Unione Terred'Acqua

# PIANO DELLA SICUREZZA INFORMATICA

Trattamenti con strumenti elettronici

## DECRETO LEGISLATIVO 196/2003
(allegato B)

approvato con delibera della Giunta dell'Unione n.

# Sommario


1. Struttura del sistema e protezioni ..... 3
   1.1. Architettura della rete ..... 3
   1.2. Sicurezza della rete ..... 3
   1.3. Architettura del Sistema Informatico ..... 3
      1.1.1. Banche dati ..... 3
      1.1.2. Posta elettronica ..... 3
      1.1.3. Sistema di autenticazione ..... 3
   1.4. Sicurezza dei dati ..... 4
      1.1.4. Banche dati centralizzate ..... 4
      1.1.5. Archivi documentali centralizzati ..... 4
      1.1.6. Banche dati ed archivi documentali residenti su P.C. ..... 4
   1.5. Aggiornamenti dei software ..... 4
2. Modalità di gestione delle credenziali di autenticazione e delle autorizzazioni ..... 5
   2.1. Incaricati del trattamento informatico ..... 5
   2.2. Soggetto preposto alla custodia delle credenziali, alla loro attribuzione, cancellazione, modifica ..... 5
   2.3. Assegnazione delle credenziali di autenticazione ..... 5
   2.4. Modalità di gestione delle password ..... 5
   2.5. Considerazioni generali sulle password ..... 6
      1.1.7. Sicurezza e limiti nell'uso delle password ..... 6
      1.1.8. Durata e cambio della password ..... 6
      1.1.9. Requisiti delle password ..... 6
   2.6. Disattivazione credenziali per disuso. ..... 6
3. Modalità di gestione delle stazioni di lavoro ..... 7
   3.1. Soggetto preposto alla pulizia o recupero delle banche dati su PC ..... 7
   3.2. Programmi antivirus ..... 7
   3.3. Programmi antispam ..... 7
   3.4. Interventi di Manutenzione ..... 7
   3.5. Società esterne o professionisti per la manutenzione e l'assistenza ..... 7
   3.6. Dismissione delle stazioni di lavoro ..... 8
4. Salvataggio dei dati ..... 8
5. Locali ..... 8
6. Cautele generali ..... 9
   6.1. Password ..... 9
   6.2. Uso del Computer ..... 9
   6.3. Custodia dei supporti ..... 9
   6.4. Supporti ricevuti dall'esterno ..... 9
7. Divieti ..... 9

# 1. Struttura del sistema e protezioni

## 1.1. Architettura della rete

Presso ogni comune dell'Unione c'e' un nodo principale di Lepida denominato PAL (Punto Accesso Lepida). Questi nodi sono collegati al nodo centrale di Persiceto con VPN configurando così una architettura a stella.
La rete Lepida è in fibra ottica Gbit.

Tutte le Sedi comunali sono collegate alla rete aziendale.

Tutti i dipendenti dotati di postazione di PC possono quindi collegarsi alla rete dati ed accedere ad internet. L'accesso ai dati è centralizzato verso la sede del CED SIAT a Persiceto, mentre per l'accesso ad internet, ogni comune "esce" dal proprio PAL di Lepida. Presso ogni PAL comunale è presente un firewall, gestito e configurato dal SIAT, per la protezione della rete stessa.

## 1.2. Sicurezza della rete

Tendenzialmente e preferibilmente tutte le sedi sono connesse alle sedi comunali dotate di PAL Lepida mediante LAN o MAN (metropolitan area network).
Ove non possibile si è proceduto alla connessione via VPN su linea ADSL oppure HDSL attraverso appositi firewall.
L'accesso alla rete comunale è comunque permesso solo tramite autenticazione con nome utente e password.
Tutti i sistemi elencati afferiscono a un sistema di firewall, che controlla il traffico dati in base a politiche di sicurezza prestabilite.

## 1.3. Architettura del Sistema Informatico

### 1.1.1. Banche dati

I dati strutturati delle applicazioni gestionali possono essere memorizzati in:

- banche dati centralizzate, per le applicazioni utilizzate da più utenti
- più raramente, su stazione di lavoro per applicazioni mono-utente o qualora il software non renda possibile l'installazione su server

Le banche dati degli applicativi gestionali ed ulteriori banche dati, nonché archivi documentali non strutturati sono conservati in:

- server e sistemi di memorizzazione centralizzati presso il CED dell'Unione (DB server e file server)
- server e/o sistemi di memorizzazione decentrati presso gli Enti
- server e/o sistemi di memorizzazione ubicati presso Datacenter esterni (es. Lepida, PARER, ecc.)
- Personal Computer distribuiti negli uffici degli enti.

Può quindi accadere che alcune banche dati risiedano esclusivamente sul personal computer dell'utente che le utilizza; ciò può accadere sia per scelta personale (**fortemente sconsigliata**) del singolo utente che volontariamente le mantiene solo sulla propria postazione, sia per le caratteristiche intrinseche del programma utilizzato. L'utente finale diventa quindi il responsabile unico dei documenti e delle banche dati non salvate sui server di rete (e quindi non ricomprese nel sistema centralizzato di backup schedulati). Gli addetti ai S.I. hanno sensibilizzato ed informato gli assegnatari dei P.C. su questa problematica.

### 1.1.2. Posta elettronica

La posta elettronica viene gestita esternamente; ai dipendenti o amministratori è assegnata una casella individuale nella forma nome.cognome@;
Esistono caselle non nominali corrispondenti a gruppi di lavoro o figure istituzionali ma per le quali è definito un responsabile della casella stessa.

### 1.1.3. Sistema di autenticazione

Il principale sistema di autenticazione è Microsoft Windows Active Directory, che viene utilizzato per

autenticare gli utenti di risorse condivise sulla rete quali:

- cartelle
- stampanti
- accesso agli applicativi

Alcune 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.
Altre procedure applicative, invece, non utilizzano questo sistema centralizzato, ma possiedono un proprio sistema di autenticazione.

Per l'accesso ai personal computer ci si avvale esclusivamente delle credenziali di Active Directory

Solo per manutenzione, gli amministratori o incaricati esterni (ditte esterne) possiedono delle apposite credenziali locali della postazione di lavoro stessa.

## 1.4. Sicurezza dei dati

### 1.1.4. Banche dati centralizzate

L'accesso ai dati avviene tramite le procedure gestionali che li trattano: all'utente viene richiesta la digitazione di username e password. Queste credenziali sono verificate dall'Active Directory per le procedure già integrate, oppure dalla procedura stessa.
Contestualmente viene verificato se l'utente è autorizzato all'utilizzo della funzionalità richiesta, cioè l'utente può essere abilitato solo ad alcuni moduli o funzionalità del programma applicativo.
Il sistema di autorizzazione è sempre gestito dalla procedura informatica.
La gestione del rilascio delle credenziali di Active Directory compete al servizio informativo Associato (SIAT)
Il rilascio e gestione delle credenziali o delle funzionalità utente all'interno del programma applicativo compete agli Uffici Responsabili dell'Unione e dei singoli Comuni, che agiscono nel rispetto di quanto previsto dal "Codice in materia di protezione dei dati personali", allegato B "Disciplinare tecnico in materia di misure minime di sicurezza", in particolare dei Punti 13 e 14, che vengono riportati di seguito:

*"13. I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.*
*14. Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione."*

### 1.1.5. Archivi documentali centralizzati

I server contenenti archivi documentali richiedono l'autenticazione e l'autorizzazione dell'utente tramite il dominio Active Directory.
Questa autenticazione avviene in modo trasparente per l'utente (senza la richiesta di ulteriore autenticazioni) se le credenziali di accesso al PC sono le stesse che nel dominio Active Directory.

### 1.1.6. Banche dati ed archivi documentali residenti su P.C.

I PC che contengono banche dati locali o archivi documentali, contenenti dati personali e/o sensibili sono protetti da credenziali di accesso personali di Active Directory (oltre alla password di amministratore locale del PC utilizzata solo dal SIAT per interventi tecnici).

## 1.5. Aggiornamenti dei software

I programmi per elaboratore (inclusi i sistemi operativi) vengono tempestivamente aggiornati mediante l'installazione delle nuove versioni degli stessi o delle patches rilasciate dai produttori al fine di prevenirne la vulnerabilità e correggerne i difetti.
La frequenza di aggiornamento non può essere superiore ai 6 mesi.

# 2. Modalità di gestione delle credenziali di autenticazione e delle autorizzazioni

## 2.1. Incaricati del trattamento informatico

Sono tutti gli operatori tecnici del servizio SIAT.

## 2.2. Soggetto preposto alla custodia delle credenziali, alla loro attribuzione, cancellazione, modifica

Il preposto alla gestione delle credenziali provvede a creare un account con password provvisoria da modificarsi obbligatoriamente al primo accesso.

## 2.3. Assegnazione delle credenziali di autenticazione

Le credenziali di autenticazione consistono in un codice per l'autenticazione dell'incaricato (user-id tipicamente terredacqua\cognome.nome) associato ad una parola chiave riservata (password).

Le credenziali di accesso al sistema e la relativa casella email vengono create dal SIAT a seguito di una richiesta, di norma inoltrata mediante l'apposita procedura informatica, in cui il Dirigente/Responsabile del Settore/Ufficio competente (o suo delegato alla gestione).
Nella richiesta vengono altresì esplicitate le abilitazioni che lo stesso dovrà avere relativamente al sistema gestito mediante Active Directory (cartelle condivise, applicativi e banche dati locali)
L'invio della richiesta al SIAT presuppone che il Dirigente/Responsabile che la inoltra attesti che l'utente abbia titolo ad accedere alla rete e ai dati a cui viene abilitato.
L'incaricato del SIAT crea le relative credenziali Active Directory ed email e comunica, in modo riservato, le password temporanee all'utente, che le dovrà sostituire al primo accesso con quelle definitive.

Può accadere che, per esigenze di servizio, esistano credenziali d'accesso non legate ad un singolo lavoratore e che possono essere condivise da tutto un gruppo di operatori. Queste credenziali non possono consentire l'accesso a banche dati o documenti contenenti dati personali e verranno assegnate unicamente a dipendenti del Comune individuati quali responsabili della gestione della password

## 2.4. Modalità di gestione delle password

Nel caso un utente abbia dimenticato una password, si dovrà rivolgere al SIAT che, previo riconoscimento, provvederà a resettarla e a comunicarla riservatamente all'utente, che, 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 SIAT 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.

Ai sensi di quanto previsto dal punto 10 dell'Allegato B al D. Lgs. 30 giugno 2003, n. 196, gli addetti del SIAT potranno modificare la password degli utenti e comunicare tale nuova password ad un altro utente.
Tale eventualità potrà verificarsi dietro richiesta scritta proveniente dal Responsabile apicale dell'Ufficio/Servizio qualora, in caso di prolungata assenza o impedimento dell'incaricato, sia indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. Qualora si tratti della password di un responsabile apicale di un comune o dell'Unione, la richiesta dovrà pervenire, rispettivamente, dal Sindaco o dal Presidente dell'Unione.
La richiesta dovrà contenere il nome dell'utente di cui va modificata la password, le ragioni che ne rendono indispensabile e indifferibile la modifica e il nome dell'utente a cui la nuova password dovrà essere comunicata.
Il SIAT comunicherà tempestivamente per iscritto all'utente dell'avvenuto cambio password e delle ragioni che lo hanno reso necessario, nonché il nominativo dell'utente a cui la nuova password è stata comunicata.
L'utente dovrà quindi procedere, appena possibile, a modificare la sua password.

## 2.5. Considerazioni generali sulle password

### 1.1.7. Sicurezza e limiti nell'uso delle password

L'utilizzatore ha l'obbligo di impostare la password seguendo la procedura di cambio password nel rispetto della normativa vigente
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.
Architetture in cui gli utenti non eseguano una validazione (logon) ad un dominio e non implementano complete funzionalità di sicurezza non sono e non dovranno più presenti all'interno della rete aziendale.

### 1.1.8. Durata e cambio della password

Ogni utente autorizzato ad accedere alle banche dati ha ottenuto dagli addetti al SIAT un codice identificativo (USER-NAME) ed una parola segreta (PASSWORD) che deve immediatamente cambiare.
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.

### 1.1.9. Requisiti delle password

Gli utenti sono stati 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
- deve presentare differenze significative rispetto alle password per cui non devono ricordare quelle precedenti (Es: con una minima modifica di un solo carattere).
- non deve contenere il nome, il cognome o l'user-name (account utente)
- non deve trattarsi di una parola o di un nome comune

## 2.6. Disattivazione credenziali per disuso.

Nel momento in cui un utente perde il diritto ad accedere alla rete aziendale, il dirigente referente o l'ufficio personale ne comunicano tempestivamente la data di perdita dei requisiti.
Almeno semestralmente viene fatta una verifica straordinaria del permanere, in capo agli utenti abilitati, dei requisiti necessari all'abilitazione onde evidenziare eventuali eventi di cessazione non comunicati.

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.
Per riattivare le credenziali, l'utente dovrà rivolgersi al servizio SIAT che, verificatone il diritto, lo riattiverà con le stesse modalità del caso di "dimenticanza di password"
Periodicamente il SIAT controllerà e disattiverà gli account non utilizzati nei sei mesi precedenti

Il codice di identificazione, laddove inutilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.

# 3. Modalità di gestione delle stazioni di lavoro

## 3.1. Soggetto preposto alla pulizia o recupero delle banche dati su PC

Preposto alla pulizia o recupero delle banche dati su PC è il Responsabile del SIAT che provvederà alla designazione del personale incaricato.

## 3.2. Programmi antivirus

Un software antivirus è installato su tutti i PC, sui server di posta elettronica, sui file server.
Il software antivirus viene aggiornato in maniera automatica ogni qualvolta la casa produttrice rilascia un aggiornamento riguardante la definizione dei virus o l'aggiornamento del software.

Il software produce report dettagliati sulla natura dei Client in rete LAN (utente collegato, Sistema operativo e stato dell'aggiornamento) e sul loro stato di infezione.

Gli utilizzatori di strumenti informatici sono stati informati sul pericolo che i "virus informatici" attacchino i personal computer e ne danneggino il contenuto oltre a propagarsi su altri computer o sui server di rete. Tutti sono tenuti ad utilizzare i programmi di antivirus presenti nell'ente per verificare che i supporti ottenuti dall'esterno, i files ricevuti via e-mail o scaricati da internet, non siano infetti.

Gli utenti non debbono disattivare la procedura di aggiornamento automatico, e non devono disattivare (anche temporaneamente) la funzione di protezione antivirus.

## 3.3. Programmi antispam

La protezione da Spam, è ottenuta tramite un fornitore esterno, che ha la gestione dell'intero sistema di posta elettronica.
Tipicamente le e-mail contenenti virus vengono già eliminate da questo antispam; qualora superassero l'antispam, le e-mail vengono anche sottoposte dal sistema del fornitore ad ulteriore controllo antivirus.
In definitiva una email è soggetta a un sistema antispam e due sistemi antivirus, uno del sistema centralizzato di posta ed uno del pc locale.

## 3.4. Interventi di Manutenzione

Gli interventi di manutenzione sui PC degli utenti vengono di norma effettuati, in remoto o in loco, alla presenza degli assegnatari dei PC stessi.
L'accesso remoto ai PC degli utenti avviene previo consenso espresso da questi ultimi alla richiesta di accesso remoto presentata dal software di controllo.

Nel caso sia necessario inserire la password dell'utente, verrà chiesto a quest'ultimo di digitarla e non dovrà quindi essere comunicata al tecnico.

I tecnici del SIAT o di ditte esterne incaricate della manutenzione dispongono di una password di amministratore del PC che consente l'accesso senza la necessità di conoscere la password dell'utente.

Nel caso il PC debba essere trasferito presso un laboratorio per la sua riparazione, i tecnici incaricati dovranno limitarsi alle sole operazioni tecniche necessarie alla rimozione del guasto e non dovranno accedere in modo generalizzato ai file memorizzati nel disco del PC stesso.

## 3.5. Società esterne o professionisti per la manutenzione e l'assistenza

Il Responsabile del SIAT nomina la società che effettua la manutenzione dei sistemi hardware o software responsabile del trattamento dei dati utilizzando l'apposito modello il quale andrà integrato con

una specifica assunzione di impegno da parte del responsabile stesso al rispetto delle seguenti disposizioni:

- non effettuare copie né procedere alla eliminazione degli archivi informatici di titolarità dell'ente detenuti.
- informare preventivamente gli interessati del giorno e dell'orario in cui saranno effettuati gli interventi tecnici.
- richiedere preventivamente l'autorizzazione ai tecnici del SIAT nel caso di interventi di assistenza tramite collegamento remoto. Gli stessi tecnici dovranno essere avvisati al termine delle operazioni.
- usare riservatezza su dati ed informazioni addivenuti in loro possesso.
- trasmettere al Responsabile del SIAT l'elenco degli incaricati al trattamento e successive variazioni
- trasmettere al Responsabile del SIAT il nominativo degli amministratori di sistema affinché si possa provvedere al loro incarico

### 3.6. Dismissione delle stazioni di lavoro

In caso di dismissione di PC, il SIAT comunica al Responsabile apicale del Servizio l'elenco dei PC da dismettere: questi segnala l'eventuale presenza, su dischi locali degli stessi, di banche dati da recuperare.
Il soggetto preposto, una volta recuperate le banche dati, disinstalla i dischi magnetici dalla postazione di lavoro. La postazione potrà essere smaltita mentre i dischi fissi dovranno essere resi illeggibili prima della rottamazione.
I dischi dei PC usati che eventualmente il Comune dovesse cedere in comodato d'uso, prima della consegna vengono riformattati con modalità sicure, impedendo il recupero di banche dati che vi erano contenute.

## 4. Salvataggio dei dati

Il salvataggio delle banche dati esistenti sui server è in carico all'Ufficio SIAT.
Sui sistemi centralizzati vengono fatte copie quotidiane degli archivi documentali e delle banche dati strutturate allo scopo di fornire almeno una versione aggiornata alla notte precedente.
L'esecuzione dell'operazione di salvataggio è verificata quotidianamente dagli operatori.

In caso di danneggiamento o perdita di dati, gli stessi vengono tempestivamente ripristinati mediante le copie presenti nel sistema di backup.

Ogni singolo lavoratore è invece responsabile dell'effettuazione di copie di sicurezza degli archivi e dei documenti memorizzati unicamente sul proprio PC.

## 5. Locali

La sala macchine dell'Unione dove risiedono fisicamente i server e le librerie a dischi magnetici su cui sono memorizzati i dati degli Enti, è dotata di impiantistica tale da garantire la sicurezza fisica dell'hardware, sia delle banche dati, in particolare:

- porta d'ingresso REI
- stabilizzatore di temperatura per i locali;
- doppio gruppo di continuità e di stabilizzazione della corrente;
- impianto di rilevamento fumi con invio SMS in caso di allarme;
- impianto antintrusione;

La chiave di accesso ai locali della sede centrale è in carico esclusivo al SIAT.
Solo per gestione delle emergenze, una chiave è consegnata presso il servizio Lavori Pubblici del Comune sede del SIAT

Presso ogni comune è presente un CED secondario periferico ubicato in locali chiusi a chiave. Le chiavi di a questi locali sono in carico al comune stesso.

# 6. Cautele generali

## 6.1. Password

Il sistema centralizzato di autenticazione provvede in modo automatico alla scadenza della password
Nel caso in cui le password siano impostate dall'utente in sistemi che non ne prevedano la scadenza temporale, è sua responsabilità provvedere alla loro modifica almeno ogni 90 giorni.

Le password esterne al sistema Active Directory devono rispettare i limiti, la sicurezza e la durata di quelle precedentemente indicate nella sezione "Modalità di gestione delle Password"

## 6.2. Uso del Computer

Il PC non deve essere lasciato incustodito.
In caso di allontanamento anche temporaneo, l'utente attivo al momento deve essere disconnesso o deve essere attivata la modalità salvaschermo con protezione mediante password
Il Dirigente di Settore/Responsabile delegato può impartire ulteriori istruzioni per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di lavoro.
E' impostata a livello centrale, una policy di sicurezza distribuita su tutte le postazioni informatiche che blocca il PC in caso di inattività per 30 minuti. Il nuovo accesso sarà consentito solo con password di Active Directory

## 6.3. Custodia dei supporti

Per motivi di sicurezza e al fine di evitare accessi non autorizzati e trattamenti non consentiti, devono essere impartite, da parte del Responsabile apicale del Settore, le istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili (es: CD, DVD, PenDrive) su cui sono memorizzati i dati.

## 6.4. Supporti ricevuti dall'esterno

Nel caso di supporti ricevuti dall'esterno, come nel caso di allegati ricevuti via e-mail, l'utente deve prestare massima attenzione e sottoporre il supporto a controllo antivirus

# 7. Divieti

| **Divieti per l'utente** | **Chi può fare questa operazione** | **Operazioni preliminari** | **Conseguenze** | **Responsabile nel caso di non rispetto del divieto** |
|---|---|---|---|---|
| Vietato installare programmi | Addetti al S.I. | -Sensibilizzazione e formazione sui rischi e responsabilità.<br>-Verifica compatibilità con i sistemi.<br>-Verifica esistenza di virus informatici.<br>-Verifica della regolare licenza d'uso | -Disinstallazione programma.<br>-Eliminazione virus.<br>Ripristino situazione originale.<br>-Segnalazione al direttore di area. | Consegnatario del computer |
| Vietato disinstallare programmi | Addetti al S.I. | -Sensibilizzazione e formazione sui rischi e responsabilità. | -Ripristino situazione originale.<br>-Segnalazione al direttore di area. | Consegnatario del computer |
| Vietato utilizzare (anche senza | Addetti al S.I. | -Sensibilizzazione e formazione sui rischi e responsabilità. | -Eliminazione programma non regolari senza preavviso.<br>-Eliminazione virus. | Consegnatario del computer |

| | | | | |
|---|---|---|---|---|
| installazione) di programmi non autorizzati dal S.I. | | -Verifica compatibilità con i sistemi.<br>-Verifica esistenza di virus informatici.<br>-Verifica della regolare licenza d'uso | -Ripristino situazione originale.<br>-Segnalazione al direttore di area. | |
| Vietato utilizzare programmi di intercettazione dati diretti ad altri utenti | Nessuno | Sensibilizzazione e formazione sui rischi e responsabilità. | -Eliminazione del programma.<br>-Ripristino situazione originale.<br>-Segnalazione al direttore di area. | Consegnatario del computer |
| Vietato modificare o tentare di modificare la configurazione | Addetti al S.I. | -Sensibilizzazione e formazione sui rischi e responsabilità.<br>-Verifica compatibilità con i sistemi. | -Ripristino situazione originale.<br>-Segnalazione al direttore di area. | Consegnatario del computer |

Il SIAT, in conformità alle disposizioni di legge, provvede alla descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento nell'ambito del piano di disaster recovery.

Il Responsabile apicale del SIAT provvede con propria determinazione a redigere l'elenco degli amministratori di sistema e a designarli individualmente con successivo atto precisandone le funzioni e specificandone l'ambito di attività.
Gli estremi identificativi delle persone fisiche designate, con l'indicazione delle funzioni ad esse attribuite, è riportato in un elenco agli atti del SIAT stesso. Con cadenza annuale il Responsabile del SIAT verifica l'operato degli amministratori di sistema in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali previste dalle normative vigenti.
Il SIAT ha adottato le misure necessarie a consentire un'attività di verifica dell'operato degli amministratori di sistema alla luce delle normative vigenti in merito al trattamento dei dati personali.