S.I.A.T. *Servizi Informatici Associati Terred'acqua*

Comune di Anzola dell'Emilia | Comune di Calderara di Reno | Comune di S.Agata Bolognese | Comune di Sala Bolognese | Comune di S.Giovanni in Persiceto | Comune di Crevalcore

Regolamento sull'utilizzo

degli strumenti informatici

Approvato con deliberazione della Giunta Comunale di Sala Bolognese n. 160 del 13.12.2019

INDICE GENERALE

PARTE I. PRINCIPI E DISPOSIZIONI GENERALI

Art. 1. Oggetto

Il presente Regolamento contiene i principi e le disposizioni in materia di utilizzo degli strumenti informatici, dei prodotti software e di sicurezza dell'informazione, utilizzo della rete TERREDACQUA.local e dei servizi tramite essa erogati o usufruiti.

Art. 2. Ambito di applicazione

Chiunque, pur non trattando dati personali, accede alla rete informatica e telematica e/o utilizza i servizi tramite essa erogati o usufruiti è soggetto al rispetto dei principi e delle prescrizioni contenute nel presente Regolamento.

Art. 3. Finalità

1. Gli Enti promuovono l'utilizzo della rete e dei servizi tramite essa erogati o usufruiti.
2. L'utilizzo dei sistemi informatici e telematici risponde, in ottemperanza al principio di buon andamento dell'azione amministrativa, all'esigenza di dematerializzazione della documentazione cartacea attraverso la progressiva informatizzazione dei procedimenti degli enti. La rete TERREDACQUA.local costituisce uno strumento tecnologico a supporto di tale azione di semplificazione e modernizzazione amministrativa.
3. Il SIAT promuove un approccio metodologico alla tutela dei dati impegnandosi nella realizzazione di un proprio sistema di gestione della sicurezza delle informazioni al fine di assicurare il più elevato livello di protezione del patrimonio informativo degli Enti. Il SIAT si ispira agli standard internazionali e alle metodologie di analisi e gestione del rischio che considerano in modo integrato tutte le componenti della sicurezza dei dati – i dati stessi, le persone, le tecnologie e le procedure – e prevedono la definizione e il coordinamento delle politiche di sicurezza, l'analisi del rischio, l'implementazione di controlli e la verifica periodica dell'efficacia degli stessi.

Art. 4. Definizioni

Ai fini del presente Regolamento si intende per:

a) "rete TERREDACQUA.local", l'insieme di tutte le infrastrutture e le apparecchiature che consentono il collegamento informatico e telematico all'interno del territorio dell'Unione Terre d'Acqua;
b) "Enti" - Comuni di Anzola dell'Emilia, Calderara di Reno, Crevalcore, Sala Bolognese, San Giovanni in Persiceto, Sant'Agata Bolognese e Unione Terre d'Acqua;
c) "SIAT", Servizi Informatici Associati dell'Unione terre d'Acqua - struttura dedicata alla gestione, manutenzione e sicurezza dei sistemi informativi dell'Unione Terre d'Acqua;
d) "Directory Service (DS)", sistema di autenticazione e autorizzazione istituzionale dell'Unione Terre d'Acqua;
e) "file illegale" o "software illegale", i file o i programmi che si pongono in contrasto a principi o prescrizioni sanciti dalla normativa vigente o dal presente regolamento;
f) "dorsale TERREDACQUA.local", l'insieme delle infrastrutture e delle apparecchiature che consentono il collegamento informatico e telematico tra le diverse sedi, nonché l'accesso alle reti telematiche esterne;
g) "Referente informatico", persona fisica che rappresenta il proprio Ente di appartenenza all'interno di tavoli di coordinamento dell'attività informatica organizzati dall'Unione Terre d'Acqua;
h) "gestione automatica delle autorizzazioni tramite sistema d'identificazione centrale (DS)", autorizzazioni all'utilizzo delle risorse gestite in base a criteri oggettivi (ad esempio: la qualifica, l'incarico, l'appartenenza alla struttura) nel sistema d'identificazione centrale (DS) sulla base delle informazioni presenti nelle banche dati dell'Unione Terre d'Acqua o su richiesta degli incaricati dal Titolare del trattamento dei dati (legale rappresentante dell'Ente).

PARTE II. RETE, SERVIZI DI RETE E APPLICAZIONI INFORMATICHE

TITOLO I. PROFILI GENERALI

Art. 5. Principi generali

1. Tutti i servizi informatici e telematici, la posta elettronica, nonché le applicazioni rese disponibili dal SIAT, sono da considerarsi strumento di lavoro per tutto il personale degli Enti, nonché un mezzo per favorire la dematerializzazione dei procedimenti amministrativi e la comunicazione interna ed esterna.
2. L'utilizzo della rete TERREDACQUA.local, dei servizi e delle applicazioni informatiche è consentito esclusivamente nell'ambito dei fini istituzionali degli Enti.
3. Tutte le applicazioni e i sistemi di posta elettronica, ivi compresi quelli gestiti localmente dalle strutture degli Enti, devono essere conformi alle disposizioni di legge e a quelle contenute nel presente Regolamento.

Art. 6. Autenticazione informatica e telematica

1. L'accesso alla rete, ai servizi di rete e alle applicazioni informatiche degli Enti, da parte degli utenti, avviene mediante l'utilizzo delle credenziali di autenticazione appositamente attribuite mediante il Directory Service (DS) o altri dispositivi di identificazione forniti dal SIAT, definiti "credenziali istituzionali".
2. La struttura che rende disponibile agli utenti eventuali applicazioni, servizi o connettività alla rete TERREDACQUA.local, assicura che gli utenti si identifichino secondo quanto indicato al comma 1 del presente articolo e utilizzino, come sistema unitario di identificazione e autorizzazione informatica e telematica, le credenziali istituzionali.
3. Eventuali eccezioni al comma 2 sono valutate, anche per periodi limitati, in accordo con il SIAT.
4. La struttura di cui al comma 1 garantisce l'adozione delle misure di sicurezza definiti dai Titolari degli Enti nel rispetto del principio di Accountability come definito dal GDPR (Regolamento UE 2016/679) e dal D.Lgs. 101/2018.
5. Le credenziali istituzionali sono personali, non cedibili e utilizzabili esclusivamente dal proprietario.
6. Le credenziali istituzionali possono essere attribuite anche a utenti temporanei mediante gli strumenti individuati e messi a disposizione dal SIAT.
7. Le credenziali istituzionali non possono essere assegnate ad altri incaricati, neppure in tempi diversi.

Art. 7. Obblighi dell'utente

1. L'utente è pienamente responsabile delle proprie attività e dei dati trasmessi e/o resi pubblici mediante l'uso delle credenziali istituzionali a lui associate.
2. L'utente è tenuto a conservare segretamente la propria password, a non cederla a terzi e a non lasciare sessioni di lavoro aperte e incustodite.
3. È fatto obbligo all'utente di segnalare al SIAT l'abuso o un eventuale sospetto abuso di utilizzo delle proprie credenziali.
4. In caso di accertato o sospetto furto nonché smarrimento delle credenziali personali, l'assegnatario è tenuto a darne comunicazione tempestiva al SIAT che provvederà immediatamente alla disattivazione e contestuale nuova consegna.

Art. 8. Limiti d'uso

1. In relazione a quanto disposto in via generale dall'Art. 5 comma 2, è vietato, a titolo esemplificativo, usare la rete, i servizi e le applicazioni degli Enti:
    a. per scopi che violino le leggi penali, civili e amministrative in materia di disciplina delle attività e dei servizi svolti sulla rete;
    b. per scopi e/o attraverso modalità contrastanti con il presente Regolamento;
    c. per qualsiasi tipo di uso commerciale non inerente all'attività istituzionale compiuta;
    d. per attività che danneggiano l'immagine e il buon nome degli Enti;
    e. per compiere atti che violino la riservatezza altrui;
    f. per attività che violino le leggi a tutela delle opere dell'ingegno e dei diritti di autore (tra cui

trasferimenti illeciti di software, basi di dati, filmati, musica etc.);

g. per attività non istituzionali che influenzino negativamente la regolare operatività della rete o ne limitino l'utilizzo e le prestazioni per gli altri utenti;

h. per conseguire l'accesso non autorizzato a risorse di rete interne o esterne agli Enti;

i. per attività che distraggano risorse (persone, capacità, elaboratori) dall'utilizzo cui sono state destinate;

j. in modo anonimo o utilizzando risorse che consentano tale uso.

2. L'utente non può svolgere inoltre attività che possano recare danno o pregiudizio agli Enti o a terzi. A titolo esemplificativo, non è consentito utilizzare le reti e i servizi tramite essa erogati o usufruiti per finalità inerenti alla comunicazione e/o diffusione di:

a. pubblicità di prodotti e/o servizi manifesta o occulta;

b. messaggi di carattere commerciale privato;

c. altri contenuti contrari o non conformi alla legge e alle attività istituzionali degli Enti.

3. E' consentita la navigazione internet ad uso personale, purché tale attività avvenga fuori dell'orario di lavoro e sia di modica entità. Anche l'eventuale attività di navigazione personale è soggetta all'applicazione del presente Regolamento.

4. E' vietata la copia dei dati e documenti istituzionali su dispositivi mobili quali pen-drive, dischi esterni, ecc. ed il loro trasferimento all'esterno dei luoghi di lavoro. Ciò costituisce un palese Data-Breach e verrà comunicato al Garante per la Protezione dei Dati Personali

TITOLO II. RETE TERREDACQUA.local

Art. 9. Rete TERREDACQUA.local

1. La rete TERREDACQUA.local rappresenta un servizio fornito all'utenza istituzionale, tecnica e amministrativa, le cui modalità di utilizzo sono regolate dal presente Regolamento e dagli allegati A, B, C e D.

2. La rete TERREDACQUA.local è connessa alla rete Lepida e, tramite quest'ultima, a Internet. Pertanto l'uso delle risorse e dei servizi di Internet tramite la rete TERREDACQUA.local è subordinato al rispetto da parte degli utenti delle norme tecniche dettate dal gestore della connettività.

3. Ogni struttura collegata alla rete TERREDACQUA.local non può essere connessa a reti di altri provider o di organizzazioni esterne, salvo casi eccezionali espressamente autorizzati dal SIAT, che ne verifica la congruenza con le politiche di routing e di sicurezza.

Art. 10. Misure tecniche di sicurezza

1. Conformemente a quanto stabilito nel presente Regolamento e compatibilmente con le risorse finanziarie e di personale disponibili, il SIAT deve, a titolo esemplificativo:

a. garantire la fornitura e la funzionalità dei servizi essenziali di rete;

b. garantire lo sviluppo e la gestione di TERREDACQUA.local, conformemente alle delibere degli Enti;

c. implementare le misure tecniche a protezione dei collegamenti verso l'esterno e della dorsale TERREDACQUA.local;

d. disporre le misure tecniche che gli Enti e/o gli utenti devono adottare al fine di garantire il miglior funzionamento della rete e dei servizi.

Art. 11. Gestione dell'infrastruttura della dorsale TERREDACQUA.local

1. Le politica e la gestione del routing sono di competenza esclusiva del SIAT, così come la gestione delle reti TCP/IP (Internet) e delle relative sottoreti, dei domini DNS di secondo livello di tutti gli Enti e dei relativi sottodomini, del monitoraggio della dorsale TERREDACQUA.local.

PARTE III. CONTROLLI E SANZIONI

Art. 12. Controlli ammessi

1. Il SIAT ha facoltà di effettuare controlli, anche preventivi, sul corretto uso e funzionamento degli strumenti informatici nel rispetto dei diritti e delle libertà fondamentali dei lavoratori o dei soggetti esterni che utilizzano strumenti informatici al fine di evitare usi impropri della rete o dei servizi di rete messi a disposizione.
2. Possono essere effettuati controlli automatizzati sul traffico di rete volti a inibire l'accesso a siti o categorie di siti di palese natura non istituzionale.
3. I controlli sulle attività svolte mediante utilizzo dei sistemi informatici sono ammessi nei seguenti casi:
    a. quando previsti da fonte normativa o regolamentare;
    b. nel caso in cui si verifichino eventi dannosi o situazioni di pericolo non impediti da preventivi accorgimenti tecnici;
    c. su segnalazione dell'Autorità Giudiziaria;
    d. quando, per ragioni di continuità del servizio, sia indispensabile reperire dei file o dei messaggi di un lavoratore, secondo le modalità di cui al comma 5 del presente articolo;
    e. nel caso in cui, nell'ambito delle ordinarie attività di gestione dei sistemi informativi di competenza, siano rilevati file illegali o dal contenuto palesemente non istituzionale;
    f. nell'ambito di controlli saltuari a campione per le finalità di cui al comma 1.
4. Nei casi in cui, a seguito di un controllo, si rilevino comportamenti illegali o non istituzionali, il SIAT o altri soggetti delegati dal Titolare potranno intervenire valutando se:
    a. inviare avvisi collettivi o individuali in cui verranno segnalati i comportamenti non corretti;
    b. rimuovere i file, senza alcun preavviso all'utente, nei casi in cui i file possano limitare l'utilizzo di risorse o possano recar danno agli Enti;
    c. inibire l'accesso a siti o categorie di siti di palese natura non istituzionale;
    d. informare, nei casi in cui i comportamenti non corretti si ripetano nel tempo o risultino particolarmente gravi, i Segretari Generali degli Enti, per i rispettivi ambiti di competenza, che adotteranno i provvedimenti più opportuni.
5. Un Responsabile di servizio, al fine di garantire la continuità lavorativa, può chiedere al SIAT di reperire i file di interesse per l'Ente, giustificando adeguatamente i motivi della richiesta e informando per conoscenza il proprio lavoratore con l'invio di una comunicazione all'indirizzo di posta elettronica personale comunicato all'Ente di appartenenza. Tale richiesta può essere avanzata in caso di:
    a. assenza prolungata di un lavoratore
    b. termine del periodo di collaborazione con l'Ente

Art. 13. Sanzioni

1. I comportamenti in violazione della normativa vigente e del presente Regolamento che hanno una rilevanza disciplinare, fermi restando i diversi profili di responsabilità civile e penale, saranno sanzionati secondo le forme e le modalità previste dai rispettivi ordinamenti del personale coinvolto.
2. Tali comportamenti sono segnalati al Dirigente o al Segretario Generale che valuterà le modalità di intervento più idonee, anche a tutela di eventuali danni economici e/o di immagine subiti dal'Ente.
3. Salvo quanto previsto nell'Art. 13 dell'Allegato B, nel caso di necessità e di urgenza e al fine di evitare compromissioni al normale funzionamento della rete o porre termine ad attività contrarie alla normativa vigente o al presente Regolamento, il Direttore del SIAT potrà disporre con proprio atto la sospensione temporanea dell'accesso alla Rete TERREDACQUA.local o ai servizi, a un utente o a un gruppo di utenti, fino alla rimozione delle cause che hanno originato il problema.

PARTE IV. DISPOSIZIONI ABROGATIVE E INTEGRATIVE

Art. 14. Disposizioni abrogative

1. Dalla data di entrata in vigore del presente Regolamento sono sostituiti integralmente tutti i precedenti regolamenti relativi all'utilizzo degli strumenti informatici già approvati dalla Giunta .

Art. 15. Disposizioni integrative

1. Sono da considerarsi parte integrante al presente Regolamento i seguenti documenti:
   ALLEGATO A. Disciplinare per il corretto uso delle credenziali
   ALLEGATO B. Disciplinare tecnico in materia di accesso e utilizzo della rete TERREDACQUA.local
   ALLEGATO C. Disciplinare per l'utilizzo della posta elettronica
   ALLEGATO D. Disciplinare di utilizzo dei servizi internet
   ALLEGATO E. Categorie di filtraggio dei siti web
   ALLEGATO F. Elenco delle tipologie di file bloccati in download da internet
   ALLEGATO G. Istruzioni operative per la cancellazione della cronologia delle pagine web visitate
   ALLEGATO H. Istruzioni operative per la cancellazione della memoria cache delle pagine web visitate
   ALLEGATO I. Istruzioni operative per la cancellazione dei cookie
   ALLEGATO J. Istruzioni operative sull'utilizzo del software Anti-Virus

Art. 16. Entrata in vigore

1. Il presente Regolamento entra in vigore dalla data di approvazione da parte della Giunta

Allegato A. DISCIPLINARE PER IL CORRETTO TRATTAMENTO DELLE CREDENZIALI ISTITUZIONALI

Art. 1. Utenti e convenzioni sui nomi

1. Le credenziali istituzionali, salvo casi di omonimia, possono essere fornite nella forma nome.cognome alle seguenti categorie di soggetti:
    a. Personale dipendente degli Enti;
    b. Amministratori degli Enti;
    c. Collaboratori e consulenti titolari di un contratto con gli Enti;
    d. Altre forme di collaborazione in cui l'attività lavorativa sia prevalentemente svolta presso gli Enti.
2. Per scopi di mera gestione tecnica e accesso a servizi informatici da parte di altre applicazioni informatiche sono fornite credenziali, dette di servizio, nella forma <descrizioneservizio>@terredacqua.net.
3. Nelle credenziali indicate ai commi precedenti, il prefisso «nome.cognome» può subire aggiustamenti per motivi organizzativi (es.: casi di omonimia) o tecnici (es.: eccessiva lunghezza del nome o del cognome rispetto agli standard informatici), salvaguardando, in ogni caso, la piena riconoscibilità del soggetto.
4. Eventuali deroghe alle convenzioni sui nomi devono essere concordate con il SIAT, compatibilmente con eventuali vincoli tecnologici.
5. Il SIAT valuta l'opportunità di assegnazione di altre tipologie di account per particolari esigenze organizzative e/o tecniche.

Art. 2. Obblighi inerenti alle password

1. È fatto obbligo all'utente di:
    a. utilizzare password composte da almeno otto caratteri alfanumerici e simboli speciali, non contenenti riferimenti agevolmente riconducibili all'incaricato;
    b. modificare la propria password al primo utilizzo;
    c. cambiare la propria password almeno ogni 90 giorni.
2. Il SIAT, mediante i sistemi di autenticazione forniti centralmente, può implementare meccanismi per il cambio password obbligatorio, anche con scadenze più restrittive di quelle previste al comma 1 lettere c) e d).

Art. 3. Richiesta delle credenziali istituzionali

1. La richiesta di credenziali per l'accesso di un nuovo utente alla rete TERREDACQUA.local deve essere effettuata dal Titolare del Trattamento o suo delegato (Responsabile o Dirigente) compilando il modulo pubblicato sulla intranet http://intranet.terredacqua.local ed allegarlo ad un ticket utilizzando la piattaforma in uso http://srvassistenza/glpi
2. Lo username e la password temporanea verranno comunicate al richiedente che avrà cura di consegnarle direttamente al nuovo utente.
3. Il nuovo utente dovrà autenticarsi quanto prima e verrà obbligato a sostituire la password temporanea con una propria.

Art. 4. Disattivazione delle credenziali istituzionali

1. Le credenziali di autenticazione sono disattivate dal SIAT al termine del rapporto di lavoro o collaborazione con gli Enti.
2. E' compito del Responsabile o Dirigente del servizio, comunicare al SIAT quando un'utenza deve essere disattivata per le ragioni di cui al comma 1;
3. Le credenziali di autenticazione sono disattivate dopo due mesi di inutilizzo da parte dell'utente a cui sono state assegnate;
4. La riattivazione delle credenziali è eseguita dal SIAT su richiesta dell'interessato, nei casi in cui esse siano associate a un dipendente in servizio che non ne abbia fatto uso per un periodo maggiore di due mesi;
5. Le credenziali sono altresì disattivate nei casi e con le modalità di cui all"Art. 13 comma 3 del presente Regolamento.

Art. 5. Cancellazione delle credenziali

1. La cancellazione delle credenziali può essere effettuata:
   a. decorsi tre mesi dalla disattivazione delle credenziali nei casi in cui il soggetto titolare delle stesse sia deceduto o ne sia dichiarata la morte presunta;
   b. nei casi di credenziali istituzionali create dal SIAT e assegnate a persone fisiche per brevissimi periodi o per gestione tecnica, entro un termine non eccedente rispetto alle finalità per le quali si è fornito l'account.

Art. 6. Autorizzazione a risorse informatiche

1. La concessione del diritto di un soggetto incaricato al trattamento ad accedere a una o a più risorse informatiche dell'Ente, in cui la profilazione dei diritti d'accesso per l'utente non sia gestita automaticamente dal sistema di identificazione centrale (DS) bensì localmente alla risorsa in oggetto, deve essere valutata dal relativo Responsabile di trattamento (o persona da lui delegata per tale attività).
2. L'attribuzione delle credenziali e dei relativi profili di accesso, per i soggetti di cui al comma 1 del presente articolo, vengono assegnate direttamente dal Responsabile di trattamento (o persona da lui delegata per tale attività).
3. L'accesso alle risorse informatiche degli Enti è consentito agli utenti abilitati in relazione al ruolo ricoperto, per il solo periodo di durata del rapporto con l'Ente e, nei casi di cui al comma 3, non oltre i termini di disattivazione delle credenziali.
4. Costituiscono eccezione al comma di cui sopra:
   a. l'utilizzo della posta elettronica, come regolato nell"Allegato C;
   b. l'abilitazione a connettersi a internet, come regolato nell'Allegato B;
   c. l'accesso o l'utilizzo di specifici servizi o applicazioni, espressamente individuati dal SIAT e inerenti al rapporto di lavoro con gli Enti (Es: Presenze Web).

Allegato B. DISCIPLINARE IN MATERIA DI ACCESSO E UTILIZZO DELLA RETE TERREDACQUA.local

PARTE I. IDENTIFICAZIONE DELL'UTENTE IN RETE

Art. 1. Validità dell'autorizzazione ad accedere alla rete TERREDACQUA.local

1. L'autorizzazione a connettersi sulla Rete TERREDACQUA.local mediante i punti di accesso wired (via cavo) resi disponibili dagli Enti è concessa agli utenti per un tempo non eccedente rispetto alle finalità per le quali tale autorizzazione è stata concessa;
2. L'abilitazione o il prolungamento, alla scadenza, dell'autorizzazione al servizio di connettività tramite la rete TERREDACQUA.local può essere effettuata solo per motivi legittimi e su richiesta motivata del proprio Dirigente o Responsabile di Servizio.

Art. 2. Accesso remoto alla Rete TERREDACQUA.local

1. Su richiesta del Dirigente o Responsabile di servizio, l'accesso remoto agli applicativi gestionali è consentito utilizzando l'infrastruttura di virtualizzazione Citrix che risponde all'indirizzo https://datacenter.terredacqua.net:4443;
2. Non è consentito l'accesso remoto alla Rete TERREDACQUA.local via modem.

PARTE II. MISURE TECNICHE E ORGANIZZATIVE

TITOLO I. RETI

Art. 3. Gestione degli indirizzi IP

1. Il SIAT sovrintende all'indirizzamento IPv4 sia pubblico che privato (RFC1918) all'interno della rete TERREDACQUA.local, nonché all'indirizzamento globale IPv6 (RFC3513).
2. Le reti IPv4 pubbliche assegnate alla rete TERREDACQUA.local sono gestite dal SIAT ed assegnate da Lepida SpA;
3. L'indirizzo IP viene assegnato dal SIAT in maniera statica o dinamica ed è espressamente vietata all'utente l'autoassegnazione dell'indirizzo IP.

Art. 4. Dynamic Host Configuration Protocol (DHCP)

1. E' vietato attivare qualunque dispositivo abilitato al rilascio automatico di indirizzi IP (DHCP) senza l'autorizzazione del SIAT.

TITOLO II. SERVIZI

Art. 5. Gestione e implementazione dei servizi di rete della propria struttura

1. Un Ente che ritiene necessaria l'attivazione di un servizio informatico non fornito dal SIAT o di un servizio che, sebbene sia disponibile attraverso il SIAT, abbia funzionalità non coincidenti con quelle fornite, comunica tale esigenza al SIAT evidenziando gli obiettivi che intende raggiungere mediante tale attivazione.
2. Il SIAT, a seguito di tale comunicazione, può provvedere a:
    a. programmare l'implementazione dei nuovi servizi richiesti, laddove si rilevi un interesse concreto e diffuso;
    b. estendere le funzionalità di servizi già esistenti;
    c. consigliare alle strutture l'utilizzo di servizi già implementati o in fase di implementazione anche in altri Enti;
    d. declinare, fornendo adeguate giustificazioni, la richiesta di attivazione del nuovo servizio.

Art. 6. Utilizzo dei servizi wireless

1. I servizi wireless sono interamente gestiti da Lepida S.p.A. che mette a disposizione l'SSID "*EmiliaRomagnaWiFi wifiprivacy.it*";
2. Oltre a quanto stabilito per le reti cablate, la rete wireless deve essere usata secondo le modalità del presente Regolamento, nonché in osservanza di quanto stabilito dall'ordinamento.
3. La rete wireless consente il solo accesso alla rete internet e per connettersi alla rete TERREDACQUA.local occorre attenersi a quanto descritto nell'art. 2 dell'Allegato B;
4. L'Ente che intende implementare o estendere il servizio wireless è tenuto a darne comunicazione al SIAT che, a seguito di tale comunicazione, assume il compito di verificarne la conformità alla normativa e al presente Regolamento. Il SIAT ha altresì il compito di autorizzare preventivamente il posizionamento degli apparati nelle diverse sedi degli Enti affinché non si generino interferenze che possano compromettere il buon funzionamento di impianti preesistenti.
5. E' vietato collegare alla rete TERREDACQUA.local apparati non autorizzati che distribuiscono il servizio WiFi. Opportuni sistemi di controllo e prevenzione sono attivati dal SIAT al fine di individuare e bloccare tempestivamente tali comportamenti scorretti.

Art. 7. Utilizzo di cartelle condivise e spazi di rete personali

1. Il SIAT può mettere a disposizione degli utenti, cartelle di rete a uso esclusivo o condiviso ovvero unità di memoria accedibili dall'interno della Rete TERREDACQUA.local, mediante le quali è possibile condividere e/o conservare file inerenti alla propria attività lavorativa che vengono memorizzate su di un file server.
2. Tali spazi possono essere utilizzati esclusivamente per finalità istituzionali. Qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità.
3. Sulle cartelle in oggetto vengono svolte regolari attività di controllo, amministrazione e backup da parte dell'amministratore di sistema (o da suoi delegati). L'amministratore (o i suoi delegati) ha visibilità delle cartelle ed è autorizzato a cancellare i file solo nei casi di evidente natura non istituzionale.
4. L'amministratore di sistema (o suoi delegati) è tenuto al backup delle sole informazioni di natura istituzionale presenti sul file server mentre altre unità di memorizzazione a uso personale, come ad esempio il disco rigido della propria postazione di lavoro o dischi rigidi esterni, non sono soggetti a backup e, pertanto, la responsabilità del salvataggio dei dati ivi contenuti è a carico del singolo utente.
5. Per i servizi di cui al comma 1, entro sei mesi dalla conclusione del rapporto di collaborazione dell'utente con l'Ente, saranno cancellati tutti i file contenuti nelle cartelle a uso esclusivo.

Art. 7bis. Utilizzo delle cartelle cifrate condivise

1. Il SIAT mette a disposizione degli utenti, cartelle di rete a uso condiviso e cifrato, ovvero unità di memoria accedibili dall'interno della Rete TERREDACQUA.local, mediante le quali è possibile condividere e/o conservare file contenenti dati personali e/o sensibili, inerenti la propria attività lavorativa e che abbiano la necessità di essere memorizzati su di un file server in ottemperanza dell'Art. 32 comma 1 lettera A del Regolamento Europeo per la Protezione dei Dati 2019/679 (GDPR).
2. Tali spazi cifrati devono essere utilizzati esclusivamente per gli scopi di cui al comma 1 del presente articolo.

Art. 8. Utilizzo postazioni di lavoro

1. Per garantire una maggiore sicurezza dei sistemi, non è consentito agli utenti di installare e utilizzare, nelle postazioni di lavoro, software illegale, freeware, shareware o espressamente vietato dall'amministratore di sistema.
2. Nell'eventualità si rilevi, anche mediante sistemi inventariali di software, l'esistenza di programmi che violino il diritto d'autore, il SIAT agisce nel rispetto degli artt. 12 e 13 del Regolamento;
3. Le postazioni sono sostituite dall'amministratore di sistema nei casi in cui, per motivi di sicurezza o affidabilità, si renda necessaria la sostituzione del computer. In tali casi saranno correttamente trasferiti sulla nuova postazione i soli dati di rilevanza istituzionale.

Art. 9. Utilizzo dei dispositivi mobili

1. I dispositivi notebook forniti dagli Enti saranno provvisti di disco crittografato ed equipaggiati da opportuni sistemi di gestione remota. In caso di smarrimento o furto dovrà esserne data immediata comunicazione al SIAT che attiverà tutte le procedure necessarie al fine di ridurre al minimo la possibilità di esfiltrazione di dati;
2. I dispositivi mobili come tablet e/o smartphone aziendali dovranno essere consegnati al SIAT per l'installazione dei necessari prodotto di cifratura e protezione. Dovranno avere l'accesso protetto con la massima opzione disponibile (riconoscimento facciale, impronta digitale, pin, ecc.). In caso di smarrimento o furto dovrà esserne data immediata comunicazione al SIAT che attiverà tutte le procedure necessarie al fine di ridurre al minimo la possibilità di esfiltrazione di dati;
3. I dispositivi mobili come tablet e/o smartphone personali che vengano utilizzati per l'accesso alla casella di posta istituzionale dovranno avere l'accesso protetto con la massima opzione disponibile (riconoscimento facciale, impronta digitale, pin, ecc.). In caso di smarrimento o furto dovrà esserne data immediata comunicazione al SIAT che provvederà tempestivamente a bloccare l'account di posta elettronica al fine di ridurre al minimo la possibilità di esfiltrazione di dati;

Art. 10. Cancellazione di file e messaggi di un utente deceduto

1. I messaggi contenuti nella casella di posta elettronica di un utente deceduto o del quale è stata dichiarata la morte presunta o eventuali file contenuti nella sua postazione di lavoro saranno resi accessibili dalla struttura che la gestisce solo per ragioni di continuità del servizio, secondo le finalità di cui all'Art. 12 comma 5 e, comunque, entro i termini di cui all'Art. 4 comma 1 dell'allegato A.
2. Eventuali file o messaggi contenuti nella posta elettronica di un utente deceduto o del quale è stata dichiarata la morte presunta, nella sua postazione di lavoro o negli spazi di rete personali saranno eliminati dal SIAT contestualmente alla cancellazione delle credenziali.
3. Eventuali file riconducibili a un utente deceduto o del quale è stata dichiarata la morte presunta potranno essere conservati dal SIAT per un periodo superiore a quello previsto al comma 2 e al comma 3 del presente articolo, su richiesta dell'Autorità Giudiziaria, di chi ha un interesse proprio, di chi agisce a tutela dell'interessato o per ragioni familiari meritevoli di protezione. Tale richiesta dovrà essere inviata per iscritto all'Ente entro sei mesi dalla morte dell'utente.

TITOLO III. SICUREZZA E GESTIONE DEGLI INCIDENTI

Art. 11. Politiche di sicurezza sulla rete TERREDACQUA.local

1. Il SIAT implementa le politiche di sicurezza perimetrali e sulla dorsale della rete TERREDACQUA.local.
2. L'accesso alla rete TERREDACQUA.local è protetto mediante l'uso di firewall e/o di altri apparati di rete che implementano regole di controllo del traffico finalizzate a migliorare e garantire la continuità del servizio di connettività alla rete TERREDACQUA.local.
3. Il SIAT configura gli apparati di rete posti sul bordo della rete TERREDACQUA.local bloccando l'accesso a qualunque connessione proveniente dall'esterno, ad eccezione delle connessioni verso gli host e i servizi necessari allo svolgimento delle attività istituzionali degli Enti.
4. Il SIAT concede l'accesso agli host e servizi di cui al comma 3 dopo avere effettuato un vulnerability assessment sui sistemi in oggetto e aver verificato l'assenza di vulnerabilità manifeste. La connessione è fornita solo a seguito della risoluzione di eventuali vulnerabilità.
5. Il SIAT, che durante l'attività di monitoraggio (costituita anche da vulnerability assessment periodici) rilevi delle vulnerabilità di un sistema, comunica al Titolare della protezione dei dati, la necessità di attuare degli interventi correttivi comunicando anche le eventuali risorse economiche necessarie. Nel caso in cui si presentassero difficoltà, anche temporanee, che impediscano l'applicazione degli interventi correttivi, il SIAT può intervenire interrompendo la connettività del sistema in oggetto.

Art. 12. Rilevazione delle intrusioni

1. Il SIAT utilizza sistemi di rilevamento delle intrusioni, software e hardware, localizzati sulla rete

TERREDACQUA.local. Tali sistemi sono adottati dal SIAT al solo fine di identificare eventuali accessi non autorizzati ai computer e alle reti locali degli Enti e di intervenire nel caso di compromissioni.

2. I sistemi di rilevamento delle intrusioni possono essere utilizzati dal SIAT per reagire in tempo reale agli attacchi in corso.

3. Durante tali attività, pur potendo acquisire informazioni personali e non, anche riservate, che transitano sulla rete TERREDACQUA.local, i componenti del SIAT non possono raccogliere, copiare, registrare, organizzare, conservare, estrarre, comunicare, diffondere alcun dato personale ad eccezione di quelli strettamente necessari al perseguimento delle finalità indicate al comma 1 e salvo i casi espressamente previsti dalla legge o dai regolamenti.

Art. 13. Modalità di gestione degli incidenti

1. Le attività di monitoraggio della dorsale TERREDACQUA.local e di rilevazione di anomalie si svolgono sotto la responsabilità del SIAT, cui compete di norma la notifica di apertura dell'incidente. Questa avviene attraverso la segnalazione al Titolare e al Data Protection Officer (DPO) il quale valuterà se inviare adeguata comunicazione al Garante per la Protezione dei Dati. Di tale intervento è responsabile l'Amministratore di Sistema, che ha l'obbligo di provvedere al distacco dalla rete di singoli utenti o di porzioni della rete, sino alla rimozione delle cause che hanno originato il problema. L'Amministratore di Sistema può delegare l'esecuzione tecnica di tali procedure ad altri collaboratori. A seguito di tali adempimenti il SIAT, dopo gli opportuni controlli, potrà dichiarare la chiusura dell'incidente. In casi di necessità e urgenza, al fine di evitare compromissioni al normale funzionamento della rete o porre termine ad attività contrarie alla normativa vigente o al presente Regolamento, il distacco di un utente o di una porzione di rete può essere effettuato dal SIAT che ne darà comunicazione immediata all'Amministratore di Sistema.

2. Il Referente informatico di ogni Ente, qualora rilevi delle anomalie, ha l'obbligo di darne comunicazione tempestiva al SIAT, secondo le indicazioni che saranno comunicate dal SIAT stesso. La chiusura dell'incidente si svolge nelle modalità indicate nel comma 1 del presente articolo.

PARTE III. TRATTAMENTO DEI DATI DI TRAFFICO TELEMATICO

Art. 14. Ambito di trattamento

1. Il SIAT, per obblighi di legge o di regolamenti, è tenuto al mantenimento dei log file (registri informatizzati che tengono traccia delle connessioni degli utenti e dei servizi da essi acceduti). Tali dati sono trattati conformemente alla normativa.

2. Il personale del SIAT che tratta i dati di cui al comma 1 è stato incaricato dal Responsabile con apposito documento di nomina come definiti dal Regolamento UE 2016/679 (GDPR) e D.Lgs 101/2018 e contenenti:

   a. le finalità e le modalità della conservazione dei dati di traffico telematico;
   b. le categorie di soggetti che detengono i log file;
   c. l'identificazione del Titolare e dei Responsabili;
   d. i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o i soggetti esterni che possono venirne a conoscenza;
   e. gli obblighi a cui attenersi durante il trattamento.

Art. 15. Modalità di conservazione

1. Per una corretta registrazione dei log file, la struttura è obbligata a sincronizzare i propri server mediante NTP con i time server individuati e resi noti dal SIAT

2. Le modalità di conservazione dei file di log, le specifiche sulle informazioni da conservare nonché l'individuazione delle misure di sicurezza a tutela dei dati sono definite dal Garante per la Protezione dei Dati Personali e dalla normativa vigente.

Allegato C. DISCIPLINARE PER L'UTILIZZO DELLA POSTA ELETTRONICA

Art. 1. Oggetto e finalità

1. Il SIAT, rende disponibile al personale ed amministratori degli Enti, un indirizzo di posta elettronica istituzionale.
2. Le comunicazioni ufficiali e istituzionali da parte degli Enti sono inviate esclusivamente all'indirizzo di posta istituzionale di cui al comma 1 del presente articolo; è fatto obbligo a ogni utente di utilizzare tale casella di posta.
3. L'utilizzo degli indirizzi di cui al comma 1 del presente articolo costituisce "trattamento dei dati personali" e, pertanto, da conformarsi alle disposizioni del Regolamento UE 2016/679 e D.Lgs. 101/2018.

Art. 2. Soggetti utilizzatori del servizio di posta elettronica

1. Tutti gli utenti definiti all'Art. 1 comma 1 e 2 dell'Allegato A possono accedere al servizio di posta elettronica utilizzando le credenziali a loro assegnate.
2. Nel caso di assenza programmata, il dipendente è tenuto ad attivare sistemi di risposta automatica ai messaggi di posta elettronica ricevuti, nei quali indicherà eventuali indirizzi istituzionali alternativi ai quali fare riferimento per l'invio di comunicazioni.
3. Al fine di agevolare la comunicazione istituzionale e favorire la circolazione delle informazioni, sono altresì forniti indirizzi per unità/strutture organizzative o indirizzi legati alla carica, utilizzati prevalentemente per liste di distribuzione o caselle di posta elettronica, il cui accesso è consentito a uno o più lavoratori. A titolo esemplificativo, l'account di posta elettronica può essere fornito a:
    a. Uffici, nella forma <acronimo ufficio>@<ente>.it;
    b. Carica, nella forma <carica>@<ente>.it;

Art. 3. Gestione tecnica del servizio

1. Il SIAT implementa misure di protezione automatizzate antivirus e antispam per il servizio di posta istituzionale, decidendone le tecnologie e le modalità operative, per contrastare la ricezione di messaggi di posta elettronica non desiderati contenenti virus, comunicazioni e/o materiali pubblicitari o altro materiale dal contenuto potenzialmente dannoso.
2. Il SIAT decide le politiche di backup dei messaggi di posta.
3. Il SIAT, pur adottando tutte le misure tecniche ritenute necessarie e sufficienti a minimizzare il rischio di perdita di informazioni di interesse dell'utente, non può essere ritenuto responsabile dell'eventuale cancellazione, danneggiamento, mancato invio, mancata ricezione o ritardo nella consegna di messaggi, se dovuti a malfunzionamenti o a guasti dei sistemi di posta, dei sistemi di protezione e di backup.
4. Il SIAT si impegna ad adottare delle soluzioni tecniche che limitino la cancellazione immediata dei messaggi di posta identificati come spam, entro i limiti consentiti dall'infrastruttura adottata e salvaguardando, per quanto possibile, l'operatività degli utenti.

Art. 4. Validità dei profili autorizzativi per l'uso del servizio di posta elettronica

1. Il servizio di posta elettronica istituzionale sarà disattivato contestualmente il termine del rapporto con Ente.
2. Costituiscono eccezione al predetto termine i seguenti casi:
    a. per gli amministratori, il servizio sarà disattivato su richiesta esplicita dell'interessato a seguito dell'interruzione della carica di Amministratore o, comunque, nei tempi e con le modalità definite dal SIAT, funzionali alla sostenibilità della gestione del servizio, e opportunamente rese note all'utente;
    b. per i dirigenti e responsabili di area, il servizio sarà disattivato su richiesta esplicita dell'interessato a seguito dell'interruzione rapporto di lavoro o collaborazione, comunque, nei tempi e con le modalità definite dal SIAT, funzionali alla sostenibilità della gestione del servizio, e opportunamente rese note all'utente; per i dipendenti il servizio sarà disattivato al momento della disattivazione delle credenziali;

c. nel caso di soggetti deceduti, il servizio verrà disattivato entro un mese dalla notifica al SIAT dell'avvenuto decesso.

3. La cancellazione di tutti i messaggi contenuti nella casella disabilitata avverrà dopo due mesi dalla disattivazione del servizio di posta elettronica. Verranno conservate le copie di backup delle caselle disabilitate su richiesta del relativo Dirigente/Responsabile di servizio.

4. Su richiesta motivata del relativo Dirigente/Responsabile di servizio, il SIAT può autorizzare l'accesso ad una casella di posta istituzionale ad altri utenti dandone immediata informazione al diretto interessato, qualora assente per lunghi periodi.

5. Per i casi non contemplati nel presente Regolamento, il SIAT individua le politiche di disattivazione del servizio di posta elettronica e di cancellazione dei messaggi.

Art. 5. Utilizzo della posta elettronica da parte degli utenti

1. La posta elettronica istituzionale è da considerarsi quale necessario strumento di lavoro e pertanto non deve essere utilizzata per scopi personali.

2. La posta elettronica è un servizio consultabile via web e non ne è autorizzata la consultazione utilizzando software quali Outlook®, Thunderbird®, ecc.

3. La posta elettronica, per via delle caratteristiche di sicurezza e tecnologiche intrinseche al servizio stesso, non è in alcun modo da considerare quale metodo di archiviazione di documenti. Deve essere considerata come canale di interscambio di corrispondenza e comunicazione e, pertanto, tutti i documenti allegati o comunicazioni contenenti informazioni personali o sensibili, devono essere scaricati e memorizzati sui fileserver a disposizione di tutti gli utenti i quali rispondono a tutti i requisiti di sicurezza richiesti.

4. Nell'invio di una comunicazione a più di un utente esterno contemporaneamente, è buona consuetudine inserire l'indirizzo email dei destinatari nel campo Ccn: (Copia carbone nascosta) per garantire la riservatezza degli indirizzi dei destinatari;

5. Nel caso di invii di cui al comma 2 è opportuno ricordare che il campo A: che identifica il destinatario, va comunque compilato inserendo un indirizzo email valido (es. il proprio indirizzo) per evitare che il messaggio venga intercettato dalle sonde anti-spam;

Allegato D. DISCIPLINARE DI UTILIZZO DEI SERVIZI INTERNET

Art. 1. Utilizzo dei programmi che fanno uso di internet

1. Il SIAT mette a disposizione dei lavoratori i programmi necessari per navigare in internet ed utilizzare i servizi internet necessari per l'attività lavorativa. Tali programmi sono stati testati e validati dal SIAT. Onde evitare problemi di malfunzionamento, sicurezza e instabilità dei sistemi, i lavoratori sono tenuti ad utilizzare solamente il software fornito. L'elenco dei programmi a disposizione dei lavoratori per la navigazione in internet comprende:
   - Microsoft Internet Explorer
   - Microsoft Edge
   - Google Chrome
   - Mozilla Firefox

2. Per la navigazione internet il lavoratore deve attenersi alle seguenti regole:
   - non è consentita la navigazione in siti i cui contenuti siano compresi nelle categorie di filtraggio di cui all'ALLEGATO E - CATEGORIE DI FILTRAGGIO DEI SITI WEB del presente disciplinare;
   - non è consentito l'utilizzo di servizi web proxy o di servizi web di anonimizzazione al fine di eludere i filtri e le regole di sicurezza implementate dall'Unione Terre d'Acqua;
   - non è consentito il download, la copia, il salvataggio, l'installazione o l'utilizzo di software prelevato da siti internet, se non espressamente autorizzato dall'Amministratore di Sistema;
   - non è consentito l'uso di software di condivisione di risorse (peer to peer o shared);
   - non è consentito l'uso di software di telefonia su ip (VOIP) e di instant messaging se non espressamente autorizzati dall'Amministratore di Sistema;
   - è vietata ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa a nome dell'Ente di appartenenza fornendo i dati relativi a e-mail istituzionale;
   - non è permessa la partecipazione per motivi non professionali a forum, l'utilizzo di chat line, di bacheche elettroniche e le registrazioni in guest book nemmeno utilizzando pseudonimi (o nicknames);
   - non sono consentiti il download, la copia o il salvataggio di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;
   - ferme restando le attività dell'Amministratore di Sistema di implementazione, configurazione e gestione dei software antivirus presenti nel sistema informatico, spetta al lavoratore sottoporre a verifica tutti i file di provenienza incerta o esterna scaricati da internet, ancorché attinenti all'attività lavorativa, tramite gli strumenti antivirus in dotazione. Le istruzioni operative sull'utilizzo del software antivirus sono contenute nell'ALLEGATO J - ISTRUZIONI OPERATIVE SULL'UTILIZZO DEL SOFTWARE ANTIVIRUS al presente disciplinare.

Art. 2. Strumento di web / e-mail content filter

L'Unione Terre d'Acqua, onde garantire che le descritte policy per l'utilizzo di Internet siano effettivamente rispettate dai lavoratori, si è dotato di strumenti finalizzati a prevenire un utilizzo indebito dei servizi Internet mediante azioni di filtraggio, in relazione sia alla navigazione che all'utilizzo dell'e-mail.

1. Navigazione web e programmi Internet

Con riferimento alla navigazione su Internet, il Unione Terre d'Acqua utilizza software implementati sui firewall che presidiano la rete TERREDACQUA.local. Tale strumento è configurato per effettuare:

2. Azioni di filtraggio dei siti web

L'elenco delle categorie di filtraggio dei siti web è contenuto nell'ALLEGATO E - CATEGORIE DI FILTRAGGIO DEI SITI WEB al presente disciplinare.

3. Blocco dei servizi/applicativi Internet indesiderati

Ad eccezione della navigazione in internet (su porte 80-HTTP e 443-HTTPS) sono bloccati gli accessi a tutti i servizi internet (es: instant messaging, voip, skype, peer to peer, giochi on line, ecc.) ad eccezione di quelli autorizzati dall'Amministratore di Sistema. E' possibile la navigazione su alcune porte non standard che verranno abilitate per consentire l'accesso a particolari servizi on-line.

4. Blocco del download di file per tipologia

L'elenco delle tipologie di file bloccati in download da internet è contenuto nell'ALLEGATO F - ELENCO DELLE TIPOLOGIE DI FILE BLOCCATI IN DOWNLOAD DA INTERNET al presente disciplinare.

Art. 3. Dati conservati dal sistema relativamente all'utilizzo degli strumenti elettronici

1. Navigazione internet
   - I log di navigazione rilevati dai sistemi di sicurezza vengono generati, salvati in file giornalieri e conservati in copia di backup su disco per un massimo di 180 giorni. L'intero processo è svolto dal sistema informatico in forma totalmente automatica.
   - Sono generati i seguenti tipi differenti di log giornalieri di navigazione:
     1. Log giornalieri di navigazione generati in forma anonima: i sistemi di sicurezza generano log giornalieri di navigazione in forma anonima per poter produrre statistiche aggregate utili ai fini di manutenzione, sviluppo e aggiornamento del sistema informatico.
     2. Log giornalieri di navigazione generati in forma che identifica la postazione di lavoro: i sistemi di sicurezza generano anche log giornalieri di navigazione in forma nominativa per le verifiche di eventuali comportamenti anomali allo scopo di far cessare una o più violazioni al presente disciplinare nel rispetto dei principi di pertinenza e non eccedenza e soprattutto di gradualità dei controlli.
   - Tutti i log giornalieri di navigazione vengono archiviati e sono accessibili esclusivamente dall'Amministratore di Sistema e dagli incaricati del SIAT designati.
2. Cronologia delle pagine web visitate
   - La cronologia delle pagine web visitate è memorizzata nel profilo dei singoli lavoratori e conservata in locale sul computer utilizzato per quanto riguarda la navigazione effettuata dal computer stesso.
   - E' possibile la cancellazione a carico del singolo lavoratore come da procedura contenuta nell'ALLEGATO G - ISTRUZIONI OPERATIVE PER LA CANCELLAZIONE DELLA CRONOLOGIA DELLE PAGINE WEB VISITATE al presente disciplinare.
3. Memoria cache delle pagine web visitate
   - La memoria cache delle pagine web visitate è memorizzata nel profilo dei singoli lavoratori e conservata in locale sul computer utilizzato per quanto riguarda la navigazione effettuata dal computer stesso. E' possibile la cancellazione a carico del singolo lavoratore come da procedura contenuta nell'ALLEGATO H - ISTRUZIONI OPERATIVE PER LA CANCELLAZIONE DELLA MEMORIA CACHE DELLE PAGINE WEB VISITATE al presente disciplinare.
4. Cookies
   - I cookies, ossia le piccole quantità di informazioni che vengono inviati dai siti visitati e conservati per migliorare la navigazione, sono memorizzati nel profilo dei singoli lavoratori e conservati in locale sul computer utilizzato per quanto riguarda la navigazione effettuata dal computer stesso. E' possibile la cancellazione a carico del singolo lavoratore come da procedura contenuta nell'ALLEGATO I - ISTRUZIONI OPERATIVE PER LA CANCELLAZIONE DEI COOKIES al presente disciplinare.
5. Statistiche (anonime giornaliere,settimanali e mensili) relative a:
   - - siti visitati
   - - file scaricati
   - - n° connessioni
   - - byte scaricati
   - - tempo di navigazione
   - - protocolli utilizzati
   - - browser utilizzati

ALLEGATO E - CATEGORIE DI FILTRAGGIO DEI SITI WEB

1. **Categoria - Potenzialmente Dannosi**
   - Abuso di Minori (consentita la navigazione)
   - Discriminazione (consentita la navigazione)
   - Abuso di Droghe (consentita la navigazione)
   - Violenza esplicita (inibita la navigazione)
   - Gruppi Estremisti (inibita la navigazione)
   - Hacking (inibita la navigazione)
   - Illegali o Non Etici (inibita la navigazione)
   - Plagio (inibita la navigazione)
   - Elusione dei Proxy (inibita la navigazione)

2. **Categoria - Contenuti per adulti**
   - Aborto (consentita la navigazione)
   - Organizzazioni di Avvocatura (consentita la navigazione)
   - Alcool (inibita la navigazione)
   - Credo Alternativi (inibita la navigazione)
   - Appuntamenti (inibita la navigazione)
   - Gioco d'azzardo (inibita la navigazione)
   - Lingerie and Costumi da bagno (inibita la navigazione)
   - Marijuana (inibita la navigazione)
   - Nudità e Comportamenti audaci (inibita la navigazione)
   - Altri Materiali per Adulti (inibita la navigazione)
   - Pornografia (inibita la navigazione)
   - Educazione Sessuale (consentita la navigazione)
   - Caccia e Giochi di Guerra (inibita la navigazione)
   - Tabacco (inibita la navigazione)
   - Vendita armi (inibita la navigazione)

3. **Categoria - Elevato consumo di banda**
   - File Sharing e Storage (inibita la navigazione)
   - Freeware e Download di Software (inibita la navigazione)
   - Internet Radio e TV (consentita la navigazione)
   - Telefonia Internet (consentita la navigazione)
   - Condivisione file Peer-to-peer (inibita la navigazione)
   - Streaming contenuti multimediali e Download (inibita la navigazione)

4. **Categoria - Rischiosi per la sicurezza**
   - DNS Dinamici (inibita la navigazione)
   - Siti Web Dannosi (inibita la navigazione)
   - Newly Observed Domain (inibita la navigazione)
   - Newly Registered Domain (inibita la navigazione)
   - Phishing (inibita la navigazione)
   - Spam URLs (inibita la navigazione)

5. **Categoria - Interessi Generali Privati**

- Annunci pubblicitari (consentita la navigazione)
- Arte e Cultura (consentita la navigazione)
- Vendite all'Asta (consentita la navigazione)
- Brokerage e Trading (consentita la navigazione)
- Educazione infantile (consentita la navigazione)
- Content Servers (consentita la navigazione)
- Cartoline digitali (consentita la navigazione)
- Domain Parking (consentita la navigazione)
- Contenuto dinamico (consentita la navigazione)
- Formazione scolastica (consentita la navigazione)
- Intrattenimento (consentita la navigazione)
- Folklore (consentita la navigazione)
- Giochi (consentita la navigazione)
- Religione (consentita la navigazione)
- Salute e Benessere (consentita la navigazione)
- Messaggistica Istantanea (consentita la navigazione)
- Ricerca di Impiego (consentita la navigazione)
- Contenuto senza significato (consentita la navigazione)
- Medicina (consentita la navigazione)
- News e Media (consentita la navigazione)
- Newsgroup e Piattaforme di messaggi (consentita la navigazione)
- Privacy (consentita la navigazione)
- Veicoli (consentita la navigazione)
- Siti Web e Blog (consentita la navigazione)
- Organizzazioni Politiche (consentita la navigazione)
- Immobiliari (consentita la navigazione)
- Reference (consentita la navigazione)
- Ristoranti e Pasti (consentita la navigazione)
- Shopping (consentita la navigazione)
- Social Networking (consentita la navigazione)
- Società e Stili di Vita (consentita la navigazione)
- Sport (consentita la navigazione)
- Viaggi (consentita la navigazione)
- Web Chat (consentita la navigazione)
- Web-Email (consentita la navigazione)

6. **Categoria - Interessi Generali di Lavoro**
   - Forze Armate (consentita la navigazione)
   - Business (consentita la navigazione)
   - Organizzazioni Caritatevoli (consentita la navigazione)
   - Finanza e Banche (consentita la navigazione)
   - Organizzazioni (consentita la navigazione)
   - Governo ed Organizzazioni Legali (consentita la navigazione)
   - Tecnologia dell'Informazione (consentita la navigazione)
   - Informazione e Sicurezza Informatica (consentita la navigazione)
   - Meeting Online (consentita la navigazione)
   - Accesso Remoto

- Motori di Ricerca e Portali (consentita la navigazione)
- Siti Web Sicuri (consentita la navigazione)
- Web Analytics (consentita la navigazione)
- Web Hosting (consentita la navigazione)
- Applicazioni Web-based (consentita la navigazione)

ALLEGATO F - ELENCO DELLE TIPOLOGIE DI FILE BLOCCATI IN DOWNLOAD DA INTERNET

.adp - Access Project (Microsoft)
.app - Executable Application
.asp - Active Server Page
.bas - BASIC Source Code
.bat - Batch Processing
.cer - Internet Security Certificate File
.chm - Compiled HTML Help
.cmd - DOS CP/M Command File, Command File for Windows NT
.cnt - Help file index
.com - Command
.cpl - Windows Control Panel Extension (Microsoft)
.crt - Certificate File
.csh - csh Script
.der - DER Encoded X509 Certificate File
.exe - Executable File
.fxp - FoxPro Compiled Source (Microsoft)
.gadget - Windows Vista gadget
.hlp - Windows Help File
.hpj - Project file used to create Windows Help File
.hta - Hypertext Application
.inf - Information or Setup File
.ins - IIS Internet Communications Settings (Microsoft)
.isp - IIS Internet Service Provider Settings (Microsoft)
.its - Internet Document Set, Internet Translation
.js - JavaScript Source Code
.jse - JScript Encoded Script File
.ksh - UNIX Shell Script
.lnk - Windows Shortcut File
.mad - Access Module Shortcut (Microsoft)
.maf - Access (Microsoft)
.mag - Access Diagram Shortcut (Microsoft)
.mam - Access Macro Shortcut (Microsoft)
.maq - Access Query Shortcut (Microsoft)
.mar - Access Report Shortcut (Microsoft)
.mas - Access Stored Procedures (Microsoft)
.mat - Access Table Shortcut (Microsoft)
.mau - Media Attachment Unit
.mav - Access View Shortcut (Microsoft)
.maw - Access Data Access Page (Microsoft)
.mda - Access Add-in (Microsoft), MDA Access 2 Workgroup (Microsoft)
.mdb - Access Application (Microsoft), MDB Access Database (Microsoft)
.mde - Access MDE Database File (Microsoft)
.mdt - Access Add-in Data (Microsoft)
.mdw - Access Workgroup Information (Microsoft)
.mdz - Access Wizard Template (Microsoft)
.msc - Microsoft Management Console Snap-in Control File (Microsoft)
.msh - Microsoft Shell
.msh1 - Microsoft Shell
.msh2 - Microsoft Shell
.mshxml - Microsoft Shell

.msh1xml - Microsoft Shell
.msh2xml - Microsoft Shell
.msi - Windows Installer File (Microsoft)
.msp - Windows Installer Update
.mst - Windows SDK Setup Transform Script
.ops - Office Profile Settings File
.osd - Application virtualized with Microsoft SoftGrid Sequencer
.pcd - Visual Test (Microsoft)
.pif - Windows Program Information File (Microsoft)
.plg - Developer Studio Build Log
.prf - Windows System File
.prg - Program File
.pst - MS Exchange Address Book File, Outlook Personal Folder File (Microsoft)
.reg - Registration Information/Key for W95/98, Registry Data File
.scf - Windows Explorer Command
.scr - Windows Screen Saver
.sct - Windows Script Component, Foxpro Screen (Microsoft)
.shb - Windows Shortcut into a Document
.shs - Shell Scrap Object File
.ps1 - Windows PowerShell
.ps1xml - Windows PowerShell
.ps2 - Windows PowerShell
.ps2xml - Windows PowerShell
.psc1 - Windows PowerShell
.psc2 - Windows PowerShell
.tmp - Temporary File/Folder
.url - Internet Location
.vb - VBScript File or Any VisualBasic Source
.vbe - VBScript Encoded Script File
.vbp - Visual Basic project file
.vbs - VBScript Script File, Visual Basic for Applications Script
.vsmacros - Visual Studio .NET Binary-based Macro Project (Microsoft)
.vsw - Visio Workspace File (Microsoft)
.ws - Windows Script File
.wsc - Windows Script Component
.wsf - Windows Script File
.wsh - Windows Script Host Settings File
.xnk - Exchange Public Folder Shortcut
.ade - ADC Audio File
.cla - Java class File
.class - Java class File
.grp - Microsoft Widows Program Group
.jar - Compressed archive file package for Java classes and data
.mcf - MMS Composer File
.ocx - ActiveX Control file
.pl - Perl script language source code
.xbap - Silverlight Application Package

ALLEGATO G - ISTRUZIONI OPERATIVE PER LA CANCELLAZIONE DELLA CRONOLOGIA DELLE PAGINE WEB VISITATE

Per la cancellazione della cronologia di navigazione memorizzata sul computer locale è necessario procedere in maniera differente in relazione alla tipologia di browser utilizzato:

1. Internet Explorer
   - Selezionare il pulsante Strumenti in alto a destra, scegliere Sicurezza, quindi seleziona Elimina cronologia esplorazioni.
   - Scegliere Cronologia e quindi selezionare Elimina.
2. Microsoft Egde
   - Selezionare i tre punti orizzontali in alto a destra.
   - Nella sezione Cancella i dati delle esplorazioni premere il tasto Scegli gli elementi da cancellare.
   - Selezionare la voce Cronologia esplorazioni.
   - Selezionare Cancella.
3. Mozilla Firefox
   - Fare clic sul pulsante Libreria, successivamente su Cronologia e fare infine clic su Cancella la cronologia recente….
   - Fare clic sul menu a discesa Intervallo di tempo da cancellare per scegliere quanta cronologia eliminare (si può scegliere tra l'ultima ora, le ultime due ore, le ultime quattro ore, l'ultima giornata o tutta la cronologia).
   - Contrassegnare la casella “Cronologia navigazione e download”.
   - Fare clic su Cancella adesso.
4. Google Chrome
   - Fare clic sui tre punti verticali in alto a destra.
   - Fare clic su Altri Strumenti.
   - A sinistra, Fare clic su Cancella dati di navigazione. Verrà visualizzata una finestra.
   - Nel menu a discesa, selezionare il periodo della cronologia da eliminare. Per cancellare tutti i dati, selezionare Tutto.
   - Selezionare "Cronologia di navigazione".
   - Fare clic su Cancella dati.

ALLEGATO H - ISTRUZIONI OPERATIVE PER LA CANCELLAZIONE DELLA MEMORIA CACHE DELLE PAGINE WEB VISITATE

Per la cancellazione della memoria cache delle pagine visitate memorizzata sul computer locale è necessario procedere in maniera differente in relazione alla tipologia di browser utilizzato:

1. Internet Explorer
   - Selezionare il pulsante Strumenti in alto a destra, scegliere Sicurezza, quindi seleziona Elimina cronologia esplorazioni.
   - Scegliere File temporanei Internet e file di siti Web e quindi selezionare Elimina.
2. Microsoft Egde
   - Selezionare i tre punti orizzontali in alto a destra.
   - Nella sezione Cancella i dati delle esplorazioni premere il tasto Scegli gli elementi da cancellare.
   - Selezionare la voce Dati e file memorizzati nella cache.
   - Selezionare Cancella.
3. Mozilla Firefox
   - Fare clic sul pulsante Libreria, successivamente su Cronologia e fare infine clic su Cancella la cronologia recente….
   - Fare clic sul menu a discesa Intervallo di tempo da cancellare per scegliere quanta cronologia eliminare (si può scegliere tra l'ultima ora, le ultime due ore, le ultime quattro ore, l'ultima giornata o tutta la cronologia).
   - Contrassegnare la casella “Cache”.
   - Fare clic su Cancella adesso.
4. Google Chrome
   - Fare clic sui tre punti verticali in alto a destra.
   - Fare clic su Altri Strumenti.
   - A sinistra, Fare clic su Cancella dati di navigazione. Verrà visualizzata una finestra.
   - Nel menu a discesa, selezionare il periodo della cronologia da eliminare. Per cancellare tutti i dati, selezionare Tutto.
   - Selezionare "Immagini e file memorizzati nella cache".
   - Fare clic su Cancella dati.

ALLEGATO I - ISTRUZIONI OPERATIVE PER LA CANCELLAZIONE DEI COOKIES

1. Internet Explorer
   - Selezionare il pulsante Strumenti in alto a destra, scegliere Sicurezza, quindi seleziona Elimina cronologia esplorazioni.
   - Scegliere Cookie e dati di siti Web e quindi selezionare Elimina.
2. Microsoft Egde
   - Selezionare i tre punti orizzontali in alto a destra.
   - Nella sezione Cancella i dati delle esplorazioni premere il tasto Scegli gli elementi da cancellare.
   - Selezionare la voce Cookie e dati di siti Web salvati.
   - Selezionare Cancella.
3. Mozilla Firefox
   - Fare clic sul pulsante Libreria, successivamente su Cronologia e fare infine clic su Cancella la cronologia recente….
   - Fare clic sul menu a discesa Intervallo di tempo da cancellare per scegliere quanta cronologia eliminare (si può scegliere tra l'ultima ora, le ultime due ore, le ultime quattro ore, l'ultima giornata o tutta la cronologia).
   - Contrassegnare la casella “Cookie”.
   - Fare clic su Cancella adesso.
4. Google Chrome
   - Fare clic sui tre punti verticali in alto a destra.
   - Fare clic su Altri Strumenti.
   - A sinistra, Fare clic su Cancella dati di navigazione. Verrà visualizzata una finestra.
   - Nel menu a discesa, selezionare il periodo della cronologia da eliminare. Per cancellare tutti i dati, selezionare Tutto.
   - Selezionare "Cookie e altri dati dei siti".
   - Fare clic su Cancella dati.

ALLEGATO J - ISTRUZIONI OPERATIVE SULL'UTILIZZO DEL SOFTWARE ANTI-VIRUS

Per effettuare la scansione di file o cartelle di file al fine di individuare la presenza di eventuali virus occorre procedere come segue:

- selezionare file o cartella con il tasto destro del mouse
- dal menu contestuale selezionare la voce "Scansione con Sophos Anti-Virus.

A scansione effettuata verrà visualizzato un report con le relative informazioni. Tutte le altre operazioni di sicurezza e protezione sono effettuate e configurate centralmente dal SIAT.