aggiornamento e revisione

Il presente Disciplinare è stato redatto tenendo conto del Regolamento UE 2016/679, delle Linee guida dell'Autorità Garante per la protezione dei dati personali, emanate con delibera n. 13 del 1° marzo 2007 e della Direttiva n.2/2009 del Ministro per la Pubblica Amministrazione e Innovazione.

Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni motivate al presente documento. Il presente Disciplinare è soggetto a revisione come per Legge o qualora se ne ravveda la necessità.

Copia del presente documento verrà consegnata a ciascun dipendente ovvero messo a disposizione per ogni Utente autorizzato all'utilizzo della rete informatica dell'Ente.

Il presente Disciplinare entra in vigore a seguito della esecutività della deliberazione di approvazione. Dalla predetta data tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi sostituite dalle presenti.