Unione dei Comuni
Terre e Fiumi
Copparo - Berra - Tresigallo - Formignana - Ro

Regolamento per l'utilizzo degli strumenti informatici e telematici dell'Unione dei Comuni Terre e Fiumi

Approvato con delibera di Giunta dell'Unione Terre e Fiumi n°32 del 14/05/2018

Perché un Regolamento informatico?

La diffusione delle nuove tecnologie informatiche ed in particolare l'utilizzo della rete internet tramite le risorse informatiche e l'aumento di informazioni trattate con strumenti elettronici aumentano di fatto i rischi legati alla sicurezza e all'integrità delle informazioni oltre alle conseguenti responsabilità previste dalla normativa civile e penale.
L'Unione dei Comuni Terre e Fiumi (nel seguito Ente), pertanto, deve provvedere a garantire la continuità della sua attività e assicurare la riservatezza delle informazioni e dei dati, in maniera tale da evitare che comportamenti consapevoli e/o inconsapevoli possano innescare problemi o minacce alla sicurezza nel trattamento dei dati o diminuire l'efficienza delle risorse informatiche dell'Ente.
In questo contesto, l'Ente ha ritenuto necessario adottare il presente Regolamento al fine di evidenziare ai dipendenti e collaboratori le indicazioni e le misure necessarie e opportune per il corretto utilizzo nel rapporto di lavoro dei personal computer (fissi e portatili), della posta elettronica e di internet inclusi social network, definendo le modalità di utilizzo nell'ambito dell'attività lavorativa e dando la massima diffusione alla cultura sulla sicurezza informatica intesa come capacità e consapevolezza dell'utilizzo delle risorse informatiche.

1. Principi generali

Con l'approvazione del presente regolamento l'Ente si pone l'obiettivo di fornire a tutti i dipendenti le linee di comportamento per il corretto utilizzo delle risorse informatiche, della posta elettronica e dell'accesso alla rete internet.
Inoltre, l'Ente, in qualità di Titolare del trattamento dei dati personali dell'Unione , ritiene opportuno dotarsi di questo Regolamento al fine di adempiere gli obblighi fissati dal Regolamento Europeo sul trattamento dei dati personali (GDPR) e fornire le necessarie indicazioni ai comuni membri in quanto titolari dei dati degli enti stessi.

I trattamenti effettuati dall'Ente rispettano le garanzie poste in essere dal legislatore in materia di protezione dei dati personali e si svolgono nell'osservanza dei principi sanciti dalla normativa privacy.
In quest'ottica, l'Ente tratta i dati dei lavoratori nella misura meno invasiva possibile, affidando eventuali attività di monitoraggio esclusivamente a quei soggetti opportunamente preposti ed effettuando eventuali controlli esclusivamente in maniera mirata sull'area di rischio.
Ogni lavoratore potrà far valere i propri diritti sanciti dalla normativa sul trattamento dei dati personali rivolgendo una specifica richiesta scritta al Titolare del trattamento.

1.1. Campo di applicazione

Il presente Regolamento si applica a tutti i lavoratori ed a tutti i collaboratori dell'Ente, a prescindere dal rapporto contrattuale con la stessa intrattenuto (lavoratori somministrati, collaboratori a progetto, stagisti, consulenti ecc).
Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche e telematiche, per

"Utente" deve intendersi ogni dipendente e collaboratore (collaboratore a progetto, in stage, agente, ecc.) in possesso di specifiche credenziali di autenticazione e autorizzato all'utilizzo delle risorse informatiche ed al trattamento dei dati personali.

1.2. Entrata in vigore e Aggiornamenti

Il Regolamento è stato approvato con delibera n°32 del 14/05/2018 e sarà adottato dal 15/05/2018. Con l'entrata in vigore del presente regolamento tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi abrogate e sostituite dalle presenti.

Al fine di informare i propri dipendenti del contesto del presente Regolamento lo stesso sarà:

a) consegnato a ciascun dipendente ed a ciascun collaboratore ad inizio attività;
b) pubblicato sulla pagina intranet aziendale;

L'Ente si riserva la facoltà di apportare, in qualsiasi momento, modifiche al presente documento, dandone comunicazione a tutti gli incaricati con le modalità che riterrà opportune. La versione a cui fare riferimento sarà sempre quella pubblicata sulla pagina intranet aziendale.
Il presente Regolamento è stato predisposto ad uso esclusivamente interno dell'Ente e, pertanto, non potrà essere riprodotto, divulgato, copiato, utilizzato e/o altrimenti reso pubblico in assenza di una previa approvazione scritta dell'Ente stesso.

Nel presente regolamento si farà riferimento alla figura dell'**Amministratore di Sistema**, che dovrà essere nominato ufficialmente, e al **Servizio IT** che coincide con l'Ufficio Sistemi Informativi e Telematici dell'Unione Terre e Fiumi.

Il presente regolamento **si applica a tutti gli Enti,** facenti parte dell'Unione dei Comuni Terre e Fiumi.

2. Regole di comportamento generali

L'Unione Terre e Fiumi è titolare di qualsiasi diritto connesso ai sistemi informativi ed alle risorse informatiche, ai dati, ai contenuti di ogni tipo e genere, elaborati, creati, o modificati nell'ambito delle attività lavorative e tramite l'opera dei suoi dipendenti e collaboratori.

Per **Risorse informatiche** si intende qualsiasi strumento informatico di proprietà dell'Ente o dei Comuni membri, ed utilizzato dal lavoratore per rendere la prestazione lavorativa. A titolo esemplificativo ma non esaustivo sono risorse informatiche: personal computers fissi e portatili; tablets; telefoni cellulari semplici; telefoni cellulari smartphone; viacard; telepass; carte di credito; sistemi di geolocalizzazione (navigazione satellitare e sistemi di antifurto satellitare) installati su veicoli aziendali, indirizzo email aziendale, rete aziendale.

L'utilizzo delle risorse informatiche e telematiche aziendali, deve avvenire nell'ambito del generale contesto di diligenza, fedeltà e correttezza che caratterizza il rapporto lavorativo fra l'Ente ed i propri dipendenti. L'Utente dovrà adottare 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.
L'Ente, pertanto, consapevole delle potenzialità fornite dagli strumenti informatici e telematici, li mette a disposizione dei propri dipendenti e collaboratori esclusivamente per finalità di tipo lavorativo.
Non è quindi permesso utilizzare detti strumenti per altre finalità non connesse all'attività lavorativa o in modo che violino qualsiasi disposizione normativa.
Al riguardo si evidenzia che l'Ente adotterà ogni accorgimento tecnico necessario a tutelarsi da eventuali comportamenti non permessi, salvaguardano il rispetto della libertà e della dignità dei lavoratori.

Di seguito vengono descritte le linee di comportamento a cui gli Utenti devono attenersi nell'esecuzione dei compiti che implicano un trattamento di dati personali tramite le risorse informatiche.
In generale l'Utente deve osservare le seguenti regole di ordinaria diligenza, nonché tutte le altre ulteriori misure ritenute necessarie per garantire il rispetto di quanto disposto dalla normativa privacy:

a) tutte le operazioni di trattamento devono essere effettuate in modo tale da garantire il rispetto delle misure di sicurezza, la massima riservatezza delle informazioni di cui si viene in possesso considerando tutti i dati confidenziali e, di norma, soggetti al segreto d'ufficio;
b) le singole fasi di lavoro e la condotta da osservare devono consentire di evitare che i dati siano soggetti a rischi di perdita o distruzione, che vi possano accedere persone non autorizzate, che vengano svolte operazioni di trattamento non consentite o non conformi ai fini per i quali i dati stessi sono stati raccolti;
c) non devono essere eseguite operazioni di trattamento per fini non previsti tra i compiti assegnati dal diretto responsabile;
d) devono essere svolte le sole operazioni di trattamento necessarie per il raggiungimento dei fini per i quali i dati sono stati raccolti;
e) deve essere costantemente verificata l'esattezza dei dati trattati e la pertinenza rispetto alle finalità perseguite nei singoli casi.

Quanto sopra descritto impone, in altri termini, all'Utente di operare con la massima attenzione in tutte le fasi di trattamento, dalla esatta acquisizione dei dati, al loro aggiornamento, alla conservazione ed eventuale distruzione.

3. Regole operative

3.1. Uso del Pc

Il personal computer (comprese le periferiche ad esso connesse) ed i relativi programmi e/o applicazioni affidati al dipendente sono, come è noto, strumenti di lavoro; tali strumenti pertanto:

a) vanno custoditi in modo appropriato;
b) possono essere utilizzati solo per fini professionali (in relazione, ovviamente, alle mansioni assegnate) e non a fini personali, tanto meno per scopi illeciti; Ogni utilizzo non inerente all'attività lavorativa è vietato perché può contribuire ad innescare disservizi, costi di manutenzione. Eventuali minacce alla sicurezza debbono essere prontamente segnalati al Servizio IT, come anche il furto, il danneggiamento, lo smarrimento;
c) Il personal computer assegnato all'Utente permette l'accesso alla rete dell'Ente solo attraverso specifiche credenziali di autenticazione**;**
d) Non è consentito l'uso di programmi diversi da quelli ufficialmente installati ed autorizzati dal Servizio IT, 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. Per ogni modifica alla configurazione delle risorse informatiche assegnate, è necessario rivolgersi al Servizio Informatico;
e) Non è consentita la riproduzione o la duplicazione di programmi informatici ai sensi della Legge 21/05/2004 n. 128. L'inosservanza della presente disposizione espone a gravi responsabilità civili, amministrative e penali, nonché disciplinari;
f) Non è consentita l'attivazione della password d'accensione (Bios) senza preventiva autorizzazione dell'amministratore di sistema, né modificare le caratteristiche hardware e software impostate sul proprio PC;
g) Ogni Utente deve prestare la massima attenzione ai supporti USB forniti dall'Ente, avvertendo immediatamente l'Amministratore di Sistema nel caso in cui siano rilevati virus. Non è consentito collegare dispositivi USB diversi da quelli forniti, ad eccezioni delle chiavette USB per la firma digitale di soggetti esterni;
h) Si rimanda al paragrafo 3.11 per quanto concerne i salvataggi dei file;
i) Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici, in caso di assenze prolungate dall'ufficio o in caso di suo inutilizzo. In ogni caso, 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**.**
j)

3.2. Utilizzo di Pc Portatili

L'Utente è responsabile del PC portatile assegnatogli dall'Ente e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.
I PC portatili:
□ utilizzati all'esterno dell'Ente, devono essere custoditi con diligenza, adottando tutti i provvedimenti che le circostanze rendono necessari per evitare danni o sottrazioni.
□ non devono essere lasciati incustoditi e sul disco devono essere conservati solo i file strettamente necessari.
Nel caso di accesso alla rete aziendale tramite RAS (Remote Access Server) / Accesso Remoto / VPN (Virtual Private Network), deve essere utilizzato l'accesso in forma esclusivamente personale attraverso le Credenziali di Autenticazione fornite. Al termine della sessione di collegamento, dovrà essere effettuata la disconnessione attraverso il software utilizzato.
I PC portatili, dovranno essere periodicamente collegati alla Rete interna al fine di consentire gli aggiornamenti antivirus.

3.3. Credenziali di autenticazione

Le credenziali di autenticazione per l'accesso al PC, la connessione alla rete e/o per l'accesso ai diversi applicativi, vengono assegnate all'Utente dal Servizio IT, in seguito alla sottoscrizione del contratto di assunzione o di collaborazione.
Le credenziali di autenticazione consistono in un codice per l'identificazione dell'Utente (user id), associato ad una parola chiave (password) riservata che dovrà venir custodita dall'Utente con la massima diligenza e non divulgata.
La password, che rappresenta la parte segreta delle credenziali, è conosciuta solo dall'Utente, è composta da almeno da 8 caratteri, deve essere formata da lettere (maiuscole o minuscole) e/o numeri, anche in combinazione fra loro, e non deve contenere riferimenti facilmente riconducibili all'Utente (nome, cognome, data di nascita ecc.).
L'Utente, ha l'obbligo di modificare la password dopo il primo utilizzo e la stessa va poi modificata con cadenza trimestrale.
Per garantire la segretezza delle credenziali e la sicurezza durante le sessioni di trattamento dei dati, ogni Utente dovrà:
a) Evitare di condividere in qualsiasi modo la password;
b) Non lasciare accessibile l'elaboratore durante una sessione di trattamento dei dati;
c) Accertarsi che sia impostato uno screen saver dotato di password (con tempi di avvio brevi) che blocchi l'accesso all'elaboratore in caso sia necessario allontanarsi per un tempo prolungato;
d) Qualora il pc sia utilizzato da più incaricati, ricordarsi, sempre al termine del lavoro effettuato, di disconnettersi dal sistema (dal menù avvio/start scegliere chiudi e poi disconnetti Utente).

Le credenziali sono strettamente personali e non possono essere cedute a terzi. Il mantenimento della segretezza delle credenziali è ad esclusivo carico dell'Utente, il quale sarà il solo responsabile per qualsiasi attività posta in essere tramite l'utilizzo delle stesse.
In caso di smarrimento delle credenziali o di sospetta compromissione della sicurezza delle stesse, ne va fatta immediata segnalazione al servizio IT.

Non sono consentite credenziali generiche, non associate quindi ad un utente.

3.4. Antivirus

Il sistema informatico ed i pc collegati alla rete dell'Ente sono protetti da software antivirus aggiornati quotidianamente e automaticamente.
E' vietato cancellare, riconfigurare o disattivare detto software antivirus.
Ogni Utente è comunque tenuto a comportarsi in modo tale da ridurre il rischio di attacco al sistema informatico aziendale da parte di virus o attraverso qualsiasi altro software non sicuro.
L'Utente dovrà segnalare eventuali anomalie al Servizio IT.

3.5. Utilizzo e Conservazione dei supporti rimovibili

Tutti i supporti magnetici rimovibili (CD e DVD riscrivibili, supporti USB, ecc.), contenenti dati personali, sensibili e/o informazioni riservate, devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto o, successivamente alla cancellazione, recuperato. L'Utente è responsabile della custodia dei supporti e dei dati in essi contenuti.
Al fine di assicurare la distruzione e/o inutilizzabilità di supporti magnetici rimovibili contenenti dati personali, ciascun Utente dovrà seguire la corretta procedura indicata dal servizio IT;
In ogni caso, i supporti magnetici contenenti dati personali devono essere dagli Utenti adeguatamente custoditi in armadi chiusi.
Non è consentito l'utilizzo di supporti rimovibili personali quali CD, chiavette USB, smartphone.

3.6. Utilizzo dei device (smartphone - tablet)

I device affidati all'Utente sono strumenti di lavoro e l'Ente non ne consente un utilizzo promiscuo. Gli utilizzi non strettamente inerenti all'attività lavorativa dovranno essere comunque limitati e regolati dalla massima diligenza. Rimane inteso che è assolutamente vietato l'utilizzo dei device forniti per la visione, il download ed il caricamento di contenuti contrari al buoncostume e rientranti quindi in ambiti pornografici e/o violenti; altresì vietato il download, la riproduzione e la condivisione di contenuti online e multimediali ottenuti illegalmente in violazione alla normativa sul diritto d'autore ed al codice penale.
Ogni utilizzo che possa in qualche modo contribuire ad innescare disservizi, costi di

manutenzione e, soprattutto, minacce alla sicurezza, è assolutamente vietato; qualora si riscontrassero addebiti o sanzioni derivanti da un utilizzo improprio del device questi rimarranno a carico della persona che ha commesso l'infrazione.

I device devono essere custoditi con cura evitando ogni possibile forma di danneggiamento. L'Utente è responsabile dei device assegnati e deve custodirli con diligenza sia fuori dall'Ente sia durante l'utilizzo nel luogo di lavoro.
I device utilizzati fuori dalla sede dell'Ente, devono essere custoditi con diligenza, adottando tutti i provvedimenti che le circostanze rendono necessari per evitare danni o sottrazioni.

3.7. Uso della rete aziendale

L'accesso alla rete dell'Ente avviene contestualmente all'inserimento delle credenziali di autenticazione per l'accesso al pc.
È assolutamente proibito entrare nella rete e negli applicativi con un codice d'identificazione Utente diverso da quello assegnato.
Le cartelle utenti presenti nei server dell'Ente sono aree di memorizzazione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto, qualunque file che non sia legato all'attività lavorativa non vi può essere collocato. Su queste unità vengono svolte regolari attività di controllo, amministrazione e back up da parte del Servizio IT.
Si ricorda che tutti i dischi o altre unità di memorizzazione locali (es. disco C: interno al pc) non sono soggette a salvataggio da parte del personale incaricato sel Servizio IT. La responsabilità del salvataggio dei dati ivi contenuti è pertanto a carico del singolo Utente.
E' vietato connettere in rete (via cavo o in Wi-Fi) stazioni di lavoro o altri dispositivi hardware, diversi da quelli forniti dell'Ente. A titolo esemplificativo, ma non esaustivo, è vietato:

- Connettere alla rete aziendale personal computer personali o comunque non forniti dall'Ente;
- Connettere alla rete aziendale qualsiasi apparato di rete (nas, switch, router, access point).;

A tal scopo verranno attivate tutte le misure tecniche, atte ad impedire l'accesso alla rete da parte di qualunque dispositivo non autorizzato e censito dall'Amministratore di Sistema.

Il Servizio IT potrà in qualunque momento e senza alcun preavviso rimuovere i dispositivi non autorizzati, dando seguito alle opportune azioni disciplinari nei confronti dei trasgressori.

E' vietato monitorare, attraverso qualsiasi dispositivo hardware o software, ciò che transita in rete.
Per qualunque attività che preveda l'utilizzo della rete dati, anche se riguardanti ambiti non conferiti al servizio IT dell'Unione, è necessario informare e procedere in accordo con il servizio IT stesso e con l'amministratore di sistema.

3.8. Uso della rete internet

La rete Internet è ormai divenuta uno strumento operativo di comunicazione imprescindibile pertanto costituisce a tutti gli effetti uno strumento aziendale necessario allo svolgimento dell'attività lavorativa.
Un suo utilizzo non corretto, però, può rendere l'Ente vulnerabile sotto il profilo della sicurezza. È quindi assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa.

Pertanto, l'Utente deve usare internet in modo da non rivelare o diffondere al pubblico informazioni di tipo confidenziale o di proprietà dell'azienda (database ed informazioni in essi contenute, liste clienti, software, codici di accesso ai computer ed alla rete, dati ed informazioni personali e relazioni di lavoro). Non è consentito l'uso di sistemi di cloud storage, anche tramite applicazione web, quali DropBox, se diversi da quelli espressamente autorizzati.

Alla luce di ciò, l'Ente, anche per limitare il più possibile i controlli, ha adottato alcune misure ritenute opportune per proteggere i propri sistemi elettronici dall'eventuale utilizzo non accorto della navigazione su Internet da parte dei lavoratori.

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

a) l'upload o il download di software gratuiti (freeware) e shareware, nonché l'utilizzo di documenti provenienti da siti web o http, se non strettamente attinenti all'attività lavorativa (filmati e musica) e previa verifica dell'attendibilità dei siti in questione;
b) l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, fatti salvi i casi direttamente autorizzati dall'Ente e comunque nel rispetto delle normali procedure di acquisto;
c) ogni forma di registrazione a siti i cui contenuti non siano strettamente legati all'attività lavorativa;
d) la partecipazione a Forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche come i social network e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames) se non espressamente autorizzati dall'Ente;
e) l'accesso, tramite internet, a caselle webmail di posta elettronica personale.

Al fine di evitare la navigazione in siti non pertinenti (a rischio) all'attività lavorativa, l'Ente rende peraltro nota l'adozione di un sistema di blocco o filtro automatico che prevenga determinate operazioni quali l'upload o l'accesso a siti ad alta rischiosità inseriti in una black list.
I filtri sopraindicati limitano l'accesso ai siti Internet che presentano i seguenti contenuti:
□ illegali o non etici;
□ materiale per adulti, pornografia;

□ giochi, scommesse, intermediazione e trading, download software;
□ social network, radio e tv internet;
□ peer to peer;
□ malware, spyware, hacking, bypass proxy, phishing.
Gli eventuali controlli, compiuti dal Servizio IT potranno avvenire mediante un sistema di controllo dei contenuti (Proxy server) o mediante "file di log" della navigazione svolta. Il controllo sui file di log non è continuativo ed i file stessi vengono conservati non oltre il tempo indispensabile per il corretto perseguimento delle finalità organizzative e di sicurezza dell'azienda.

3.9. Uso della posta elettronica

La casella di posta elettronica assegnata all'Utente è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.
È vietato utilizzare le caselle di posta elettronica **istituzionali** 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 per:
a) l'invio e/o il ricevimento di allegati contenenti filmati o brani musicali (es.mp3) non legati all'attività lavorativa;
b) l'invio e/o il ricevimento di messaggi personali o per la partecipazione a dibattiti, aste on line, concorsi, forum o mailing-list se non legati all'attività lavorativa;
c) la partecipazione a catene telematiche (o di Sant'Antonio).
Non si dovrà in alcun caso procedere all'apertura degli allegati a tali messaggi.
La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.

Nel caso di mittenti sconosciuti o messaggi insoliti, per non correre il rischio di essere infettati da virus, contattare il Servizio IT.
Nel caso di messaggi provenienti da mittenti conosciuti ma che contengono allegati sospetti (file con estensione .exe, .scr, .bat ecc), o comunque in caso di dubbio, è necessario sincerarsi della veridicità della mail contattando il mittente stesso. È obbligatorio quindi porre la massima attenzione nell'aprire i file attachements di posta.

Al fine di ribadire agli interlocutori la natura esclusivamente istituzionale della casella di posta elettronica, i messaggi devono contenere il seguente avvertimento standardizzato nel quale sia dichiarata la natura non personale dei messaggi stessi.
Pertanto, nei messaggi inviati tramite posta elettronica aziendale verrà inserito il seguente testo
" Si segnala che il presente messaggio e le risposte allo stesso potranno essere conosciute dall'organizzazione lavorativa di appartenenza del mittente secondo le modalità previste dal regolamento aziendale adottato in materia. Se per un disguido avete ricevuto questa email

senza esserne i destinatari vogliate cortesemente distruggerla e darne comunicazione all'indirizzo mittente"

Al fine di garantire la funzionalità del servizio di posta elettronica istituzionale e di ridurre al minimo l'accesso ai dati, nel rispetto del principio di necessità e di proporzionalità, in caso di assenze programmate (ad es. per ferie o attività di lavoro fuori sede dell'assegnatario della casella) sarà compito dell'Utente impostare un messaggio di risposta automatica contenente le "coordinate" di posta elettronica di un altro soggetto o altre utili modalità di contatto della struttura. Si ribadisce che, in tal caso, la funzionalità deve essere attivata dall'Utente che potrà altresì impostare un inoltro automatico della posta in arrivo, a un indirizzo mail di un collega, delegato a gestire i messaggi ritenuti rilevanti per lo svolgimento dell'attività lavorativa.
In caso di assenza non programmata (ad es. per malattia) la procedura di risposta automatica - qualora non possa essere attivata dal lavoratore avvalendosi del servizio webmail entro due giorni – su richiesta di un responsabile, potrà essere attivata a cura dell'Ente, avvalendosi del Servizio IT, dandone comunicazione all'interessato appena possibile.

In caso di cessazione del rapporto di lavoro, la casella verrà definitivamente eliminata, compreso tutto l'eventuale contenuto, entro 30 giorni dalla data di cessazione. Opportune risposte automatiche o inoltri devono essere impostati dall'Utente con congruo anticipo. Nessuna operazione di salvataggio dei messaggi eventualmente presenti verrà fatta dal personale del Servizio IT dell'Ente. In merito, è pertanto compito del responsabile accordarsi preventivamente con l'utente che cesserà il rapporto di lavoro.

L'Utente, potrà altresì, tramite apposita modulistica, autorizzare l'Ente ad accedere alla casella di posta elettronica, per utilizzare a fini lavorativi eventuali messaggi presenti, ferma restando la chiusura definitiva della stessa entro i tempi prestabiliti.

3.10. Stampanti

Per quanto concerne l'utilizzo delle stampanti, gli utenti sono tenuti a:
□ stampare documenti e atti solo se strettamente necessari per lo svolgimento delle proprie funzioni lavorative;
□ prediligere le stampanti di rete in luogo di quelle locali al fine di ridurre l'utilizzo di materiali di consumo;
□ le stampanti locali devono essere spente ogni sera prima di lasciare gli uffici o in caso di loro utilizzo.
Qualora l'Utente dovesse stampare documenti contenenti dati o informazioni riservate, dovrà avere cura di monitorare la stampante e preservare, limitatamente alle oggettive possibilità, la conoscibilità di tali dati o informazioni da parte di terzi non autorizzati.

Qualunque configurazione delle stampanti di rete, sia al momento della prima installazione che successivamente, va obbligatoriamente fatta in accordo e tramite il Servizio IT.

3.11. Gestione dati

L'Ente raccomanda di salvare frequentemente i documenti su cui si lavora ed in particolare, quando ci si allontana dalla postazione anche per breve tempo.

I dipendenti e collaboratori devono salvare i dati ed i documenti aziendali aventi importanza rilevante, in primo luogo nel software gestionale utilizzando gli strumenti messi a disposizione ed in particolare il fascicolo informatico. Al momento della stesura del presente Regolamento, è in corso di attivazione la procedura di conservazione a norma presso il Parer.

In secondo luogo i propri file devono essere salvati sul file server, nella cartelle a cui si ha accesso. Ad ogni settore/servizio è attribuita una quota disco fissa pari a 10 GB; tale spazio è da utilizzare per tutti i lavori correnti. Sarà fornito un ulteriore spazio per l'archiviazione, ribadendo però l'importanza del gestionale e della conservazione a norma.
Costituisce comunque regola fondamentale la periodica pulizia di tutte le cartelle a cui si ha accesso sul file server, con cancellazione dei file obsoleti o che non hanno alcuna finalità e/o utilità per il business aziendale o perché non utilizzabili, per le attività/funzioni/mansioni assegnate. Particolare attenzione deve essere prestata alla duplicazione dei dati. E' infatti assolutamente da evitare un'archiviazione ridondante.
Tutto ciò che viene memorizzato su file server è sottoposto a backup quotidiano, con una profondità di 7 giorni.

E' comunque possibile memorizzare dati e documenti sul proprio pc, con la consapevolezza che in caso di guasto al disco fisso, tutto sarà irrimediabilmente perduto.

4. Monitoraggi e controlli dell'Ente

4.1. Accesso ai Dati Dell'Utente

L'Amministratore di Sistema o i suoi delegati possono accedere ai dati trattati dall'Utente esclusivamente per motivi di sicurezza e protezione del sistema informatico (ad es., contrasto virus, malware, intrusioni telematiche, fenomeni quali spamming, phishing, spyware, etc.), ovvero per motivi tecnici e/o manutentivi e/o di regolare svolgimento dell'attività lavorativa (ad esempio, aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware).
A titolo esemplificativo, ma non esaustivo, il personale del Servizio IT può accedere al pc di un Utente non presente, per l'installazione di un software, dandone comunicazione all'interessato, informandolo in merito alle attività svolte.

Il personale del Servizio IT, in caso di assenza improvvisa o prolungata dell'Utente o comunque non programmata e per improrogabili necessità di sicurezza o di continuità di servizio è abilitato ad accedere alla postazione dell'Utente, per le strette necessità operative. Di tale avvenuto accesso dovrà comunque essere data tempestiva comunicazione all'Utente tramite verbale d'intervento.
L'Amministratore di Sistema può procedere a controlli sulla navigazione finalizzati a garantire l'operatività e la sicurezza del sistema, nonché il necessario svolgimento delle attività lavorative, es. mediante un sistema di controllo dei contenuti (Proxy server) o mediante "file di log" della navigazione svolta. Si intende per file di log la registrazione sequenziale e cronologica delle operazioni effettuate da un sistema informatico in formato testuale.
Il sistema informativo fornisce una serie di informazioni inerenti l'utilizzo dei software e/o dell'hardware di ciascuna postazione di lavoro. In via esemplificativa e non esaustiva il sistema informativo fornisce:
□ log di accesso a internet;
□ log inerenti la posta elettronica e servizi mail to fax;
□ log inerenti l'accesso alle banche dati e agli applicativi;
□ log di attività di computer (accensione , spegnimento);
□ log di stampa.

L'eventuale controllo sui file di log da parte dell'Amministratore di Sistema non è comunque continuativo ed è limitato ad alcune informazioni, ad esempio:

a) Posta elettronica: l'indirizzo del mittente e del destinatario, la data e l'ora dell'invio e della ricezione e l'oggetto.
b) Navigazione Internet: il nome dell'Utente, l'identificativo della postazione di lavoro, indirizzo IP, la data e ora di navigazione, il sito visitato e il totale degli accessi effettuati.

I file di Log vengono conservati per il periodo strettamente necessario per il perseguimento delle finalità organizzative, produttive e di sicurezza dell'azienda, e comunque non oltre 6 mesi, fatti salvi in ogni caso specifici obblighi di legge.
Il sistema di registrazione dei log è configurato per cancellare periodicamente ed automaticamente (attraverso procedure di sovrascrittura) i dati personali degli utenti relativi agli accessi internet e al traffico telematico.
L'Amministratore di Sistema è altresì abilitato ad accedere ai dati contenuti negli strumenti informatici restituiti dall'Utente all'azienda per cessazione del rapporto, sostituzione delle apparecchiature, etc. Sarà cura dell'Utente la cancellazione preventiva di tutti gli eventuali dati personali eventualmente ivi contenuti.
In caso di cessazione tutti i dati contenuti negli strumenti informatici saranno comunque eliminati definitivamente entro 30 giorni dalla data di cessazione e saranno disabilitate tutte

le credenziali dell'utente stesso. Tramite opportuna modulistica, l'Utente potrà autorizzare l'Ente ad utilizzare a fini lavorativi i dati presenti nei dispositivi avuti in affidamento.

In ogni caso, l'Ente garantisce la non effettuazione di alcun trattamento mediante sistemi hardware e software specificatamente preordinati al controllo a distanza, quali, a titolo esemplificativo:
a) lettura e registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori (log) al di là di quanto tecnicamente necessario per svolgere il servizio e-mail;
b) riproduzione ed eventuale memorizzazione sistematica delle pagine web visualizzate dal lavoratore;
c) lettura e registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo.

4.2. Controlli

L'Ente ha l'obbligo di salvaguardare la funzionalità e il corretto impiego degli strumenti informatici da parte dei lavoratori, pertanto, si riserva il diritto di effettuare controlli per verificare il rispetto del presente Regolamento.
A tale proposito si sottolinea che le Risorse Informatiche sono di proprietà dell'Ente di appartenenza in quanto mezzo di lavoro. E' pertanto fatto divieto di utilizzo delle Risorse Informatiche e dell'accesso alla rete internet per fini ed interessi non strettamente coincidenti con quelli dell'Ente stesso.
Con riferimento a tali controlli il presente Regolamento costituisce preventiva e completa informazione nei confronti dei dipendenti e collaboratori.

Le verifiche sugli strumenti informatici saranno eseguite dall'Ente nel pieno rispetto dei diritti e delle libertà fondamentali degli utenti e del presente Regolamento, secondo i principi di pertinenza e non eccedenza.
L'Ente, pertanto, si riserva il diritto di controllare, anche in maniera occasionale e/o discontinua il corretto utilizzo degli strumenti di lavoro, implementando, però, ogni misura tecnologica volta a minimizzare il più possibile l'uso di dati identificativi dei lavoratori, nei modi e nei limiti esplicitati di seguito e nel successivo paragrafo denominato "Graduazione dei controlli".

In nessun caso tali controlli verranno impiegati per un monitoraggio dell'efficienza dell'attività lavorativa del singolo individuo come prescritto dall'art. 4 Statuto dei lavoratori.

I controlli si svolgeranno in forma graduata:

a) in via preliminare l'Ente provvederà ad eseguire dei controlli su dati aggregati, riferiti all'intera struttura ovvero a sue aree e dunque un controllo anonimo che può concludersi con un avviso generalizzato relativo ad un rilevato utilizzo anomalo degli strumenti aziendali e con invito ad astenersi scrupolosamente ai compiti assegnati ad alle istruzioni impartite;

b) in assenza di successive anomalie non si effettueranno controlli su base individuale. In tali casi, il controllo si concluderà con un avviso ai dipendenti interessati ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite.

Nel caso vengano rilevate continue anomalie si procederà a controlli su base individuale o per postazione di lavoro e in caso di abusi di singoli e reiterati si eseguiranno controlli nominativi o su singoli dispositivi e/o postazioni di lavoro (indicando le ragioni legittime, specifiche e non generiche, per cui i controlli vedrebbero effettuati – anche per verifiche sulla funzionalità e di sicurezza del sistema – inoltrando preventivi avvisi collettivi o individuali).

Le attività sull'uso del servizio di accesso ad Internet vengono automaticamente registrate in forma elettronica attraverso i c.d. "log di sistema". Questi sistemi software sono programmati e configurati in modo da cancellare periodicamente e automaticamente, attraverso procedure di sovrascrittura dei log file, i dati personali relativi agli accessi ad Internet e al traffico telematico, la cui conservazione non sia più necessaria.

Oltre che per motivi di sicurezza del sistema informatico, anche per motivi tecnici e/o manutentivi (ad esempio, aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, etc.) o per finalità di controllo e programmazione dei costi aziendali (ad esempio, verifica costi di connessione ad internet), comunque estranei a qualsiasi finalità di controllo dell'attività lavorativa, è facoltà dell'Ente, tramite il personale del Servizio IT o addetti alla manutenzione, accedere direttamente, nel rispetto della normativa sulla privacy, a tutti gli strumenti informatici aziendali ed ai documenti ivi contenuti, nonché alle caselle email.

4.3. Violazioni e sanzioni disciplinari

È fatto obbligo a tutti gli utenti di osservare le disposizioni portate a conoscenza con il presente Regolamento. Il mancato rispetto o la violazione delle regole sopra ricordate è perseguibile nei confronti del personale dipendente con i provvedimenti disciplinari previsti dalla normativa vigente e dai regolamenti interni, nonché con le azioni civili e penali previste dalla normativa di riferimento.
L'amministratore di sistema e il personale del Servizio IT, qualora ne vengano a conoscenza, sono **obbligati** a segnalare l'inosservanza delle presenti norme in modo da dar seguito alle opportune sanzioni disciplinari.

4.4. Gestione credenziali di livello amministrativo.

Le credenziali di amministratore di tutti i server in gestione all'Unione Terre e Fiumi verranno mantenute segrete ed utilizzate solo ed esclusivamente in caso di emergenza. Pertanto saranno note solo all'Amministratore di Sistema e al personale da esso autorizzato.
Al momento dell'entrata in vigore del presente regolamento, tutte le credenziali di amministratore verranno cambiate.
Il personale del Servizio IT, sempre su autorizzazione dell'Amministratore di Sistema, sarà dotato di credenziali personali di livello amministrativo, relativamente alle proprie competenze. A titolo esemplificativo, ma non esaustivo, tutti gli accessi ai server saranno fatti con il proprio nome e quindi tracciati.
Nei casi in cui servissero credenziali amministrative generiche con password non rinnovata periodicamente, queste saranno gestite dal Servizio IT.

Le credenziali di amministratore di tutti i gestionali di ciascun Comune membro dell'Unione possono essere gestite dal servizio IT dell'Unione con le stesse modalità, solo tramite conferimento da parte dei Comuni stessi.
Un esempio pratico possono essere le credenziali di amministratore del sistema di gestione del protocollo. In caso di autorizzazione queste possono essere detenute dal Servizio IT dell'Unione per situazioni di emergenza. Tali credenziali, se gestite dal servizio IT, saranno mantenute segrete e non verranno comunicate ad alcun dipendente o collaboratore. Inoltre, sempre a seguito di autorizzazione, potranno essere create delle credenziali amministrative per il personale del Servizio IT
Nessun dipendente o collaboratore deve accedere a qualunque gestionale con credenziali amministrative generiche (del tipo admin e password) in quanto si perderebbe ogni forma di tracciabilità. Al contrario possono essere individuati ufficialmente utenti che potranno avere privilegi amministrativi . Queste scelte rimangono in capo a ciascun Ente membro dell'Unione Terre e Fiumi.

Eventuali situazioni non corrette verranno sanate con l'entrata in vigore del presente regolamento.

5. Richieste

5.1. Richieste hardware

Tutte le richieste di acquisto di materiale informatico (esempio computer, monitor, switch) sono da considerarsi acquisti da effettuarsi da parte dell'Ente in conto capitale, con successivo rimborso da parte dei Comuni membri, all'Unione. E' pertanto necessario che la spesa venga opportunamente prevista, se approvata dal dirigente del servizio IT, in fase di previsione di bilancio. Di conseguenza, le richieste pervenute dopo il 30/09 dell'anno in corso, non saranno contemplate negli acquisti dell'anno successivo.

Eventuali acquisti non preventivati di materiale di consumo e pezzi di ricambio possono essere fatte nel bilancio ordinario, compatibilmente con la disponibilità del rispettivo capitolo di spesa.

5.2. Richieste software

Il Servizio IT dell'Unione Terre e Fiumi, su indicazione della Giunta, in ambito software opera con l'obiettivo dell'unificazione dei gestionali per motivi tecnici, organizzativi ed economici. Il principio applicato è quello della necessità di dotarsi di un opportuno strumento software per tutti gli Enti membri dell'Unione. Richieste da parte del singolo Ente o Servizio, verranno sempre valutate nell'ottica dell'utilità generale. Di conseguenza tutte le personalizzazioni specifiche, rimarranno in carico al singolo Ente. Qualora, nell'interesse dell'Unione e dei Comuni membri, sia necessaria l'acquisizione di una licenza software il relativo acquisto verrà fatto in conto capitale con rimborso delle relative quote da parte dei singoli Enti all'Unione. Le richieste dovranno essere fatte entro il 30/09 dell'anno in corso per potere prevedere l'eventuale spesa nel bilancio dell'anno successivo.

5.3. Richieste di assistenza informatica

Qualunque richiesta di assistenza informatica deve essere fatta aprendo un ticket al Servizio IT inviando una semplice mail al seguente indirizzo:
assistenza@unioneterrefiumi.fe.it
Il sistema risponderà automaticamente con una mail, comunicando il numero di ticket associato e tramite il link indicato sarà possibile seguire lo stato di avanzamento della segnalazione. L'accesso avverrà indicando il proprio indirizzo mail e la password. Qualora sia stata smarrita va richiesta direttamente dalla pagina di login cliccando su "Hai dimenticato la password ?".

In caso di assoluta emergenza (esempio mancanza della connettività, blocco del pc con impossibilità di procedere con le attività lavorative) è possibile chiamare i seguenti numeri telefonici:
0532 864 678
0532 864 671
335 66 77 275
Il ticket andrà comunque aperto in un secondo momento.

I ticket verranno presi in carico in base alla gravità e all'ordine con cui sono stati inseriti.

Le seguenti richieste vanno fatte tramite apposita modulistica disponibile sul sito intranet aziendale, firmata da parte di un responsabile:

- **Richiesta nuova mail**
- **Richiesta chiusura mail**
- **Richiesta accesso rete wifi**
- **Richiesta accesso alla rete via VPN**
- **Richiesta fornitura materiale hardware**
- **Richiesta attivazione utente di dominio**
- **Richiesta abilitazione procedure**
- **Richiesta disabilitazione utente.**

Tale elenco sarà aggiornato ogni qualvolta se ne presenti la necessità.

6. Wifi

Ove disponibile, la rete wi-fi, dell'Unione o dei Comuni membri, è assolutamente equivalente a quella fornita tramite cavo ethernet. Valgono pertanto tutte le disposizioni precedenti.
L'accesso alla rete wi-fi avverrà tramite credenziali fornite su richiesta di un responsabile. La richiesta dovrà indicare con quale dispositivo **aziendale** si intende collegarsi alla rete wi-fi, in modo da escludere tutti gli apparati non censiti. Sono comunque esclusi gli smartphone anche se aziendali, per questioni di sicurezza.

Ove disponibili sono utilizzabili liberamente le reti wi-fi denominate Wisper (con credenziali Federa) e EmiliaRomagnaWifi. A tal proposito, al momento della stesura del presente regolamento, si è in attesa di concordare una convezione con Lepida spa per l'utilizzo di tale rete anche tramite access point non forniti da Lepida stessa.

7. Assistenza remota da parte di ditte esterne

Il collegamento telematico di ditte esterne per qualunque tipo di assistenza deve essere preventivamente autorizzato dal Servizio IT, tramite compilazione da parte della ditta dell'apposita modulistica. L'elenco delle ditte autorizzate sarà disponibile sulla pagina intranet.