REGOLAMENTO PER L'UTILIZZO DEGLI STRUMENTI INFORMATICI

Titolo documento: **Regolamento per l'utilizzo degli strumenti informatici**			
Tipo documento: **Disciplinare**	Codice documento:	Versione: **1.0**	Data di emissione: **04/12/2025**
Redatto da:	Sistema Informativo Innovazione Tecnologica e Statistica		
Approvato da:	Giunta dell'Unione Valdera		

INDICE

Premesse e termini utilizzati

L'Unione Valdera e i Comuni aderenti mettono a disposizione del proprio personale, per il corretto svolgimento dell'attività lavorativa, le necessarie risorse informatiche, telematiche, elettroniche e telefoniche quali sistemi di rete e di archiviazione, sistemi applicativi, personal computer e in alcuni casi smartphone e tablet (con possibilità di navigazione in Internet, utilizzo della posta elettronica, ecc.), stampanti e altro.

Al fine di eliminare o quantomeno ridurre i rischi derivanti da un uso poco corretto o poco consapevole delle risorse messe a disposizione, dando per acquisito che l'utilizzo di qualsiasi strumento di lavoro deve sempre ispirarsi ai principi di diligenza e correttezza impliciti nell'ambito del rapporto di lavoro, vengono impartite a tutti gli utenti che utilizzano dette risorse (siano essi dipendenti, amministratori, collaboratori, consulenti, dipendenti di enti o aziende esterne legate da contratti di fornitura di servizi o altri individui a cui ne è concesso l'uso) le modalità e le condizioni di utilizzo per evitare di esporre l'Ente a problematiche di sicurezza, di immagine e patrimoniali per eventuali danni cagionati anche a terzi o alla comunità.

Oltre che per mitigare i rischi di un uso insicuro degli strumenti, questo documento si propone anche di chiarire alcuni aspetti fondamentali relativi alle modalità e alle condizioni di utilizzo delle risorse, al fine di migliorarne l'efficienza d'uso, evitare utilizzi non conformi alla destinazione delle risorse stesse e garantire tempestività nell'attività di assistenza tecnica.

È utile definire in questa premessa i termini maggiormente ricorrenti nel documento o quelle definizioni tecniche che potrebbero essere difficilmente comprensibili:

- ***Risorse informatiche***: qualsiasi combinazione di apparati tecnologici, hardware o software utilizzati dall'Ente per l'elaborazione dei dati e le comunicazioni elettroniche.
- ***Dispositivi Mobili***: cellulare, smartphone, tablet e simili.
- ***Situazione d'emergenza***: circostanza in cui la tempestività d'azione è di fondamentale importanza al fine di evitare danni significativi a cose o persone, perdita di informazioni o di prove di rilievo per l'Ente, danni economici e di immagine o l'interruzione della continuità operativa.
- ***SIIT***: la struttura che si occupa della gestione operativa delle risorse informatiche per l'Unione e per i Comuni aderenti
- ***Amministratore di sistema***: il soggetto abilitato all'amministrazione, alla gestione o alla configurazione di un sistema informatico, di una applicazione o di una banca dati.
- ***Log o File di Log***: registrazioni sequenziali e cronologiche delle operazioni effettuate da un sistema informativo, necessarie per la risoluzione di problemi ed errori; tali operazioni possono essere effettuate da un Utente oppure avvenire in modo totalmente automatizzato.
- ***Dato personale***: qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.
- ***Dati particolari***: i dati personali idonei a rivelare l'origine razziale ed etnica, convinzioni religiose, filosofiche o di altro genere, opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, dati idonei a rivelare lo stato di salute e la vita sessuale, dati genetici e biometrici.
- ***Trattamento***: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;.
- ***Titolare del trattamento***: L'Ente nel suo complesso.
- ***Responsabile del trattamento:*** la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento. Nel dettaglio si tratta principalmente di fornitori di servizi dell'Ente che, in relazione al servizio affidato, effettuano operazioni su dati personali di cui l'Ente è Titolare o Responsabile o su strumenti e risorse sui cui transino o sono conservati tali dati personali.
- ***Incaricato***: ogni persona fisica (dipendenti, collaboratori, lavoratori somministrati, stagisti o tirocinanti) autorizzata a compiere operazioni di trattamento dei dati personali dal Titolare.

- ***Utente***: ciascuna persona che, in virtù di un rapporto di qualsiasi titolo con l'Unione Valdera o altro Ente, siano autorizzati all'utilizzo delle risorse informatiche.
- ***Sistema di ticketing***: strumento utilizzato dal SIIT per le segnalazioni di malfunzionamenti, guasti o altri interventi relativi alle risorse informatiche affidate agli utenti.

1. Scopo e ambito di applicazione

Lo scopo del presente disciplinare (di seguito anche solo "Regolamento") è di definire l'ambito di applicazione, le modalità e le norme sull'utilizzo della strumentazione informatica da parte degli utenti assegnatari (dipendenti, amministratori etc.), al fine di tutelare i beni dell'Ente e i dati dei cittadini, nonché per evitare condotte inconsapevoli e/o scorrette che potrebbero esporre l'Ente a problematiche di sicurezza, di immagine e patrimoniali per eventuali danni cagionati anche a terzi o alla comunità.

L'insieme delle norme comportamentali ivi incluse è volto inoltre a conformare l'Ente ai principi di diligenza, informazione e correttezza nell'ambito dei rapporti di lavoro, con l'ulteriore finalità di prevenire eventuali comportamenti illeciti dei dipendenti, pur nel rispetto dei diritti ad essi attribuiti dall'ordinamento giuridico italiano. A tal fine, pertanto, si rileva che gli eventuali controlli ivi previsti escludono finalità di monitoraggio diretto ed intenzionale dell'attività lavorativa e sono disposti sulla base della vigente normativa, con particolare riferimento al Regolamento UE n. 2016/679 (GDPR), alla Legge n. 300/1970 (c.d. Statuto dei Lavoratori), ai provvedimenti appositamente emanati dall'Autorità Garante (si veda in particolare Provv. Lavoro: le linee guida del Garante per posta elettronica e internet. Gazzetta Ufficiale n. 58 del 10 marzo 2007), all'art. 12 del D.lgs. 7 marzo 2005, n. 82 (CAD), agli artt. 11, 11-bis e 11-ter del D.P.R. 16 aprile 2013, n. 62 (Codice di comportamento dei dipendenti pubblici).

Le norme contenute in questo regolamento si applicano, in quanto compatibili, a tutti gli utenti che utilizzano anche temporaneamente le risorse informatiche dell'Ente (a titolo di esempio si citano i dipendenti di enti o aziende esterne legate da contratti di fornitura di servizi), comprendendo oltre all'Unione Valdera anche tutti i comuni aderenti o convenzionati con la funzione informatica prevista dallo Statuto Articolo 6 comma 1 lett. g. e comma 2 lett. h. per le parti compatibili.

Il presente regolamento è redatto sulla base dei seguenti e principali riferimenti normativi:

- Codice penale, con particolare riferimento ai reati informatici;
- L. 300/1970 (Statuto dei lavoratori) - artt. 4, 7 e 8;
- D. Lgs. 196/2003 e s.m.i. (Codice in materia di protezione dei dati personali);
- D. Lgs. 82/2005 e s.m.i. (Codice dell'amministrazione digitale);
- Provvedimenti del Garante per la protezione dei dati personali applicabili al contesto oggetto del presente documento, fra cui le "Linee guida per la posta elettronica e Internet" di cui alla deliberazione 13/2007;
- D. Lgs. 81/2008 e s.m.i. (Testo Unico sulla sicurezza);
- D.P.R 62/2013 (Codice di comportamento dei dipendenti della pubblica amministrazione) e Codice di comportamento approvato dall'Unione Valdera;
- Regolamento (UE) 2016/679 (General Data Protection Regulation)

2. Principi generali

Le risorse informatiche sono assegnate agli utenti per lo svolgimento dell'attività lavorativa e devono essere utilizzati con modalità e mediante comportamenti adeguati ai compiti loro assegnati e alle responsabilità connesse, nel rispetto del Codice di comportamento dei dipendenti della Pubblica Amministrazione e delle normative e direttive interne.

Nell'esecuzione delle proprie attività gli utenti sono tenuti ad attenersi alle seguenti istruzioni generali:

- Effettuare la propria attività uniformandosi alle disposizioni e alle istruzioni ricevute;
- Custodire con diligenza le risorse informatiche loro affidate, segnalando tempestivamente alle strutture preposte, secondo le modalità previste, ogni danneggiamento, smarrimento o furto;
- Mantenere la riservatezza sulle informazioni e sui dati personali di cui siano venuti a conoscenza durante lo svolgimento delle proprie attività;

- In caso di cessazione dal servizio o dal rapporto di collaborazione, astenersi dalla diffusione di informazioni, dati e documenti acquisiti durante lo svolgimento della propria attività;
- Adottare ogni misura di sicurezza idonea a scongiurare rischi di perdita o distruzione (anche accidentale) dei dati;
- Garantire la corretta custodia di atti e documenti relativi alla propria attività.

3. Gestione delle credenziali di autenticazione

3.1 Le credenziali di autenticazione per l'accesso alle risorse informatiche, alla rete e ai programmi vengono assegnate dal SIIT o dall'Amministratore di Sistema, previa formale richiesta del responsabile dell'Unità Organizzativa. Ove possibile saranno privilegiati sistemi a più fattori di autenticazione.

3.2 Le password devono rispettare i seguenti criteri di complessità:

- non contenere nomi o username dell'utente o parte di essi
- essere lunghe almeno 8 caratteri
- contenere caratteri da almeno tre delle categorie seguenti:
  - Lettere maiuscole
  - Lettere minuscole
  - cifre numeriche (da 0 a 9)
  - Caratteri speciali: (~! @ # $% ^& * -+ =' | \ \ (){}\ []:; "' <>,.? /)
- devono essere diverse da quelle precedentemente utilizzate

3.3 Al primo accesso al sistema l'utente sarà obbligato alla modifica della password assegnata in modo temporaneo e, successivamente, si dovrà procedere al cambio password almeno ogni 180 giorni. Il sistema comunque avvertirà l'utente della necessità di procedere a tale modifica con 14 giorni di anticipo rispetto alla scadenza fissata.

3.4 In caso di molteplici tentativi falliti di inserimento della password l'utenza verrà bloccata, e sarà quindi necessario contattare il SIIT per procedere allo sblocco della stessa.

3.5 Le credenziali di autenticazione sono strettamente personali e non devono essere comunicate né rese disponibili ad altri soggetti, salvo i casi specifici in cui per esigenze tecniche e/o organizzative siano stabilite credenziali condivise. In caso di diffusione accidentale, anche solo presunta, la password deve essere immediatamente modificata e l'incidente va immediatamente segnalato al SIIT.

3.6 Qualora l'utente dimentichi la password o venga a conoscenza di quella di altro utente, è tenuto a darne immediata notizia al SIIT o all'Amministratore di Sistema, che procederanno al ripristino della stessa.

3.7 Le password personali non devono mai esser salvate sul PC o in rete in file di testo (o simili) non protetti, possono invece essere utilizzati sistemi di salvataggio protetti da credenziali di autenticazione che fanno capo ai sistemi autorizzati all'interno dell'Ente. Si raccomanda di non utilizzare la stessa parola chiave per sistemi di autenticazione interni al dominio di rete e per sistemi di autenticazione esterni, come ad esempio la registrazione a siti o servizi Web, o a quella utilizzata per l'accesso alla propria posta elettronica privata o a qualunque altro accesso non pertinente alle attività lavorative.

4. Autenticazione a più fattori (MFA)

4.1 In alcuni contesti sarà possibile attivare l'autenticazione a più fattori, che comporta l'utilizzo di un "fattore" aggiuntivo rispetto all'utilizzo della sola password; tali fattori aggiuntivi possono essere: One-Time-Password (OTP), chiamata telefonica o SMS.

4.2 Essendo le credenziali di autenticazione strettamente personali per tale sistema potrà essere utilizzato anche un dispositivo personale (smartphone) e quindi non assegnato dall'Amministrazione in modo tale da consentire l'accesso alle risorse anche in caso di lavoro da remoto.

5. Utilizzo delle risorse informatiche

5.1 L'utilizzo delle risorse informatiche è riservato agli utenti espressamente autorizzati dall'Ente, sulla base dei requisiti operativi e dei requisiti di sicurezza dei sistemi informativi e di rete. È vietato qualsiasi utilizzo che deturpi o rovini le risorse assegnate. Si ricorda che le risorse informatiche sono strumenti di lavoro appartenenti al patrimonio dell'Ente e pertanto vanno custoditi in modo appropriato; il furto, il danneggiamento o lo smarrimento

di tali strumenti debbono essere prontamente segnalati al SIIT, inoltre in caso di furto o smarrimento dovrà essere presentata regolare denuncia alle autorità competenti.

5.2 Tutti i computer, i dispositivi, gli apparati di rete e le applicazioni sono protetti da credenziali di autenticazione assegnate a ciascun utente. L'abilitazione all'accesso alla rete, a specifiche cartelle di memorizzazione sui server o ambienti cloud, a specifiche applicazioni necessarie per ciascun utente, vanno richieste al proprio responsabile di ufficio/area che dovrà provvedere ad inoltrare la richiesta al SIIT.

5.3 I diritti di accesso sono attribuiti sulla base dei principi della "necessità di sapere", del privilegio minimo e della separazione delle funzioni; tutti i responsabili di ufficio/area sono invitati a comunicare prontamente al SIIT o all'Amministratore di Sistema, tramite il servizio di ticketing dedicato, qualsiasi modifica relativa all'organico o all'assegnazione di compiti e mansioni operative che richieda l'attivazione o la sospensione di servizi informatici o autorizzazioni all'accesso a risorse o banche dati, in modo da poter garantire che i diritti di accesso siano modificati di conseguenza.

5.4 Le risorse informatiche affidate all'utente sono strumenti di lavoro e come tali possono essere utilizzate solo per scopi strettamente professionali, salvo nei casi espressamente previsti, in relazione alle mansioni assegnate. Ciò vale sia per le risorse condivise (risorse di rete, stampanti di rete, risorse di memorizzazione cloud, applicazioni, ecc.), sia per quelle affidate al singolo dipendente (smartphone, personal computer, periferiche, stampanti locali, ecc.). Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.

5.5 Al dipendente è comunque consentito l'utilizzo degli strumenti informatici forniti dall'Amministrazione per poter assolvere ad incombenze personali, sempre nel rispetto della correttezza e buona fede, senza doversi allontanare dalla sede di servizio, purché l'attività sia contenuta in tempi ristretti e senza alcun pregiudizio per i compiti istituzionali.

6. Utilizzo dei personal computer

6.1 L'accesso al computer è protetto da credenziali che devono essere custodite dall'utente con la massima diligenza e non divulgate per nessun motivo.

6.2 Non è consentito all'utente modificare le caratteristiche e le impostazioni del proprio personal computer, salvo previa autorizzazione esplicita del SIIT.

6.3 Non è consentito salvare sui dispositivi assegnati file personali non connessi all'attività lavorativa.

6.4 Non è consentito installare autonomamente programmi, in quanto sussiste il grave pericolo di introdurre virus informatici e di alterare la stabilità delle applicazioni dell'elaboratore e/o dell'intera rete.

6.5 Non è consentito l'uso di programmi diversi da quelli autorizzati e distribuiti ufficialmente dall'Ente riportati nel documento "Elenco software autorizzati" adottato nel rispetto dell'art. 29 del presente regolamento. L'inosservanza di questa disposizione, infatti, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre l'Ente a gravi responsabilità civili ed anche penali in caso di violazione della normativa a tutela dei diritti d'autore sul software (L. 633/41 e successive modifiche; D.lgs. 518/92 sulla tutela giuridica del software; L. 248/2000, nuove norme di tutela del diritto d'autore; L. 128/2004 e successive modifiche) che impone la presenza nel sistema di software regolarmente licenziato o comunque non protetto dal diritto d'autore.

6.6 Qualora si renda necessario per l'attività lavorativa utilizzare, e quindi installare, nuovi applicativi sulle postazioni di lavoro, si dovrà contattare il SIIT che provvederà a verificarne la sicurezza e la compatibilità con i sistemi esistenti nonché, in caso di esito positivo delle verifiche, all'inserimento dell'applicativo nell'elenco dei software approvati e quindi alla conseguente installazione.

6.7 Non è consentito l'utilizzo e l'installazione sul proprio PC di alcun dispositivo di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, hard disk, memorie USB, modem per le comunicazioni), se non con l'autorizzazione espressa del SIIT.

6.8 Il personal computer non deve essere lasciato incustodito e con la sessione di lavoro attiva. In caso di allontanamento dalla postazione di lavoro l'utente deve attivare il blocco della sessione. Per questioni di sicurezza è comunque attiva una impostazione di sistema che blocca la sessione dell'utente dopo 15 minuti di inattività.

6.9 L'utente è responsabile del computer portatile eventualmente assegnatogli, sia in via temporanea che definitiva, e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo per lo svolgimento delle attività lavorative. Ai computer portatili si applicano le stesse regole di utilizzo previste per i computer fissi connessi in

rete. Particolare attenzione deve essere posta alla rimozione e/o salvataggio di eventuali file elaborati sullo stesso prima della riconsegna.

6.10 L'utente è tenuto a spengere la propria postazione di lavoro al termine della giornata lavorativa, con l'eccezione dell'utilizzo della postazione quando l'Utente debba effettuare attività di lavoro da remoto.

6.11 I documenti di lavoro devono essere conservati nelle cartelle preposte del proprio profilo utente (Desktop e Documenti), queste cartelle possono essere soggette a backup e/o a sincronizzazione con le risorse cloud personali. Costituisce comunque buona regola il periodico salvataggio dei documenti di lavoro sulle risorse cloud dell'ufficio e/o sulle risorse di rete, poiché in caso di malfunzionamenti gravi delle postazioni di lavoro i dati contenuti in esse potrebbero non essere recuperabili, con la perdita definitiva delle informazioni. Particolare attenzione deve essere prestata alla duplicazione dei dati e dei documenti, con il consiglio di effettuare una pulizia periodica degli stessi.

6.12 Per prevenire eventuali accessi non autorizzati ai documenti, oltre che per motivi relativi allo spazio disco dei personal computer, saranno cancellati periodicamente i profili utente non utilizzati da almeno 6 mesi.

7. Utilizzo della rete

7.1 Hanno diritto ad accedere alla rete dell'Ente tutti gli utenti autorizzati dall'Amministrazione. L'accesso alla rete è assicurato compatibilmente con le potenzialità delle attrezzature. Il SIIT o l'Amministratore di Sistema può limitare l'accesso alla rete di determinate categorie di utenti, quando ciò sia richiesto da ragioni tecniche.

7.2 L'utente che ottiene l'accesso alla rete e agli applicativi si impegna ad osservare le indicazioni presenti in questo documento e le eventuali altre norme disciplinanti le attività e i servizi che si svolgono via rete e si impegna a non commettere abusi e a non violare i diritti degli altri utenti e dei terzi.

7.3 L'utente che ottiene l'accesso alla rete e agli applicativi si assume inoltre la totale responsabilità delle attività che svolge tramite la rete.

7.4 Tutti i file, anche temporanei, che si riferiscono all'attività lavorativa e per i quali vi è la necessità di un salvataggio ai fini di garantirne la costante disponibilità, dovranno essere memorizzati sulle unità di rete e cloud appositamente predisposte. Tale disposizione vale in modo particolare per i documenti contenenti dati personali per i quali, per obbligo di legge, va garantito un salvataggio costante.

7.5 Le unità di rete e i sistemi di memorizzazione in cloud sono aree di condivisione di informazioni strettamente professionali e non devono in alcun modo essere utilizzate per scopi diversi. Pertanto, qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità sulle quali vengono svolte regolari attività di amministrazione, controllo e backup.

7.6 Costituisce buona regola la periodica pulizia degli archivi informatici di rete e sulle risorse cloud, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati e dei documenti.

8. Servizi Cloud

8.1 È vietato utilizzare di propria iniziativa qualsiasi servizio di cloud pubblico, a titolo puramente esemplificativo e non esaustivo, Google Drive, Apple iCloud, Dropbox, Microsoft OneDrive, WeTransfer e simili, che prevedano la memorizzazione e/o lo scambio, anche solo temporaneo, di dati e documenti di proprietà dell'Amministrazione, ed in particolare che contengano dati personali facendoli transitare da sistemi informatici e spazi di memorizzazione dati di proprietà di terzi.

8.2 È fatto salvo l'utilizzo di servizi del cloud pubblico specificatamente autorizzati dall'Amministrazione, come specificato nel documento "Elenco dei servizi Cloud autorizzati" adottato nel rispetto dell'art. 29 del presente regolamento, purché ciò avvenga secondo le indicazioni e le modalità specificatamente indicate da parte del servizio SIIT.

8.3 Ove si renda necessario accedere ad un servizio di cloud pubblico per vincoli imposti dall'esterno, l'utente deve preventivamente ricevere autorizzazione da parte del servizio SIIT e seguire le indicazioni ed istruzioni di sicurezza eventualmente indicate da quest'ultimo. È comunque necessario, ove tale utilizzo si svolga nell'ambito di trattamenti di dati personali, che sia garantito il rispetto del GDPR.

9. Accesso ai file su PC, dispositivi mobili e cartelle di rete

9.1 L'accesso alle applicazioni e ai file contenuti nei personal computer desktop e portatili, nei mobile device, nelle cartelle di rete presenti sui server e sui sistemi cloud dell'Ente è regolato da disposizioni e sistemi di autorizzazione

studiati in base alle specifiche esigenze delle Amministrazioni. La richiesta di abilitazione all'accesso agli applicativi e alle cartelle di rete o sul cloud va rivolta al proprio Responsabile di Ufficio/Area che farà richiesta al SIIT tramite il sistema di ticketing interno.

9.2 In caso di assenze prolungate o in situazioni di emergenza, alla persona che sostituisce nella funzione il dipendente assente possono essere assegnati diritti di autorizzazione tali da potere accedere a tutti gli applicativi e ai file necessari allo svolgimento della propria mansione presenti sulle cartelle di rete o in cloud. La richiesta di abilitazione all'accesso agli applicativi e alle cartelle di rete o sul cloud dovrà essere inoltrata attraverso il sistema di ticketing interno dal Responsabile di Ufficio/Area.

9.3 In caso di cessazione del rapporto di lavoro, alla persona che sostituisce nella funzione il dipendente cessato, vengono assegnati diritti di autorizzazione tali da potere accedere a tutti gli applicativi e ai file necessari allo svolgimento della propria mansione presenti sulle cartelle di rete o in cloud. Al personale che si appresta a concludere il rapporto di lavoro non è permesso cancellare file di interesse dell'Amministrazione sulle unità di rete o sul cloud.

10. Utilizzo di dispositivi personali per lo svolgimento delle attività lavorative (BYOD)

10.1 È consentito all'utente l'utilizzo del proprio dispositivo personale per l'accesso alle risorse locali dell'Ente solo dopo espressa autorizzazione da parte del SIIT.

10.2 L'autorizzazione avviene a seguito di verifica dei dispositivi personali dell'utente e delle autorizzazioni ai dati ai quali si dovrà accedere. Ove possibile saranno creati comunque ambienti ad-hoc per suddividere le attività lavorative da quelle personali

10.3 Sono esclusi dal processo autorizzativo i dispositivi utilizzati per la generazione della OTP, relativi all'accesso MFA, per l'accesso alle risorse in cloud autorizzate e i dispositivi utilizzati per l'accesso in smart working tramite portale web.

11. Posta elettronica

11.1 La casella di posta elettronica assegnata dall'Amministrazione all'utente è uno strumento di lavoro e rappresenta uno strumento di comunicazione fondamentale nei rapporti interni dell'Ente, nei rapporti con altre amministrazioni e nei rapporti con il cittadino, anche per la trasmissione di documenti, come previsto dall'art 47 del Decreto Legislativo 7 marzo 2005, n. 82 (Codice dell'Amministrazione Digitale) e dall'articolo 43 del D.P.R. n. 445/2000.

11.2 Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

11.3 È fatto divieto di utilizzare le caselle di posta elettronica dell'Amministrazione per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mailing-list salvo diversa ed esplicita autorizzazione del Responsabile dell'Unità Organizzativa. È vietato partecipare a catene telematiche (o di Sant'Antonio). Non si devono in alcun caso aprire gli allegati di tali messaggi.

11.4 Ogni utente deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico mediante virus o altro software dannoso. In particolare, l'utente deve:

- limitare allo stretto necessario lo scambio fra computer di file con estensione: exe, dll, zip, com, bat, chm, cmd, cpl, hlp, hta, inf, lnk, ocx, pif, reg, scr, url, vbs, rar;
- non aprire gli allegati di posta se non si è certi della loro provenienza;
- non cliccare mai un link presente in un messaggio di posta elettronica di provenienza sconosciuta o dubbia;
- non cliccare mai, durante la navigazione Internet, su banner o link pubblicitari non necessari per l'attività lavorativa.

11.5 La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti. È obbligatorio controllare gli allegati ai messaggi di posta elettronica prima del loro utilizzo.

11.6 Nelle normali e-mail la ricevuta di ritorno per avere la conferma dell'avvenuta ricezione/lettura dei messaggi da parte del destinatario può non essere abilitata, pertanto, per le comunicazioni ufficiali è obbligatorio avvalersi di strumenti adatti, quali la casella di Posta Elettronica Certificata.

11.7 Le comunicazioni che contengono messaggi di cui è necessaria la conservazione o tali da impegnare giuridicamente l'Amministrazione verso l'esterno devono essere registrati sul protocollo dell'Ente.

11.8 Non è consentito il reindirizzamento automatico dei messaggi ricevuti sulle caselle di posta elettronica fornite dall'Amministrazione verso caselle e-mail esterne a quelle fornite dall'Ente, salvo che ciò sia necessario per l'assolvimento di compiti istituzionali e comunque dopo specifica autorizzazione. In caso si rilevassero configurazioni in contrasto il servizio SIIT provvederà alla rimozione dell'anomalia e alla successiva comunicazione all'Utente della modifica effettuata.

11.9 Si precisa che le caselle di posta elettronica non sono da considerarsi archivi ed il contenuto deve essere considerato esclusivamente temporaneo e non destinato alla conservazione nel tempo. L'archiviazione di documenti digitali nel tempo può avvenire esclusivamente mediante gli appositi applicativi e nel rispetto, ove necessario, delle norme del D.lgs. 82/2005 (CAD) in merito all'archiviazione sostituiva.

11.10 Sono presenti sistemi automatici di controllo al fine di prevenire la diffusione di posta contenente malware, phishing e spam o comunque del corretto funzionamento del sistema.

12. Tipologia di caselle di posta elettronica

12.1 Le caselle di posta elettronica messe a disposizione dall'Amministrazione possono essere di tre tipi:

- Personale: è la casella di posta elettronica nominale assegnata direttamente all'utente per lo svolgimento delle normali attività lavorative, questa casella di posta elettronica è accessibile unicamente all'assegnatario e non può essere accessibile da altri;
- Lista di distribuzione: è una casella di posta elettronica che reindirizza, e quindi non ha un archivio dedicato, la posta in arrivo verso le caselle di posta elettronica personali degli utenti che fanno parte di questa lista;
- Condivisa: questa tipologia di casella di posta elettronica viene assegnata ad uno specifico servizio/ufficio o ad una specifica funzione, o per casi particolari a seguito di richiesta specifica dell'Ente. Nello specifico le caselle condivise assegnate al servizio/ufficio devono essere considerate come le caselle principali di comunicazione istituzionale, le caselle condivise di funzione (es. sindaco, segretario, presidente) sono caselle che possono essere istituite per separare la corrispondenza istituzionale relativa alla funzione da quella della casella personale assegnata.

13. Gestione della posta elettronica del personale assente o cessato

13.1 La casella di posta elettronica è uno strumento che può contenere informazioni utili per l'attività dell'Amministrazione, pertanto, in caso di assenze prolungate o per urgenti necessità l'Ente potrà richiedere l'impostazione di un messaggio automatico di "fuori ufficio", in modo da segnalare l'assenza della persona incaricata. Ove possibile, nel messaggio sarà segnalato anche il periodo dell'assenza e, se necessario, un indirizzo di posta alternativa a cui inviare il messaggio.

13.2 La casella di posta elettronica del dipendente personale che cessa il rapporto di lavoro viene disabilitata all'invio dei messaggi. Viene contestualmente impostato, su richiesta del dipendente o dell'amministrazione, un messaggio di risposta automatico che segnali la prossima cessazione della casella e l'indicazione di un indirizzo di posta alternativo a cui inviare il messaggio, tale messaggio di risposta sarò attivo per un tempo non superiore ai 30 giorni, passato tale tempo la casella di posta elettronica sarà eliminata definitivamente.

13.3 La casella di posta elettronica del dipendente personale cessato non può in alcun caso essere messa a disposizione di altri utenti o del Responsabile dell'Unità Organizzativa, dovrà essere cura del dipendente stesso trasferire eventuali mail di interesse dell'ufficio verso altri dipendenti o verso la mail condivisa assegnata all'ufficio.

14. Intranet Aziendale

14.1 L'Unione Valdera dispone di uno spazio informativo, denominato "intranet", visualizzabile a tutti gli utenti del sistema informativo.

14.2 La intranet è accessibile previa autenticazione utilizzando le stesse credenziali della posta elettronica.

14.3 Sulla intranet sono presenti collegamenti e documenti utili allo svolgimento delle attività lavorative.

14.4 Le notizie pubblicate possono essere di carattere generale oppure indirizzate ad uno specifico gruppo di utenti.

14.5 La intranet deve essere considerata il canale ufficiale per veicolare le informazioni verso tutti gli utenti interni dell'Unione Valdera e degli Enti che la compongono.

15. Uso della rete internet e dei relativi servizi

15.1 Il PC e gli altri dispositivi abilitati alla navigazione in Internet costituiscono strumento necessario allo svolgimento della propria attività lavorativa.

15.2 Non è consentito lo scaricamento né l'esecuzione online di file musicali, video o multimediali; non è consentita la connessione a siti musicali o l'ascolto in linea di musica, notizie, radio o altro o il download di brani musicali: tali pratiche possono essere causa di sovraccarico della rete e ne limitano l'utilizzo per fini lavorativi; analogo problema comporta l'accesso a filmati e webcam, salvo naturalmente i casi direttamente attinenti all'attività lavorativa.

15.3 È fatto divieto assoluto per gli utenti di connettersi autonomamente alla rete Internet attraverso il tethering del proprio cellulare o utilizzare chiavette o router portatili, salvo per i computer portatili e per i dispositivi mobili o comunque quando espressamente consentito dal SIIT.

15.4 È da evitare ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa. È vietata tramite gli strumenti messi a disposizione dall'Amministrazione la partecipazione a forum non professionali, la partecipazione personale a social network, l'utilizzo di chat line non autorizzate, di bacheche elettroniche o l'inserimento di commenti online, anche utilizzando pseudonimi (o nickname).

15.5 Al fine di controllare che la navigazione Internet avvenga verso siti utili all'attività lavorativa e per impedire l'accesso a quelli ritenuti pericolosi (siti di pedofilia, pornografia, terrorismo e altro), potranno essere utilizzati degli strumenti per selezionare e limitare gli accessi ad alcune tipologie di siti o impedire l'esecuzione o lo scaricamento di alcune tipologie di file. In caso il sistema di filtro blocchi erroneamente un sito o una risorsa online necessaria all'attività lavorativa, è possibile richiederne l'accesso tramite il servizio di ticketing interno.

15.6 I sistemi informatici e le procedure software preposte al funzionamento del sistema di accesso a Internet producono, nel corso del loro normale esercizio, alcuni dati la cui trasmissione è implicita nell'uso dei protocolli di comunicazione di Internet (file di log). Si tratta di informazioni che per loro stessa natura permetterebbero, attraverso elaborazioni ed associazioni, di identificare le attività degli utenti. In questa categoria di dati rientrano, ad esempio, gli indirizzi dei siti visitati, l'orario della visita, la tipologia di file visualizzato. Il trattamento di tali file di log è ispirato ai principi di pertinenza e non eccedenza e ne è prevista la conservazione per 21 giorni. In presenza di gravi anomalie o problemi tecnici dovuti al comportamento degli utenti, si procederà alla loro conservazione per un periodo di tempo maggiore controllando, in prima battuta e quando possibile, i dati in forma aggregata, riferiti all'intera struttura lavorativa o a sue aree. Tale controllo si concluderà preferibilmente con l'applicazione di filtri o limitazioni per tutti o per gruppi omogenei di utenti, con un avviso generalizzato relativo ad un rilevato utilizzo anomalo degli strumenti informatici e con l'invito generale ad attenersi scrupolosamente a compiti assegnati e alle istruzioni impartite. L'avviso potrà essere circoscritto a dipendenti afferenti all'area o settore in cui è stata rilevata l'anomalia. Se a seguito di tali provvedimenti le gravi anomalie dovessero ripetersi, si procederà con controlli su base individuale.

16. Servizio Wi-Fi

16.1 Nei locali dell'Amministrazione possono essere realizzate infrastrutture Wi-Fi sia ad accesso pubblico, e quindi scollegate dalle risorse interne dell'Ente, che per l'esclusivo utilizzo per scopi di servizio.

16.2 Per le reti ad accesso pubblico le regole di utilizzo sono stabilite dal fornitore del servizio individuato.

16.3 Per le reti predisposte per scopi di servizio le regole di utilizzo sono stabilite dal servizio SIIT

16.4 È fatto divieto agli Utenti, ed è considerata grave violazione della sicurezza dell'infrastruttura telematica dell'Amministrazione, la realizzazione di infrastrutture Wi-Fi diverse da quelle realizzate dalla stessa Amministrazione.

16.5 È vietato realizzare infrastrutture di rete personali che consentano la condivisione dei dati accessibili dai propri dispositivi in dotazione (es.: tethering, bluetooth) se non espressamente autorizzati

17. Lavoro da remoto (smart working)

17.1 Sarà possibile svolgere il lavoro da remoto mediante l'utilizzo di una connessione sicura all'infrastruttura telematica dell'Amministrazione, tale connessione potrà avvenire:

- in caso di utilizzo di dispositivi di proprietà dell'Amministrazione attraverso l'utilizzo di VPN (Virtual Private Network) protette da cifratura SSL,

– in caso di utilizzo di un dispositivo di proprietà del dipendente sarà invece utilizzata una modalità di lavoro che consente tramite l'accesso ad un portale web cifrato esclusivamente l'accesso al desktop del computer fisso connesso alla rete dell'ufficio per lo svolgimento del proprio lavoro.

17.2 Per la connessione da remoto potrà essere utilizzata qualunque tipo di connessione fissa o mobile, privata del dipendente o messa a disposizione dall'Amministrazione, purché di caratteristiche adeguate all'utilizzo di questi sistemi.

17.3 L'abilitazione per il lavoro da remoto del dipendente dovrà essere richiesta attraverso il sistema di ticketing dal Responsabile dell'Ufficio/Area e secondo le procedure proprie dell'Amministrazione, per l'attivazione della procedura sarà necessario indicativamente un giorno lavorativo. La stessa procedura deve essere adottata in caso l'utente perda il diritto di accesso a tale modalità.

17.4 Gli accessi del lavoro da remoto, per entrambe le tipologie, sono memorizzati in un file di log che consente di tenere traccia dei periodi di connessione, il traffico generato dalla normale attività di lavoro rientra invece nei normali sistemi di monitoraggio attivati dall'Ente.

18. Utilizzo di telefoni e dispositivi mobili

18.1 Quando necessario l'Amministrazione mette a disposizione, a seconda del ruolo o della funzione del singolo utente, dispositivi di telefonia fissa e/o mobile - quali smartphone e/o tablet - che consentono di usufruire del servizio di telefonia tramite rete cellulare e /o della navigazione in Internet tramite rete dati.

18.2 I dispositivi affidati all'utente sono strumenti di lavoro. Ne viene concesso l'uso esclusivamente per lo svolgimento dell'attività lavorativa e non è quindi consentito il loro uso per attività o comunicazioni a carattere personale o comunque non strettamente inerenti all'attività lavorativa stessa. La ricezione o l'effettuazione di telefonate personali è consentita solo nel caso di comprovata necessità ed urgenza, tranne per gli utenti che hanno fatto espressamente richiesta di utilizzo dei dispositivi mobili anche per uso personale.

18.3 L'utente è responsabile dell'utilizzo e della custodia dei dispositivi affidategli. Ai dispositivi di telefonia fissa e mobili si applicano le medesime regole previste per l'utilizzo dei personal computer.

18.4 I dispositivi mobili assegnati devono essere protetti da account e credenziali di autenticazione con password strutturate, come descritto nei capitoli precedenti, con codice pin o con autenticazione biometrica del dispositivo che ne impedisca l'utilizzo da parte di soggetti non autorizzati. La password o il codice pin non può essere disattivato.

18.5 L'eventuale installazione di applicazioni, sia gratuite che a pagamento, sui dispostivi non concessi anche ad uso personale deve essere espressamente autorizzata. I dispositivi assegnati possono essere connessi a sistemi MDM che ne consentono la gestione e il monitoraggio da remoto.

18.6 In caso di danneggiamento o malfunzionamento dei dispositivi assegnati, l'utente dovrà darne immediato avviso al SIIT; in caso di furto o smarrimento del dispositivo mobile in oggetto, l'utente dovrà denunciare il fatto alle autorità competenti. Ove detti eventi siano riconducibili ad un comportamento negligente o imprudente dell'utente e/o comunque a sua colpa nella custodia del bene, lo stesso potrà essere ritenuto responsabile dei danni derivanti; quindi, il SIIT provvederà alla quantificazione del danno e alla successiva comunicazione al Dirigente responsabile dell'utente coinvolto. In caso di furto o smarrimento il SIIT si riserva la facoltà di attuare, ove possibile, la procedura di remote-wipe (cancellazione da remoto di tutti i dati sul dispositivo), rendendo il dispositivo inutilizzabile e i dati in esso contenuti irrecuperabili.

18.7 I dispositivi mobili possono essere soggetti a controlli sul traffico effettuato. I controlli sul corretto utilizzo dei telefoni e degli altri dispositivi verranno effettuati in presenza di evidenti anomalie, mediante screening generale dei tabulati. Quando, a seguito dei controlli effettuati, emergano comportamenti in violazione del presente regolamento o comunque "anomali", si procederà con un avviso circoscritto a dipendenti afferenti all'area o settore in cui è stata rilevata l'anomalia. Se a seguito di tali provvedimenti le anomalie dovessero ripetersi, si procederà con controlli su base individuale.

18.8 Per i dispositivi di telefonia fissa, nel rispetto della normativa in materia di tutela della libertà e dignità dei lavoratori e della normativa in materia di protezione dei dati personali, sono attivi sistemi di monitoraggio delle comunicazioni che consentono di verificare mittente, destinatario (con mascheramento delle ultime cifre del numero), durata, data e stato (risposta, non risposta o rifiutata). Questi sistemi sono destinati esclusivamente all'analisi del tipo di traffico ai fini di reportistica e manutenzione e le relative informazioni, in modalità aggregata, sono accessibili ai soli amministratori dei sistemi.

19. Utilizzo di scanner, fotocopiatrici, stampanti e fax

19.1 I soggetti che, quando previsto, provvedono all'acquisizione in forma digitale della documentazione cartacea utilizzando uno scanner o strumenti analoghi, devono sempre verificare che l'operazione avvenga correttamente e che il contenuto del documento oggetto di scansione risulti leggibile; qualora vi fossero errori di acquisizione ovvero si verifichino anomalie di processo, occorrerà ripetere l'operazione.

19.2 È cura dell'utente effettuare la stampa dei documenti solo se strettamente necessaria. Le stampanti, a seconda dell'organizzazione del singolo Ente, sono dotate di sistemi che evitano di produrre le stampe senza la presenza dell'utente (stampa privata con inserimento del PIN o sistema di rilascio analogo), in mancanza di tali sistemi si deve comunque porre particolare attenzione nel non lasciare incustodite le copie, recuperando immediatamente i documenti stampati soprattutto quando questi contengono dati personali o informazioni riservate.

19.3 Eventuali fotocopie/stampe non riuscite debbono essere distrutte, in un apposito trita documenti se disponibile oppure manualmente in modo tale da non consentire la ricostruzione del contenuto. È tassativamente proibito utilizzare le fotocopie/stampe non riuscite contenenti dati personali o riservati come carta per appunti.

19.4 È vietato l'utilizzo degli apparati fax per la trasmissione o la ricezione di documenti tra Pubbliche Amministrazioni come disposto dall'Art.14 della Legge n.98/2013, è altresì vietato l'utilizzo per motivi personali o comunque non legati all'attività lavorativa.

19.5 Nell'utilizzare il fax occorre prestare particolare attenzione a digitare correttamente il numero a cui inviare la comunicazione, controllare l'esattezza del numero digitato prima di inviare la comunicazione, attendere la fine della trasmissione, verificando nel rapporto di trasmissione la corrispondenza tra il numero di pagine da inviare e quello effettivamente inviato. Qualora, per motivi legittimi, vengano trasmessi con questo mezzo dati particolari o altre informazioni riservate, può essere opportuno anticipare l'invio del fax chiamando il destinatario della comunicazione al fine di assicurarsi che il ricevimento avverrà nelle mani del medesimo, evitando che soggetti estranei o non autorizzati possano conoscere il contenuto della documentazione inviata.

20. Utilizzo e custodia dei supporti di memorizzazione rimovibili

20.1 In linea generale è vietato utilizzare cd, dvd, hard disk, penne usb o simili (di seguito identificati come "supporti di memorizzazione rimovibili") se non espressamente autorizzati ed abilitati all'utilizzo degli stessi.

20.2 È In linea generale vietata la copia su supporti di memorizzazione rimovibili di dati personali, dati particolari, informazioni su condanne penali o reati o dati riservati. Ciò premesso, ove nello svolgimento della normale attività assegnata all'utente, nell'ambito del suo profilo di autorizzazione, sia indispensabile effettuare una copia di tali dati su supporti rimovibili, occorre attenersi alle seguenti cautele:

- Tutti i supporti rimovibili 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.
- In caso di spedizione ad altro incaricato, occorre accertarsi che il destinatario abbia lo stesso profilo di autorizzazione del mittente e che il supporto rimovibile venga spedito in una busta sigillata, intestata personalmente all'incaricato, con controfirma sul lembo di chiusura. Non si deve spedire un supporto rimovibile senza aver prima concordato con il destinatario stesso le modalità e tempi di consegna ed aver stabilito la procedura che permette di confermare l'avvenuta consegna al destinatario del supporto stesso.
- Se il supporto deve contenere dati personali o particolari deve essere utilizzata la cifratura degli stessi e/o dovranno essere memorizzati in volumi protetti da password.
- L'utente è responsabile della custodia dei supporti rimovibili utilizzati e dei dati in essi contenuti. Si faccia sempre attenzione a non dimenticare il supporto all'interno del computer quando, al termine della copia, si spegne il computer e ci si allontana. Il supporto rimovibile non deve mai essere lasciato abbandonato sul tavolo, ma deve essere immediatamente posto all'interno di una custodia sicura, quando non utilizzato (in funzione della criticità dei dati archiviati, si può andare da un cassetto della scrivania chiuso a chiave, sino ad un armadio blindato od una cassaforte idonea alla custodia di supporti magnetici).

20.3 L'utente è tenuto a informare immediatamente il SIIT di qualsiasi furto o smarrimento che coinvolga i supporti di memorizzazione rimovibili in proprio possesso, fatti salvi gli obblighi di denuncia alle autorità competenti, in modo da attivare tutte le procedure necessarie in particolare in materia di privacy.

21. Strumenti di firma digitale

21.1 I responsabili di ufficio/area possono richiedere, per motivate esigenze operative, il rilascio di firma digitale per i propri collaboratori

21.2 L'utilizzo dei kit di firma digitale, anche remota, rilasciati ai dipendenti che ne hanno fatto richiesta per i fini di attività lavorativa è strettamente personale e non cedibile a terzi.

21.3 La responsabilità dell'utilizzo e della segretezza delle credenziali di tali strumenti è dell'utilizzatore finale.

21.4 In caso di reiterati episodi di dimenticanza/smarrimento delle credenziali di autenticazione alla firma digitale con conseguente revoca della precedente firma e rilascio di una nuova, ove detti eventi siano riconducibili ad un comportamento negligente o imprudente dell'utente e/o comunque a sua colpa nella custodia del bene, lo stesso potrà essere ritenuto responsabile dei danni derivanti; quindi, il SIIT provvederà alla quantificazione del danno e alla successiva comunicazione al Dirigente responsabile dell'utente coinvolto

22. Assistenza tecnica, gestione dei dispositivi e software di sicurezza

22.1 Per le operazioni di gestione, installazione e aggiornamento software e per garantire la sicurezza dei dispositivi, delle applicazioni e dei dati, il SIIT si avvale di strumenti di gestione remota ("Remote Monitoring and Management" e "Mobile Device Management") che consentono di compiere tutte le operazioni necessarie attraverso la rete locale o internet. L'assistenza tecnica per malfunzionamenti ordinari attraverso questi strumenti di gestione remota avviene di norma previa autorizzazione dell'utilizzatore e in presenza dell'utilizzatore stesso.

22.2 L'utente deve segnalare ogni richiesta, anomalia o problema alle postazioni di lavoro o dispositivo a lui assegnati utilizzando il sistema di ticketing messo a disposizione dall'Amministrazione.

22.3 Le postazioni sono dotate di strumenti di Endpoint Security gestiti ed aggiornati centralmente tramite strumenti di distribuzione automatica del software.

22.4 I software di Endpoint Security possono essere abilitati all'esecuzione automatica di policy di sicurezza in caso di rilevazioni di operazioni malevole che potrebbero portare al blocco temporaneo, parziale o totale, dell'operatività della macchina e/o dell'utente.

22.5 È vietato disattivare gli strumenti di cui ai punti precedente presenti sugli strumenti informatici, modificarne la configurazione o usare strumenti similari differenti da quelli forniti dal SIIT.

22.6 Ogni anomalia o problematica relativa a virus ed antivirus dovrà essere prontamente segnalata al SIIT. Nel caso il software antivirus rilevi la presenza di un file infetto non bonificato, l'utente potrà essere invitato a sospendere ogni elaborazione in corso e spegnere il PC in attesa della bonifica dello stesso.

22.7 Gli strumenti informatici possono essere dotati di software per la raccolta di eventi, operazioni e situazioni, utili ad indentificare ogni possibile tentativo di operazione malevola o dannosa ad opera sia degli utenti che di terzi. Tali eventi saranno raccolti in appositi "log" trattati nel rispetto delle disposizioni vigenti in materia.

23. Accesso ai dati da parte degli "Amministratori di Sistema"

23.1 Tutte le operazioni di assistenza tecnica e di supporto agli utenti si svolgono di norma con la presenza dell'utente ed il relativo consenso all'accesso ai dati presenti sulle postazioni di lavori e/o alle risorse in cloud.

23.2 In caso di modifiche alle configurazioni, malfunzionamenti straordinari, per diagnosi di sistema e comunque in situazioni di emergenza, gli Amministratori di Sistema hanno facoltà di accedere in qualunque momento agli strumenti informatici, anche assegnati ai singoli utenti, per l'espletamento delle proprie funzioni.

23.3 L'Amministratore di Sistema può in qualunque momento procedere alla modifica delle impostazioni, alla rimozione dalle unità di rete, dai servizi cloud, dalle postazioni di lavoro o da altri dispositivi di ogni file o applicazione che riterranno essere pericolosi per la sicurezza della rete o che dovessero, per qualsivoglia motivo, compromettere il regolare funzionamento degli apparati e dei servizi, anche mediante procedure da remoto e senza previo contatto con l'utente.

23.4 Il Titolare dispone specifiche istruzioni in relazione alle attività degli amministratori di sistema. Gli accessi degli amministratori di sistema ai sistemi informatici e la loro attività sono registrati in specifici file di log, soggetti a verifiche periodiche.

24. Social Media Policy

24.1 L'utilizzo a fini di comunicazione istituzionale e di rapporto con i cittadini e con altri interlocutori è gestito ed organizzato dall'Ente esclusivamente attraverso l'Ufficio Stampa, o servizio analogo autorizzato, o comunque tramite specifiche direttive ed istruzioni operative al personale a ciò espressamente addetto. Sono escluse iniziative individuali da parte dei singoli utenti.

24.2 Fermo restando il pieno ed inderogabile diritto della persona alla libertà di espressione ed al libero scambio di idee ed opinioni, l'Ente ritiene comunque opportuno indicare agli utenti alcune regole comportamentali, al fine di tutelare tanto la propria immagine quanto i propri dipendenti, amministratori, i cittadini, i fornitori, oltre che gli stessi utenti utilizzatori dei social media. Resta fermo che viene vietata la partecipazione agli stessi social media durante l'orario di lavoro.

24.3 La policy qui dettata deve essere seguita dagli utenti sia che utilizzino dispositivi messi a disposizione dall'Ente, sia che utilizzino propri dispositivi, sia che partecipino ai social media a titolo personale, sia che lo facciano per finalità professionali, come dipendenti dell'Amministrazione.

24.4 La condivisione dei contenuti sui social deve sempre rispettare e garantire la segretezza sulle informazioni acquisite nell'ambito del proprio ufficio.

24.5 L'utente deve garantire la tutela della privacy delle persone; di conseguenza, non potrà comunicare o diffondere dati personali (quali dati anagrafici, immagini, video, suoni e voci) di colleghi, di amministratori e in genere di collaboratori dell'Ente, se non con il preventivo personale consenso di questi, e comunque non potrà postare nel social media immagini, video, suoni e voci registrati all'interno dei luoghi di lavoro o afferenti all'attività dell'Amministrazione.

24.6 L'utente risponde personalmente dei propri comportamenti e deve astenersi dal porre in essere, nei confronti in genere di terzi e specificatamente verso l'Ente, i colleghi, i cittadini ed i fornitori, attività che possano essere penalmente o civilmente rilevanti; a titolo esemplificativo, sono quindi vietati comportamenti ingiuriosi, diffamatori e denigratori, discriminatori o che configurano molestie. In tal senso, è vivamente auspicato da parte di tutti un comportamento civile e sobrio, in particolar modo in qualunque occasione in cui l'espressione o il contesto in cui essa avviene possa essere collegata all'ambito dell'Amministrazione.

24.7 Infine, in via generale ed ove non autorizzato in senso diverso direttamente dall'Ente, l'utente, nell'uso dei social network, esprime unicamente le proprie opinioni personali; pertanto, ove necessario od opportuno per la possibile connessione con l'Ente, in particolare in forum professionali, l'utente dovrà precisare che le opinioni espresse sono esclusivamente personali e non riconducibili all'Amministrazione.

25. Osservanza delle disposizioni in materia di protezione dati personali e privacy

25.1 È obbligatorio attenersi alle disposizioni contenute nel "*Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)*", c.d. GDPR e nel "Decreto Legislativo n. 196 del 30 giugno 2003 - Codice in materia di protezione dei dati personali" e s.m.i.

25.2 Gli strumenti informatici/tecnologici considerati nel presente Regolamento costituiscono tutti strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa, anche ai sensi e per gli effetti dell'art. 4, comma secondo, della Legge n. 300/1970; conseguentemente le informazioni raccolte sulla base di quanto qui indicato possono essere utilizzate a tutti i fini connessi al rapporto di lavoro, essendone stata data informazione ai lavoratori sulle modalità di uso degli strumenti stessi, sugli interventi che potranno venir compiuti nel sistema informatico ovvero nel singolo strumento e sui conseguenti sistemi di controllo che potessero venir eventualmente compiuti, fermo restando il rispetto della normativa in materia di protezione dei dati personali.

26. Controlli graduali e accesso ai dati trattati dall'utente

26.1 Il Datore di lavoro, preso atto del divieto di utilizzo di strumenti informatici/tecnologici per il controllo dell'attività lavorativa del dipendente, assicura che tutti i già menzionati strumenti saranno installati esclusivamente per esigenze organizzative / produttive e per tutte le finalità previste dal rapporto di lavoro. Ferme restando le modalità di controllo specificate negli articoli precedenti, in caso di anomalie il personale incaricato del SIIT o l'Amministratore di Sistema, nel rispetto della normativa sulla protezione dei dati personali, potrà effettuare controlli su tutti gli strumenti informatici/tecnologici forniti dall'Amministrazione e sui documenti ivi contenuti. In particolare, potranno essere effettuati controlli per le seguenti finalità:

- tutelare la sicurezza e preservare l'integrità degli strumenti informatici e dei dati;
- evitare la commissione di illeciti;
- compiere attività di carattere difensivo e/o preventivo per la sicurezza informatica dei sistemi;
- svolgere controlli e programmazione dei costi;
- verificare e ripristinare le funzionalità del sistema e degli strumenti informatici.

A tal fine l'Unione Valdera utilizza sistemi automatizzati per la gestione centralizzata dei cosiddetti "file di log", che consentono di tracciare eventuali anomalie o minacce informatiche che potrebbero colpire i sistemi, compromettendo la funzionalità e la sicurezza degli apparati informatici e delle informazioni contenute.

Le attività di controllo potranno avvenire anche mediante Audit e Vulnerability Assesment del sistema informatico. Per tali controlli l'Ente si riserva la facoltà di avvalersi di soggetti esterni. L'elenco delle tipologie di log e delle relative retention sono specificati nel documento "Gestione dei log di sistema" adottato nel rispetto dell'art. 29 del presente regolamento.

26.2 Il personale incaricato effettuerà, in prima battuta, controlli anonimi che si concluderanno con avvisi generalizzati diretti agli incaricati dell'area o del settore in cui è stata rilevata l'anomalia, nei quali si evidenzierà l'utilizzo irregolare degli strumenti informatici e si inviteranno gli interessati ad attenersi scrupolosamente ai compiti assegnati ed alle istruzioni impartite. Controlli su base individuale potranno essere computi solo in caso di successive ulteriori anomalie.

26.3 In presenza di seri indizi, il personale incaricato potrà anche effettuare controlli rivolti ad accertare condotte illecite del singolo lavoratore (c.d. controllo difensivo del datore di lavoro), anche mediante verifica dei file log presenti sulle risorse di rete o sui singoli dispositivi in uso all'utente.

26.4 L'amministratore di sistema, nel caso in cui rilevi anomalie o configurazioni non corrette delle postazioni di lavoro, può provvedere a isolare immediatamente l'origine dell'anomalia o del malfunzionamento anche senza avvisare l'utente, così da salvaguardare la sicurezza e l'integrità dei sistemi informatici. In tal caso verrà data successiva informativa all'utente sui motivi dell'avvenuto intervento sulla risorsa informatica da parte dell'amministratore di sistema.

27. Violazione dei dati personali (cd. data breach)

27.1 In caso di violazione, anche sospetta, della sicurezza che comporti accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati, è necessario informare immediatamente il SIIT, mediante l'invio di una e-mail urgente all'indirizzo siit@unione.valdera.pi.it inserendo nell'oggetto della e-mail "URGENTE – VIOLAZIONE DATI", descrivendo nel contenuto: il motivo per cui si ritiene ci sia stata una violazione, il luogo ove si ritiene ci sia stata la violazione (pc, server, software, ecc.), l'ora (HH:MM) dell'evento rilevato.

28. Violazioni del presente regolamento

28.1 È fatto obbligo a tutti gli utenti di osservare le disposizioni portate a conoscenza con il presente Regolamento. Fermi restando gli eventuali profili di responsabilità civile e penale, il mancato rispetto o la violazione delle regole sopra ricordate è perseguibile nei confronti del personale dipendente con provvedimenti disciplinari previsti dal vigente CCNL, e nei confronti dei collaboratori, consulenti e fornitori esterni di cui al suddetto art. 1.3, verificata la gravità della violazione contestata, dall'applicazione delle penali previste dal contratto fino alla risoluzione o il recesso dal contratto ad essi relativo.

28.2 Resta ferma la responsabilità civile, penale e contabile di ogni utente per fatti illeciti e/o danni derivanti da usi non consentiti della Rete o degli strumenti informatici messi a disposizione dall'Amministrazione, anche alla luce delle prescrizioni contenute nel presente disciplinare.

29. Approvazione, aggiornamento e revisione

29.1 Il presente regolamento, in quanto Regolamento di organizzazione è approvato dalla Giunta dell'Unione Valdera, ed è applicabile a tutti i comuni aderenti o convenzionati con la funzione informatica prevista dallo Statuto Articolo 6 comma 1 lett. g. e comma 2 lett. h. per le parti compatibili.

29.2 I documenti collegati e citati nel presente regolamento, ovvero "Elenco software autorizzati", "Elenco dei servizi Cloud autorizzati", "Gestione dei log di sistema" saranno approvati con atto dal Dirigente competente dell'Unione

Valdera entro 120 gg. dall'entrata in vigore del presente regolamento, con revisione ed aggiornamento almeno annuale.

29.3 L'ufficio di coordinamento dei Responsabili per la Transizione al Digitale, i Segretari Generali, i Dirigenti compreso facenti funzione, i referenti del gruppo di lavoro in tema di protezione dati personali (Privacy) dei comuni aderenti all'Unione Valdera possono proporre, quando ritenuto necessario, integrazioni e modifiche al presente Regolamento. Le proposte verranno esaminate dal SIIT e dai Dirigenti competenti in materia.

30. Disposizioni finali e di rinvio

30.1 Il presente regolamento entra in vigore con l'approvazione dello stesso.

30.2 Dell'approvazione del presente Regolamento viene data diffusione ai dipendenti tramite la intranet comunale e/o posta elettronica.

30.3 L'Amministrazione informa gli interessati del trattamento relativo alla raccolta, conservazione ed utilizzo dei dati di log e dei metadati raccolti in modo automatico dai diversi componenti del sistema informatico dell'Amministrazione nonché delle copie dei programmi e dei dati in accordo a quanto disposto dal GDPR in materia di informativa agli interessati attraverso i consueti strumenti informativi (mail, Intranet, etc.)