DISCIPLINARE PER L'UTILIZZO DEI SISTEMI INFORMATICI NELL'UNIONE TERRE DI PIANURA E NEI COMUNI AD ESSA AFFERENTI

Approvato con Delibera di Giunta dell'Unione n. … del ...

Indice

1. Premessa

Il presente disciplinare costituisce atto a validità in ambito territoriale per tutti gli strumenti informatici gestiti dal Settore Informatico Associato (da ora SIA) dell'Unione Terre di Pianura in tutti gli Enti che ad essa afferiscono.
Ha per oggetto i criteri e le modalità di utilizzo e controllo degli strumenti informatici [1], dei servizi di posta elettronica, intranet ed internet, da parte dei propri dipendenti, a tempo determinato o indeterminato, e di tutti i collaboratori (es. personale comandato e/o distaccato, fornitori, tirocinanti,...), amministratori o comunque soggetti autorizzati che, a vario titolo, svolgono un'attività accedendo al sistema informatico, nel rispetto dei regolamenti comunali per il trattamento dei dati personali e di quanto previsto dal Codice in materia di protezione dei dati personali (D.lgs. 30/06/2003 n. 196) e delle linee-guida per posta elettronica e internet contenute nel provvedimento n. 13 dell'1/3/2007 del Garante per la protezione dei dati personali.

Si intende qui fornire indicazioni tecniche ed organizzative da applicare per garantire la sicurezza dei dati trattati con strumentazioni informatiche e permettere una crescita tecnologica ed organizzativa dei sistemi informativi dei Comuni dell'Unione Terre di Pianura in un'ottica di omogeneità tecnologica e di sviluppo, al fine di estendere l'uso delle tecnologie sia nell'organizzazione degli enti, che nel rapporto con cittadini, professionisti e imprese.
Un principio di base da tenere sempre presente è che, a causa dell'interconnettività e dell'interdipendenza fra le componenti di un sistema informatico, i problemi di sicurezza su una singola postazione o su un singolo punto della rete si propagano e incidono sul funzionamento di tutto il sistema, mettendone in pericolo la sua complessiva integrità.

1.1 Principi generali

Gli strumenti informatici forniti al personale dipendente sono utilizzati esclusivamente per lo svolgimento del lavoro assegnato, con modalità e comportamenti adeguati ai compiti ed alle responsabilità dei dipendenti pubblici, rispettando i comuni principi etici e di correttezza e i doveri stabiliti nel "Codice di comportamento dei dipendenti della pubblica amministrazione" nonché la privacy e la segretezza dei dati trattati secondo le normative vigenti (in special modo al D.Lgs. 196/2003 e ss.mm.ii., al regolamento sui procedimenti disciplinari del personale e altri regolamenti afferenti all'argomento in oggetto adottati dagli enti dell'Unione Terre di Pianura).
Ciascun dipendente è direttamente responsabile in caso di utilizzo da parte di terzi degli strumenti informatici a lui affidati; deve custodire le proprie credenziali di autenticazione e la propria strumentazione in modo appropriato e diligente, segnalando tempestivamente ogni danneggiamento, furto o smarrimento al proprio responsabile di servizio, che provvederà ad informare il SIA.

1.2 Modalità di pubblicizzazione e aggiornamento periodico

Circa l'eventuale trattamento di dati personali del lavoratore effettuato per verificare il corretto utilizzo di alcuni strumenti elettronici, questo disciplinare costituisce un'integrazione alla più generale informativa sul trattamento dei dati personali resa ai sensi dell'art. 13 del decreto legislativo n. 196/2003.
Il presente documento viene portato a conoscenza di tutti gli utilizzatori dei sistemi informativi tramite e-

1 Per strumenti informatici si intendono: personal computer fissi o portatili, videoterminali, stampanti locali o di rete, i prodotti software regolarmente licenziati, palmari, cellulari o altri dispositivi di telecomunicazione le relative periferiche nonché tutta l'infrastruttura logica e fisica che permette l'interconnessione delle postazioni di lavoro al fine di agevolare la trasmissione di dati.

mail successivamente alla sua approvazione, e agli eventuali aggiornamenti successivi.
Rimane sempre a disposizione presso il SIA e l'Ufficio Unico del Personale.
Nel rispetto e nei limiti del presente documento, ulteriori elementi di dettaglio potranno essere emanati dal Responsabile del Servizio Informatico Associato.

Il disciplinare viene aggiornato in considerazione di:

- introduzione di nuovi strumenti elettronici, rilevanti per le finalità del disciplinare;
- modifiche e/o innovazioni di carattere normativo o giurisprudenziale;
- modifiche e/o innovazioni di carattere tecnico-informatico;
- esperienze maturate, nel periodo di riferimento, in applicazione del disciplinare;
- nuove esigenze di sicurezza, produzione, organizzazione che giustifichino una revisione del disciplinare.

2. Modalità di accesso ai sistemi

2.1 Sicurezza fisica dei locali

L'accesso ai locali e alle postazioni di lavoro è riservato agli utilizzatori in base alle funzioni loro assegnate. L'accesso di personale esterno (quale, ad esempio, fornitori dell'Ente), che per necessità dovesse utilizzare in modo estemporaneo la postazione di lavoro, dovrà essere concordato, autorizzato ed avvenire sotto la responsabilità dell'utilizzatore interno che ne richiede l'intervento, in accordo col SIA, qualora sia necessario.

2.2 Rilascio e gestione delle credenziali di accesso al sistema

Il sistema di autenticazione utilizzato in tutti gli Enti afferenti all'Unione è Microsoft Windows Active Directory, che viene utilizzato per autenticare gli utenti di risorse condivise sulla rete quali:

- cartelle di file system,
- applicativi software,
- stampanti.

Quasi la totalità delle procedure applicative sono integrate con Active Directory di Windows e quindi le credenziali di accesso a queste procedure sono le stesse dell'accesso alla rete e al PC.
Alcuni sw, nonostante siano una piccola minoranza, non utilizzano questo sistema centralizzato, ma possiedono un proprio sistema di autenticazione, altri software web richiedono credenziali Federa/SPID.
Per l'accesso ai Personal Computer ci si avvale esclusivamente delle credenziali di Active Directory.

Tutti gli operatori del SIA sono soggetti preposti alla gestione delle credenziali: a fronte di una richiesta di definizione di nuova utenza, provvedono a creare un account con password provvisoria da modificarsi obbligatoriamente al primo accesso.
Le credenziali di autenticazione consistono in un codice per l'autenticazione dell'incaricato (solitamente composto dal cognome e iniziale del nome) associato ad una parola chiave riservata (password).

Le credenziali di accesso al sistema e le relative caselle e-mail vengono create dal SIA a seguito di richiesta inoltrata mediante apposito modulo condiviso con l'Ufficio Unico del Personale (*Allegato A*), in

cui il Dirigente/Responsabile del Settore/Ufficio competente (o suo delegato alla gestione), chiede le abilitazioni, dichiarando che il nuovo collaboratore avrà titolo per accedere a dati e applicativi. È onere del responsabile richiedente ottenere l'autorizzazione dei colleghi titolari delle banche dati a cui richiede l'accesso per il nuovo collaboratore.
Nella richiesta vengono esplicitate le abilitazioni che lo stesso dovrà avere relativamente all'intero sistema (cartelle condivise, applicativi e banche dati locali), nonché l'indicazione di eventuali caselle mail condivise, a cui l'utente dovrà avere accesso.

L'incaricato del SIA crea le relative credenziali Active Directory ed e-mail e comunica, in modo riservato al diretto interessato o, in caso di impossibilità, al suo responsabile di Settore o Servizio, le password temporanee, che dovranno essere sostituite al primo accesso con quelle definitive.
Non sono previste credenziali d'accesso che non siano legate ad un singolo individuo e che possono essere condivise da tutto un gruppo di operatori. Le credenziali di accesso al sistema sono sempre nominative.

Con le sue credenziali, un utente può accedere da ciascun PC collocato in qualunque punto della rete dell'Unione, anche in un Comune diverso da quello in cui lavora, trovandosi sempre a disposizione la sua scrivania di lavoro e tutti gli accessi che utilizza dalla sua postazione.
Nel caso un utente abbia dimenticato una password, si dovrà rivolgere al SIA che, previo riconoscimento, provvederà a resettarla e a comunicarla riservatamente all'utente; anche in questo caso, al primo accesso, dovrà necessariamente modificarla con una nuova di sua scelta.
Eccezionalmente, nel caso in cui si renda indispensabile ed indifferibile, per esclusive necessità tecniche di operatività e sicurezza, i tecnici SIA preposti alla gestione delle credenziali potranno modificare la password degli utenti; in questi casi, giustificandone le ragioni, ne daranno tempestiva comunicazione scritta agli stessi, che quindi provvederanno a sostituirla obbligatoriamente al primo accesso.
Non è previsto alcun caso in cui gli addetti del SIA potranno modificare la password degli utenti e comunicare tale nuova password ad un altro utente, diverso dal titolare. In caso di particolari necessità ed urgenze, sarà sempre possibile fornire altri utenti di tutte le abilitazioni necessarie.
L'utilizzatore ha l'obbligo di impostare la password seguendo la procedura di cambio password nel rispetto delle regole definite, nel seguito descritte.
Ogni incaricato che riceve le proprie password ne è direttamente responsabile e non deve in alcun modo comunicare le proprie password a persone diverse od altri incaricati.
Le password sono strettamente personali e non vanno comunicate a nessuno.
Non è tecnicamente possibile ricostruire le password impostate dagli utenti; il SIA non è autorizzato a chiedere le password agli utenti per intervenire; in caso di necessità la può resettare,

Sono disincentivate situazioni in cui gli utenti non eseguano una validazione (logon) ad un dominio e non implementano complete funzionalità di sicurezza (es. il fornitore o il consulente esterno che collega il suo PC alla rete comunale).

La durata delle password viene definita a livello centrale; il sistema avviserà l'utente quando la password sta per scadere ed è quindi necessario cambiarla. Alle password di accesso al dominio Windows è dato un periodo di vita massimo di 90 giorni. Trascorso tale periodo se l'utente non l'ha già autonomamente cambiata, il sistema lo costringe ad immetterne una nuova altrimenti il sistema non si attiva.
Per impostare la nuova password è necessario fornire anche quella vecchia; nel caso in cui l'utente l'avesse dimenticata, l'amministratore di sistema, dopo aver riconosciuto l'utente, può forzare la creazione di una nuova password provvisoria.

Un utente che non sia stato disabilitato può modificare la propria password anche prima della scadenza autenticandosi con userid e vecchia password (valida per questa funzione anche se scaduta).
Gli utenti possono modificare la propria password in qualsiasi momento, oppure essere chiamati a cambiarla dal sistema stesso, in risposta a policy aziendali o interventi amministrativi.
Gli utenti sono tenuti a cambiare la password anche nel caso in cui abbiano il sospetto che la stessa non sia più segreta.

Gli utenti sono sensibilizzati, informati ed istruiti sull'importanza dell'uso, della segretezza e sulle modalità di modifica delle password.
Le password devono essere significative e conformi ai requisiti di complessità. Ovvero:

- devono essere lunghe almeno 8 caratteri
- devono essere "complesse", cioè contenere almeno 3 delle 4 seguenti tipologie: maiuscole, minuscole, numeri, caratteri speciali.
- si deve evitare di immettere sequenze della stessa lettera
- non deve contenere il nome, il cognome o l'user-name (account utente)
- non deve trattarsi di una parola o di un nome comune.

Il mancato uso delle credenziali per almeno sei mesi continuativi determina la loro disattivazione salvo quelle preventivamente autorizzate per i soli scopi di gestione tecnica e in casi particolari valutati con il SIA di volta in volta.
Per riattivare le credenziali, l'utente dovrà rivolgersi al servizio SIA che, verificatone il diritto, lo riattiverà con le stesse modalità del caso di "dimenticanza di password".
Periodicamente il SIA effettuerà controlli e provvederà a disattivare gli account non utilizzati.
Il codice di identificazione, laddove inutilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.

2.3 Accesso dall'esterno

L'accesso dall'esterno alle applicazioni e ai dati avviene con le stesse credenziali utilizzate per l'interno.
L'accesso dall'esterno non è automatico, ma avviene a seguito di specifica abilitazione.
Per gli amministratori, i dirigenti e i responsabili apicali l'abilitazione avviene a seguito di richiesta scritta da parte dell'interessato. Per i dipendenti che non abbiano funzioni apicali l'accesso avviene a seguito di richiesta scritta da parte del dirigente o del responsabile apicale dell'area di riferimento.
Costituiscono eccezione i dipendenti del Corpo di Polizia Municipale: tutti sono dotati di abilitazione per poter accedere alla rete dalle postazioni collocate sui mezzi di servizio.
L'accesso dall'esterno può avvenire con postazioni di lavoro fornite dall'ente, ovvero con postazioni di lavoro di proprietà dell'utilizzatore; in tal caso questi è tenuto a mantenere la postazione di lavoro nelle condizioni minime di sicurezza quale l'installazione di un antivirus.

3. Norme di comportamento

Il personale deve custodire la strumentazione assegnata in modo appropriato e diligente, segnalando tempestivamente ogni danneggiamento, furto o smarrimento al proprio responsabile di servizio e al SIA.

3.1 Utilizzo delle postazioni fisse di lavoro

Tutte le applicazioni e, in generale, tutti gli strumenti software necessari allo svolgimento del lavoro per tutti gli enti afferenti all'Unione, sono distribuiti centralmente tramite il software di virtualizzazione Citrix, che consente la manutenzione centralizzata dell'intero sistema.
Sui PC in locale, ove l'utente non ha diritti di amministratore, è installato il minimo indispensabile per lavorare al di fuori dei sistemi di rete, in caso di temporanee interruzioni.
Per accedere ai servizi informatici da una postazione di lavoro l'utente deve utilizzare la credenziale rilasciata e gestita nei modi descritti al precedente paragrafo.
Le postazioni di lavoro devono sempre essere installate e gestite dal SIA, siano esse fisse, portatili, in rete o stand alone; è compito dei responsabili e dirigenti dei servizi degli enti, segnalare eventuali irregolarità e trasgressioni al SIA, il quale provvederà alla regolarizzazione delle difformità segnalate; la gestione e manutenzione dei Personal Computer dell'Ente fanno capo al SIA e non è permesso agli utenti di intervenire personalmente, se non espressamente autorizzati dal medesimo Settore, sulle apparecchiature informatiche.
Le postazioni di lavoro vengono assegnate al singolo dipendente da parte del responsabile del servizio stesso; è comunque possibile utilizzare una postazione diversa da quella assegnata utilizzando per l'accesso la coppia 'utente – password personale'.
Le postazioni al pubblico o di utilizzo generico sono affidate al dirigente del servizio assegnatario o a persona designata dal dirigente stesso.

L'utente deve essere consapevole del fatto che permettere l'accesso col proprio identificativo a terzi (anche colleghi), consente agli stessi l'utilizzo dei relativi servizi in nome dell'utente titolare, nonché l'accesso ai dati cui il medesimo utente è abilitato, anche con possibilità di gestione degli stessi (ad es. visualizzazione di informazioni riservate, come il cedolino e la posta elettronica, piuttosto che la distruzione o modifica dei dati o l'uso indebito di servizi, ecc..).

Preso atto di tale conseguenza, l'utente deve:

a) custodire con cura la parola chiave personale e, in nessun caso, comunicarla a terzi; l'utente è personalmente soggetto a responsabilità civili e penali, in caso di abusi o incidenti di sicurezza, nel caso divulghi la password, ovvero renda disponibile ad altri l'accesso;
b) non lasciare incustodita ed accessibile la propria postazione una volta connesso al sistema con le proprie credenziali di autenticazione; nel caso l'utente abbia necessità di allontanarsi è tenuto a chiudere la sessione o a bloccare la propria stazione di lavoro (utilizzando la sequenza di tasti "ctrl-alt-canc" e il tasto "Blocca Computer"); è evidente che lasciare un elaboratore incustodito può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso;
c) non cedere, una volta superata la fase di autenticazione, l'uso della propria stazione ad altra persona se non per motivi tecnici autorizzati dal SIA.

Tranne nei casi segnalati dal SIA per i lavori di manutenzione al sistema, al termine del servizio ciascun operatore deve spegnere il PC: lo spegnimento è importante al fine di evitare sprechi energetici ed inutile usura del PC stesso.

Nel seguito le regole di utilizzo:

1. è tassativamente proibito installare programmi software non autorizzati, anche se legali, (es: programmi salvaschermo, software peer-to-peer o altri software freeware o scaricati da internet) e/o modificare la configurazione hardware e software delle propria postazione di lavoro se non autorizzati dal personale del SIA; qualora venissero trovati programmi non autorizzati sulle stazioni di lavoro questi potranno essere disinstallati dal personale tecnico addetto alla manutenzione dei Personal Computer (anche senza preavviso, se ritenuti pericolosi per la sicurezza del sistema o dei dati);
2. i dati, documenti o files gestiti dagli incaricati in relazione alle mansioni attribuite, nella loro forma definitiva, devono risiedere sui server di sistema, in particolare sulle unità di rete definite nel sistema informativo comunale (lettera seguita da due punti, es. 'G:'); tali cartelle costituiscono aree di condivisione di informazioni relative all'attività lavorativa e non possono essere utilizzate per il salvataggio di file non pertinenti alla specifica attività o non istituzionali; su queste unità vengono svolte attività di amministrazione e backup da parte dell'amministratore di sistema, che potrà procedere alla rimozione senza preavviso di file o applicazioni ritenute pericolose per la sicurezza del sistema o non inerenti all'attività lavorativa;
3. sulle unità di memorizzazione della postazione (es. 'C:') non vengono svolte attività di backup; tutti i dati relativi alla propria attività lavorativa di cui si voglia salvaguardare la sicurezza vanno memorizzati nelle unità di rete predisposte dal SIA;
4. l'utilizzo di memorie (chiavette) USB per la memorizzazione ed il trasferimento dei dati deve essere circoscritto, per motivi di sicurezza, ai soli casi di effettiva necessità; per trasmettere i dati tra le postazioni dell'Ente si raccomanda l'utilizzo delle aree condivise che sono messe a disposizione, mentre per le trasmissioni di dati da e per l'esterno si raccomanda l'utilizzo della posta elettronica o altri strumenti di trasferimento dati sicuri (es. portali istituzionali ad accesso autenticato ecc.); tali modalità sono infatti soggette a controlli antivirus sistematici, mentre, viceversa, le chiavi USB possono entrare in contatto con ambienti che possono portare pericolose infezioni all'interno dell'Ente; qualora tali comportamenti venissero disattesi, il SIA si riserva di disabilitare sui PC dell'Ente il riconoscimento automatico di chiavette USB; inoltre, secondo principio di necessità, qualora sulle copie venissero trasferiti dati personali, il trattamento dovrà avvenire con le modalità previste dalla legge in materia di riservatezza e protezione degli stessi; al termine del trattamento sarà cura del dipendente distruggere o rendere inutilizzabili i supporti rimovibili o comunque rendere le informazioni non intelligibili e in alcun modo ricostruibili.
5. sono proibite le violazioni della privacy così come sancito dal D. Lgs. n. 196/2003 "Codice in materia di protezione dei dati personali" e ss.mm.ii. contenente standard e regole che disciplinano il trattamento di dati personali, sensibili o giudiziari;
6. gli utenti devono rispettare diritti d'autore, copyright e licenze d'uso di software, materiali audiovisivi, documenti ed ogni altra informazione digitale protetta a norma di legge;
7. gli utenti sono tenuti ad osservare le disposizioni di cui al presente ed eventuali direttive del SIA volte a garantire il corretto funzionamento delle procedure di sicurezza e conservazione dei dati;
8. gli utenti sono obbligati a segnalare immediatamente al SIA ogni sospetto di effrazione, incidente, abuso o violazione della sicurezza;
9. gli utenti sono tenuti a seguire le indicazioni che, in casi di necessità, il SIA fornisce.

Non è inoltre consentito:

1. usare la rete in modo difforme da quanto previsto dalle leggi penali, civili e amministrative e da quanto previsto dal presente disciplinare e dalle istruzioni del Dirigente/Responsabile del Servizio;
2. utilizzare la rete per scopi incompatibili con l'attività istituzionale;

3. utilizzare una password a cui non si è autorizzati e violare la riservatezza di altri utenti o di terzi; qualsiasi accesso alla posta elettronica di altri soggetti senza autorizzazione od al di fuori di una specifica attività di controllo, anche da parte di superiori gerarchici o di addetti al SIA costituisce "Accesso abusivo a un sistema informatico o telematico" e come tale è punito dal codice penale art.615-ter e costituisce comportamento rilevante dal punto di vista disciplinare;
4. divulgare informazioni tecniche relative alla struttura informatica comunale che possano pregiudicare la sicurezza della stessa;
5. utilizzare gli strumenti informatici comunali al fine di custodire, far circolare o promuovere materiale pubblicitario personale o codice maligno (spam, virus, trojan horses, programmi pirata o altre porzioni di codice maligno e/o altro materiale non autorizzato);
6. utilizzare la strumentazione informatica, per la realizzazione, redazione, memorizzazione e spedizione di documenti di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione, appartenenza sindacale e politica;
7. installare o connettere alla rete dei dispositivi o delle periferiche proprie e di persone esterne senza autorizzazione del SIA;
8. scaricare da internet o da supporto magnetico proveniente dall'esterno file di dubbia provenienza e sicurezza senza farli sottoporre a opportuno controllo;
9. l'utilizzo degli strumenti informatici al di fuori dell'orario di servizio senza preventiva autorizzazione del proprio responsabile o del SIA.

Il personale del SIA può, nel rispetto delle normative previste dal D.Lgs. 196/03 e dell'articolo 615-ter c.p., per fini di sicurezza, diagnostici e tecnici, verificare il corretto utilizzo della postazione di lavoro dell'utente e l'osservanza delle regole qui descritte.
Tali verifiche potranno essere effettuate anche attraverso sistemi di connessione remota previo avviso all'utente, eccezion fatta per i casi in cui l'utente non presidi la postazione in cui sussista una minaccia alla sicurezza del sistema informativo e dei dati in esso contenuti.
Su indicazione del dirigente competente, potranno essere effettuati controlli di conformità alla legge, anche saltuari o occasionali, precisando le ragioni legittime, specifiche e non generiche della richiesta. Analoghi controlli potranno essere consentiti all'autorità giudiziaria o per l'esercizio di un diritto in sede giudiziaria.

3.2 Postazioni e apparati informatici "mobili"

Le regole di utilizzo delle postazioni di lavoro portatili (notebook o netbook) o di dispositivi mobili (smartphone, palmari) sono le stesse dei PC collegati alla rete locale.
Il loro utilizzo richiede però maggiori precauzioni rispetto alle postazioni fisse in ordine ai seguenti elementi:

- attenzione rispetto al furto o allo smarrimento delle stesse;
- attenzione rispetto a virus o codici maligni tramite reti wireless (senza fili).

Le postazioni di lavoro mobili vengono assegnate per esigenze di lavoro specifiche in cui l'utilizzatore ha necessità di frequenti spostamenti. L'assegnazione delle postazioni mobili viene concordata tra la direzione dei singoli comuni e il SIA in base alle indicazioni degli organi politici.
L'utente è responsabile della postazione o dispositivo assegnatoli e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

Per quanto riguarda le smart card, business key e altri dispositivi per il riconoscimento che contengono

certificati di firma dei titolari, utilizzabili ad esempio nei procedimenti amministrativi dell'Ente, i destinatari sono responsabili del corretto utilizzo e devono custodire adeguatamente i dispositivi, il relativo PIN e altro materiale a corredo.

3.3 Stampanti e materiali di consumo

L'utilizzo delle stampanti e dei materiali di consumo in genere (carta, inchiostro, toner, supporti magnetici, supporti digitali, ecc.) è riservato esclusivamente ai compiti di natura strettamente istituzionale.
Devono essere evitati in ogni modo sprechi dei suddetti materiali o utilizzi eccessivi.

4. Regole per la navigazione web

4.1 Internet

La rete internet è una risorsa messa a disposizione del personale come fonte di informazione per finalità di documentazione, ricerca e studio utili per lo svolgimento del proprio lavoro.
Per ragioni di sicurezza e per garantire l'integrità dei sistemi informatici, l'accesso ad internet effettuato tramite elaboratori connessi alla rete comunale è scrupolosamente protetto da appositi dispositivi di sicurezza informatica (firewall, antivirus, etc.).

L'utente ha la possibilità di navigare sia all'interno del sistema Citrix, sia all'esterno.
All'interno del sistema Citrix sono abilitati solo siti istituzionali, tra cui quelli che forniscono la consultazione e la gestione di banche dati (es. Agenzia delle Entrate, INPS, …). Per l'utilizzo di questi portali si raccomanda l'accesso attraverso Citrix, perché ne è garantito il funzionamento, rispetto ad eventuali aggiornamenti di browser richiesti.
Per la navigazione libera si può provvedere al di fuori del sistema Citrix.
Per ridurre il rischio di uso improprio della navigazione sono in uso sistemi di filtraggio (proxy), che consentono di individuare categorie di siti non correlate con la prestazione lavorativa (grazie all'utilizzo di 'black list' internazionali aggiornate, ovvero liste di siti ad accesso bloccato) e prevenire accessi e operazioni reputati non attinenti all'attività d'ufficio.

Alcuni dati relativi agli accessi ai siti internet, quali l'utente, il sito visitato e l'orario di accesso, sono conservati per un periodo di 3 mesi, in appositi file di log il cui accesso è consentito al solo personale tecnico preposto. Su indicazione del dirigente competente, potranno essere effettuati su tali file controlli di conformità alla legge, anche saltuari o occasionali, precisando le ragioni legittime, specifiche e non generiche della richiesta. Analoghi controlli potranno essere effettuati per ragioni legate alla funzionalità e sicurezza del sistema. L'accesso a tali dati potrà essere consentito all'autorità giudiziaria o per l'esercizio di un diritto in sede giudiziaria.

In linea di principio e salvo casi particolari, non è consentito:

- lo scarico (upload e/o download) di files e/o programmi software, se non previsto per motivi di lavoro o esplicitamente autorizzati;
- l'effettuazione di ogni genere di transazione finanziaria, acquisti on-line e simili salvo i casi direttamente autorizzati con il rispetto delle normali procedure per gli acquisti;

- la partecipazione a forum non autorizzati, l'utilizzo di chat line, social network, bacheche elettroniche e la registrazione a mailing list o guestbooks anche utilizzando pseudonimi (o nicknames) e, più in generale, qualunque utilizzo di questi servizi internet se non connessi all'attività lavorativa;
- l'utilizzo del collegamento ad internet per attività in violazione del diritto d'autore o altri diritti tutelati dalla normativa vigente;
- l'utilizzo di sistemi Peer to Peer (P2P), di file sharing, podcasting, webcasting o similari, così come connettersi a siti che trasmettono programmi in streaming (come radio o TV via WEB) senza espressa autorizzazione.
- prelevare da internet e/o archiviare sul proprio elaboratore, ovvero sulle risorse di rete condivise, documenti informatici (testo, audio, immagini, filmati, etc.) di natura oltraggiosa, discriminatoria per sesso, religione, origine etnica, appartenenza sindacale o politica, o che comunque possano risultare offensivi della dignità umana;
- diffondere attraverso internet materiale commerciale o pubblicitario non richiesto;
- trasmettere via internet virus o altro codice maligno, per arrecare danni e malfunzionamenti a sistemi informatici;
- fornire a soggetti non autorizzati l'accesso alla connessione internet comunale;
- utilizzare la connessione internet al fine di arrecare danno o disturbo a terzi;
- lo svolgimento di qualsiasi attività intesa ad eludere o ingannare i sistemi di controllo di accesso e/o sicurezza di qualsiasi server interno o pubblico, incluso il possesso o l'uso di strumenti o software intesi ad eludere schemi di protezione da copia abusiva del software, rivelare password, identificare eventuali vulnerabilità della sicurezza dei vari sistemi, decrittare illecitamente file crittografati o compromettere la sicurezza della rete e internet in qualsiasi modo.

Il personale del SIA può in ogni momento, nel rispetto delle normative vigenti e di quanto previsto dal D.Lgs. 196/03, per fini meramente diagnostici e tecnici, verificare il corretto utilizzo delle connessioni e degli accessi ad internet. Le violazioni riscontrate al presente punto, in relazione alla loro gravità sarà oggetto di segnalazione all'Ufficio Procedimenti Disciplinari.

4.2 Intranet

Intendendo per "Intranet" un punto unico di accesso di tutti i dipendenti degli enti afferenti all'Unione, con credenziali personali, dove sono presenti informazioni, documentazione e servizi per il dipendente, si può affermare che tale rete non è ad oggi esistente.
Sono presenti alcune applicazioni web ad utilizzo dei dipendenti, non unificate in uno stesso punto e accessibili con credenziali differenti, come la consultazione del cartellino e la consultazione di cedolino/CUD.

4.3 Punti di accesso wi-fi pubblico ad internet

Presso spazi pubblici o sale ad accesso pubblico poste nei territori dei Comuni afferenti all'Unione, è possibile la realizzazione di impianti wi-fi per l'accesso ad internet tramite connettività a rete pubblica o privata (es. la rete regionale Lepida); l'attivazione di punti d'accesso pubblico ad internet sarà comunque concordato col SIA e, se non diversamente richiesto ed autorizzato, separato dalla rete MAN istituzionale.
Tutte le modalità di accesso ed autenticazione al wi-fi sono regolamentate da atti specifici e autorizzati dal

responsabile degli accessi ad internet del Comune appaltante, nel rispetto delle normative vigenti.

5. Utilizzo della posta elettronica

A tutti i dipendenti, collaboratori (se necessario) e assessori, viene fornita una casella di posta elettronica personale dell'ente di appartenenza, fatti salvi specifici impedimenti di natura tecnica e organizzativa del soggetto interessato.
Il servizio è erogato tramite un sistema gestito in forma centralizzata in capo al SIA; i dati risiedono su sistemi cloud del fornitore, su datacenter presenti in Unione Europea.
Oltre all'indirizzo di posta elettronica personale, possono essere messi a disposizione degli uffici, degli indirizzi di posta elettronica non nominali, condivisi fra più utenti o più enti, che possono essere richiesti dal dirigente o dal responsabile competente.
Per questi indirizzi deve essere indicato un referente responsabile al quale verrà delegata la funzione di stabilire i diritti di accesso alla casella; se non espressamente indicato, la responsabilità è in carico al dirigente medesimo.
La denominazione della casella di posta elettronica assegnata, personale o relativa all'ufficio, contiene, nella parte relativa al dominio (ovvero dopo la @), il riferimento all'ente di appartenenza.

Il SIA definisce le politiche per l'archiviazione dei messaggi di posta elettronica in modo da permetterne la corretta fruizione da parte degli utilizzatori nel rispetto dell'equilibrio complessivo e del dimensionamento dei sistemi. La posta elettronica è un sistema di comunicazione e non di archiviazione delle informazioni, pertanto gli utilizzatori devono, al fine di un migliore utilizzo globale, limitare la crescita della dimensione complessiva della casella.
Il fornitore del sistema di posta in uso attiva funzioni di controllo antispam e antivirus sui messaggi di posta elettronica sia in entrata che in uscita.

Nell'utilizzo della posta devono essere adottate le seguenti misure:

- l'uso della posta istituzionale è consentito unicamente per ragioni di servizio;
- le caselle nominali sono da ritenersi personali e accessibili esclusivamente da parte dell'utente proprietario attraverso l'inserimento di una password personale; la password deve essere mantenuta riservata e non deve essere comunicata; l'utente, utilizzando le apposite funzioni di delega fornite dal sistema di posta può, in caso di necessità e per ragioni di servizio, concedere l'accesso alla propria casella ad altri;
- per le comunicazioni con siti istituzionali è bene non utilizzare la casella di posta personale, ma quella di ufficio, per evitare, in caso di assenza del dipendente, che messaggi importanti per l'Ente non vengano processati nei tempi richiesti;
- è a disposizione di ciascun utente di posta, e ne è consigliabile l'utilizzo, una apposita funzionalità di sistema che consente di inviare automaticamente, in caso di assenze programmate, messaggi di risposta personalizzabili segnalando eventualmente l'indirizzo della persona da contattare;
- a seguito dell'assenza di un dipendente, su richiesta del dirigente di servizio competente o di un suo delegato espressamente nominato, esclusivamente per ragioni di servizio e in caso di necessità improrogabile, è consentito l'accesso alla casella di posta elettronica individuale di un dipendente da parte del dirigente stesso; il prima possibile, o comunque al suo ritorno, il dipendente verrà informato tempestivamente, dallo stesso richiedente, sull'intervento effettuato;

- è consentito l'accesso alla propria casella di posta elettronica anche all'esterno del sistema informativo comunale attraverso internet e il servizio di web mail; resta comunque l'obbligo dell'uso della posta unicamente per ragioni di servizio;
- l'invio di e-mail con allegati a mittenti multipli deve essere limitata onde evitare sovraccarico sul server centrale e sulle linee esterne; per questo scopo è consigliabile utilizzare lo strumento "valigetta";
- è vietata l'apertura di allegati a messaggi di posta elettronica senza il previo accertamento dell'identità del mittente e la sua identificazione come utente sicuro e pertinente all'attività istituzionale;
- le caselle di posta elettronica devono essere mantenute in ordine, cancellando i documenti inutili specialmente se contengono allegati ingombranti e/o effettuando l'archiviazione dei documenti allegati, in base alle informazioni specifiche indicate dal SIA.

In ogni caso non è consentito:

- utilizzare tecniche di "mail spamming" cioè di invio massiccio di comunicazioni a liste di distribuzione esterne o di azioni equivalenti;
- utilizzare il servizio di posta elettronica per inoltrare "catene di S. Antonio", appelli e petizioni (anche se possono sembrare veritieri e socialmente utili), giochi, scherzi, barzellette, o comunque materiale non pertinente alla propria attività lavorativa;
- utilizzare la casella personale per la partecipazioni a dibattiti, forum o mailing-list se non inerenti alla propria attività lavorativa;
- utilizzare il servizio di posta elettronica per trasmettere pubblicità personale o commerciale;
- l'invio di posta a destinatari non espressamente indicati (la cosiddetta 'copia conoscenza nascosta' o 'Ccn') se non per cause evidentemente dovute al rispetto della privacy o per inoltro di comunicazioni di carattere generico (es. comunicazioni al personale senza indicare l'elenco puntuale dei destinatari) che rendono necessario evitare la conoscenza di tutti gli indirizzi dei destinatari;
- utilizzare la posta come 'strumento di archiviazione' di dati, soprattutto se si tratta di dati sensibili o giudiziari, in quanto strumento non idoneo per la sicurezza, economicità e segretezza dei dati.

6. Procedure in caso di cessazione del rapporto lavorativo

Gli accessi ai sistemi informatici dell'Ente sono disabilitati non appena concluso il rapporto di lavoro.
Affinchè ciò avvenga, è necessario che il dirigente referente o l'ufficio personale comunichino la data di perdita del diritto di accedere alla rete aziendale al SIA con almeno una settimana di anticipo.

I documenti informatici prodotti dal lavoratore nell'esercizio dell'attività professionale a favore degli enti dell'Unione, restano nella piena ed esclusiva disponibilità dei rispettivi enti, e il lavoratore non può formare o ottenere copia dei predetti documenti né farne alcun uso dopo la cessazione del rapporto di lavoro.
I documenti conservati dal lavoratore all'interno dei dischi locali del PC in dotazione saranno eliminati a rapporto lavorativo cessato.

Le e-mail relative ad ogni account di posta elettronica non nominativo restano nella piena ed esclusiva disponibilità dell'ente.

L'account di posta elettronica nominativo sarà disattivato (ovvero reso inaccessibile al lavoratore) entro una settimana dalla cessazione del servizio.
È responsabilità del titolare, se possibile almeno 1 mese prima della disattivazione, provvedere a inoltrare ai colleghi i messaggi di competenza e informare i suoi contatti dell'imminente cessazione di servizio, nonché di fornire un indirizzo mail a cui inviare le successive comunicazioni.
La casella di posta resta nella piena disponibilità dell'ente, in particolare del responsabile della struttura di appartenenza del lavoratore per un periodo massimo di 3 mesi; l'accesso sarà consentito previa richiesta al SIA di visibilità della stessa ad un altro account di posta.
In nessun caso il lavoratore può chiedere e ottenerne una copia.

7. Assistenza agli utenti

Il SIA effettua, tramite personale proprio, l'attività di supporto nell'utilizzo dei sistemi informativi.
Le richieste di assistenza devono essere attivate tramite mail ad una casella di posta dedicata, collegata ad un sistema automatizzato di helpdesk.
Per le situazioni bloccanti, è disponibile un numero telefonico dedicato.
Per effettuare assistenza, laddove necessario, gli operatori del SIA utilizzano sistemi di accesso e controllo remoto delle postazioni di lavoro; tale accesso avviene sempre di comune accordo tra l'utilizzatore della postazione e l'operatore del SIA.

Anche i fornitori di software possono essere contattati e fornire assistenza diretta agli utenti.
Qualora soggetti esterni debbano effettuare attività sulle postazioni di lavoro degli utenti o sui server per installazioni e configurazioni, tali attività dovranno essere concordate preventivamente con il SIA, che autorizzerà il collegamento remoto necessario.

8. Privacy e informativa

Ogni operazione di trattamento dei dati avviene solo tramite archivi attinenti al proprio lavoro, nel rispetto della normativa vigente in materia di privacy e alle indicazioni del responsabile del trattamento. Si richiede particolare precauzione nelle memorizzazioni di informazioni contenenti dati personali e/o sensibili e nell'uso di cartelle ad accesso condiviso.
Il contenuto del presente disciplinare integra l'informativa già fornita ai dipendenti e ai collaboratori ai sensi dell'art. 13 del Dlgs. 196/2003.

9. Conclusioni

Tutti i dipendenti degli Enti afferenti all'Unione Terre di Pianura devono attenersi, nell'utilizzo e nella gestione degli strumenti informatici (come definiti in premessa), alle norme e ai principi del presente disciplinare e ai doveri stabiliti nel "Codice di comportamento dei dipendenti delle pubbliche amministrazioni".
La violazione da parte dei lavoratori o degli addetti ai sistemi di manutenzione informatica dei principi e delle norme contenute nel presente disciplinare costituisce violazione degli obblighi e dei doveri del

dipendente pubblico e, pertanto, in relazione alla gravità dell'infrazione, i rispettivi dirigenti, previo espletamento di procedimento disciplinare, possono procedere all'applicazione delle sanzioni previste dalle disposizioni contrattuali vigenti in materia e, in particolare, delle sanzioni penali relative all'accesso abusivo a sistemi informatici o telematici.

10. Allegati

Allegato A:
"RICHIESTA DELLE ABILITAZIONI DI UN NUOVO DIPENDENTE/COLLABORATORE NEGLI ENTI AFFERENTI L'UNIONE DEI COMUNI TERRE DI PIANURA"

Terre di Pianura
UNIONE dei COMUNI

Al SIA dell'Unione

RICHIESTA DELLE ABILITAZIONI DI UN NUOVO DIPENDENTE/COLLABORATORE NEGLI ENTI AFFERENTI L'UNIONE DEI COMUNI TERRE DI PIANURA

Nome	
Cognome	
Ente	
Settore/Servizio	
Unità Organizzativa	
Sede	
Data inizio servizio	

Applicativi e accessi alle relative banche dati:

	BAR	**BUD**	**CAS**	**GRA**	**MAL**	**MIN**	**TDP**
Protocollo							
Atti							
Contabilità							
Tributi							
Riscossioni							
Pers: presenze							
Pers: paghe							
Dem: anagrafe							
Dem: st.civile							
Dem: elettorale							
PM							
Edilizia							
SUAP							
Serv.scuola							
Serv.sociali							
Autocad LT							
ArcView							
...							

	BAR	BUD	CAS	GRA	MAL	MIN	TDP
...							
...							
...							

Caselle di posta elettronica condivise a cui è richiesto l'accesso, oltre a quella personale:

Accesso dischi di rete:

	Lettura/Scrittura	Solo lettura
es → M:\Personale\Giuridico	X	
es → M:\Segreteria\Atti		X

Note:

Il richiedente attesta che il nuovo dipendente/collaboratore, per le mansioni che andrà a ricoprire, avrà titolo per accedere ai dati contenuti negli applicativi, nelle caselle di posta elettronica e nei dischi di rete sopra indicati.

Il Responsabile del Settore / Servizio

……...