# Regolamento per l'utilizzo degli strumenti telematici

**ver. 4.0**

REGIONE DEL VENETO

ULSS7 PEDEMONTANA

| Versione | Data | Modifiche e motivazioni |
|---|---|---|
| **1.0** | **27 febbraio 2019 (del.n. 318/19)** | **Prima emissione uniforma ed integra i regolamenti delle precedenti aziende ex ULSS3 ed ex ULSS4** |
| **2.0** | **9 ottobre 2019 (del.n. 1408/19)** | **Revisione periodica** |
| **3.0** | **22 aprile 2020 (del.n. 533/20)** | **Revisione periodica** |
| **4.0** | **__ ottobre 2023 (del.n. ___/23)** | **Revisione periodica** |

# INDICE

## Premessa

Negli ultimi anni l'utilizzo da parte dell'Azienda ULSS7 PEDEMONTANA di risorse informatiche (computer, smartphone, periferiche, software, internet ed interconnessioni) è notevolmente aumentato sia in termini quantitativi che di complessità, con importanti implicazioni in termini di sicurezza, disponibilità ed integrità dei sistemi informativi dell'ente. Risulta pertanto necessario stabilire una serie di regole di comportamento che, nel rispetto della normativa in materia di protezione dei dati personali, garantiscano l'efficienza ed il corretto utilizzo di tali risorse.

Si evidenzia inoltre che tra i poteri del "datore di lavoro" rientra quello, solitamente riportato nell'ambito del potere direttivo, di controllare l'esatta esecuzione della prestazione lavorativa dovutagli, verificando se il dipendente usa la prescritta diligenza e osserva le disposizioni impartitegli, anche al fine dell'eventuale potere disciplinare. Al riguardo si ricorda che in capo al dipendente pubblico, oltre all'obbligo di adottare comportamenti conformi al corretto espletamento della prestazione lavorativa ed idonei a non causare danni o pericoli a beni mobili ed agli strumenti ad essi affidati, vige l'obbligo di non utilizzare a fini privati materiali o attrezzature di cui dispone per fini istituzionali.

Tuttavia proprio in considerazione della delicatezza dell'argomento e con riferimento alla normativa in tema di protezione dei dati personali l'attività di controllo deve essere rispettosa dei principi fondamentali di "proporzionalità", inoltre deve avvenire nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato e soprattutto, che di tale attività, debba essere fornita adeguata e preventiva informativa.

Premesso quindi che l'utilizzo delle risorse informatiche e telematiche deve sempre ispirarsi al principio della diligenza e correttezza - come da comportamenti che normalmente si adottano nell'ambito dei rapporti di lavoro - l'Azienda ULSS7 PEDEMONTANA ha adottato un Regolamento interno diretto ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla Sicurezza nel trattamento dei dati.

Considerato inoltre che l'Azienda ULSS7 PEDEMONTANA, nell'ottica di uno svolgimento proficuo e più agevole della propria attività, ha da tempo deciso di mettere a disposizione dei propri collaboratori che ne necessitassero per il tipo di funzioni svolte, telefoni e mezzi di comunicazione efficienti (computer portatili, telefoni cellulari, etc.), sono state inserite nel regolamento alcune clausole relative alle modalità ed i doveri che ciascun collaboratore deve osservare nell'utilizzo di tale strumentazione.

## Definizioni

**Utente:** è la persona autorizzata ad accedere alla rete aziendale, ad internet e alla posta elettronica

**Incaricato del trattamento:** è la persona fisica autorizzata a compiere operazioni di trattamento dal titolare o dal responsabile

**Responsabili del trattamento:** sono le figure formalmente individuate dal titolare e preposte al trattamento di dati personali

**E-mail:** indica la funzione di posta elettronica per lo scambio di messaggio e di documenti

**Download:** è l'azione di scaricamento, ricezione o prelevamento di un file dalla rete trasferendolo sul disco rigido del computer o su altra periferica dell'utente

**Upload:** è il processo di invio di un file (o più genericamente di un flusso finito di dati o informazioni) ad un sistema remoto attraverso una rete informatica

**Firma Digitale:** è l'equivalente informatico della firma autografa apposta su carta, ed ha lo stesso valore legale. Si tratta di un procedimento informatico che garantisce l'autenticità del documento, l'integrità del contenuto, ed il non ripudio

**Firma Grafometrica:** indica una modalità di firma elettronica realizzata con un gesto manuale del tutto analogo alla firma autografa su carta. I dati di una firma si acquisiscono mediante un dispositivo in grado di acquisire dinamicamente il movimento di uno stilo - azionato direttamente dalla mano di una persona su una superficie sensibile (emulando una penna sulla carta)

**MFA:** è un sistema di autenticazione dell'utente che usa almeno 2 fattori di autenticazione. È chiamata anche autenticazione forte in quanto, per accedere ai sistemi oltre alla consueta password è previsto almeno un ulteriore fattore di autenticazione (come ad es. un codice ricevuto via SMS, token, o altro)

**SIEM:** (in italiano gestione delle informazioni e degli eventi di sicurezza ) soluzione software per la sicurezza che analizza gli eventi di sicurezza, ricevuti dai sistemi aziendali, che dispone di regole e motori di analisi in grado di rilevare e analizzare le minacce sia in tempo reale che con specifici Report

**SOC:** centro operativo sicurezza, ovvero struttura con il compito di supervisionare e gestire proattivamente la Cybersecurity utilizzando strumenti, principalmente SIEM ma anche fonti esterne con l'obiettivo di prevenire, rilevare, analizzare e rispondere agli attacchi informatici

**WAF:** ovvero firewall per applicazioni web, si tratta di uno strumento per proteggere le applicazioni web filtrando, monitorando e bloccando qualsiasi traffico dannoso in entrata, impedendo al contempo l'uscita di dati non autorizzati dall'applicazione

**PAM:** strumento di sicurezza informatica per la gestione e protezione di accessi privilegiati elevati all'interno di un sistema informatico (strumento avanzato di protezione degli account di amministratori di sistema o superutenti)

**MALWARE:** qualsiasi programma informatico considerato “malvagio”, ovvero usato per disturbare le operazioni svolte da un utente di un computer, e che sostituisce il più restrittivo termine “virus informatico”

**SPYWARE:** è definito spyware per computer un tipo pericoloso di malware progettato per monitorare segretamente l'attività del computer e rubare informazioni personali, tra cui password, a insaputa dell’utente

**RANSOMWARE:** è un tipo di malware malevolo che può “infettare” un dispositivo digitale (PC, tablet, smartphone, smart TV), bloccando l'accesso a tutti o ad alcuni dei suoi contenuti (foto, video, file, ecc.) per poi chiedere un riscatto (in inglese, “ransom”) da pagare per “liberarli”

## 1- Linee Generali

1.1 Il presente Regolamento, approvato con deliberazione del Direttore Generale n. _____ del ____, entrerà in vigore dopo 15 giorni dalla sua pubblicazione nel sito Intranet aziendale e sostituisce la versione precedente. Con l'entrata in vigore del presente regolamento tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi abrogate e sostituite dalle presenti.

1.2 Copia del regolamento è pubblicato e scaricabile dalla intranet aziendale.

1.3 Il regolamento si applica a tutti i dipendenti, senza distinzione di ruolo e/o livello, nonché a tutti i collaboratori dell'azienda a prescindere dal rapporto contrattuale con la stessa intrattenuto (lavoratori somministrati, collaboratore a progetto, in stage, specializzandi, universitari, ecc.) oltre che ai dipendenti delle società esterne affidatarie di servizi autorizzati ad accedere alla rete informatica dell'Azienda ULSS7 PEDEMONTANA.

1.4 Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche e telematiche, per "utente" deve intendersi ogni dipendente e collaboratore (collaboratore a progetto, in stage, specializzando, consulente, ecc.) in possesso di specifiche credenziali di autenticazione. Tale figura potrà anche venir indicata quale "incaricato del trattamento".

1.5 Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni motivate al presente Regolamento. Le proposte verranno esaminate dalla Direzione Generale.

1.6 Il presente Regolamento è soggetto a revisione con frequenza biennale.

## 2- Credenziali

2.1 Ogni dipendente all'atto dell'assunzione verrà dotato di credenziali (nome utente e password) per accedere alla rete da qualsiasi personal computer aziendale, nonché della propria casella di posta elettronica. Il nome utente consiste in un codice univoco per l'identificazione dell'utente e viene assegnato dal servizio Sistemi Informativi, oltre ad una parola chiave (password) riservata che dovrà venir custodita dall'incaricato con la massima diligenza e non divulgata. All'atto della cessazione di rapporto professionale con l'Azienda, le credenziali verranno disattivate automaticamente.
Il servizio personale rilascia al dirigente un certificato di firma digitale (su smart card o in modalità remota) mediante il quale viene fatto obbligo di sottoscrivere esclusivamente documenti informatici aziendali, secondo quanto stabilito nel Manuale di Gestione Documentale approvato con delibera 2265 del 02/12/2022.

2.2 La password, formata da lettere maiuscole o minuscole e/o numeri caratteri speciali, anche in combinazione fra loro, deve essere composta da almeno quattordici caratteri e non deve contenere riferimenti agevolmente riconducibili all'interessato.

2.3 È necessario procedere alla modifica della parola chiave a cura dell'utente, incaricato del trattamento, al primo utilizzo e, successivamente, **ogni tre mesi**.

2.4 La password non potrà essere modificata prima che sia passato 1 giorno dal precedente cambio e non potrà essere uguale alle 24 precedenti utilizzate.

2.5 In caso di diffusione accidentale, anche solo presunta, la password deve essere immediatamente modificata.

2.6 Il personale incaricato del servizio Sistemi Informativi dell'Azienda ULSS7 Pedemontana è preposto, su richiesta degli utenti dopo verifica dell'identità degli stessi, alla modifica/reset delle credenziali di autenticazione alla rete informatica.

## 3- Dispositivi Digitali e Dati

3.1 **Il Personal Computer affidato all'utente è uno strumento di lavoro**. Ogni utilizzo non inerente all'attività lavorativa è vietato perché può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. Il personal computer deve essere custodito con cura evitando ogni possibile forma di danneggiamento. Inoltre per i dipendenti pubblici, così come previsto dalla normativa di settore, è vietato un utilizzo a fini privati di materiali o attrezzature di cui dispone per ragioni di ufficio.

3.2 Il personal computer dato in affidamento all'utente permette l'accesso alla rete dell'Azienda ULSS7 PEDEMONTANA solo attraverso specifiche credenziali di autenticazione come meglio descritto al precedente punto 2 del presente Regolamento.

3.3 L'Azienda ULSS7 PEDEMONTANA rende noto che il personale incaricato, anche dei servizi esternalizzati, che opera presso il servizio Sistemi Informativi è stato autorizzato a compiere interventi nel sistema informatico aziendale diretti a garantire la sicurezza e la salvaguardia del sistema stesso, nonché per ulteriori motivi tecnici e/o manutentivi (come ad es. aggiornamento, sostituzione o implementazione di programmi, manutenzione hardware etc.). Detti interventi, in considerazione dei divieti di cui ai successivi punti nn. 5.2 e 6.1, potranno anche comportare l'accesso in qualunque momento, a tutte le risorse informatiche rese a disposizione dell'azienda, nonché alla verifica sui siti internet acceduti dagli utenti abilitati alla navigazione esterna. La stessa facoltà, sempre ai fini della sicurezza del sistema e per garantire la normale operatività dell'Azienda, si applica anche in caso di assenza prolungata oltre il trentesimo giorno solare, o impedimento dell'utente.

3.4 Il personale incaricato dal servizio Sistemi Informativi e dei servizi affidati in outsourcing ha la facoltà di collegarsi e visualizzare in remoto, previa comunicazione all'interessato, il desktop delle singole postazioni PC al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza contro virus, spyware, malware, etc. L'intervento viene effettuato esclusivamente su chiamata dell'utente o, in caso di oggettiva necessità**,** a seguito della rilevazione tecnica di problemi nel sistema informatico e telematico. In quest'ultimo caso, e sempre che non si pregiudichi la necessaria tempestività ed efficacia dell'intervento, verrà data comunicazione della necessità dell'intervento stesso.

3.5 Non è consentito il collegamento alla rete AULSS7 di dispositivi non aziendali salvo specifica richiesta da parte del Responsabile del trattamento e conferma da parte del Sistemi Informativi.

3.6 L'account dell'utente utilizzato per accedere alla postazione di lavoro è profilato con privilegi standard (non amministrativi), solamente il personale dei sistemi informativi - o personale delegato - è autorizzato all'installazione degli applicativi standard. Ulteriori necessità lavorative potranno essere richieste al personale dei sistemi informativi, tramite l'Helpdesk, che valuterà l'ammissibilità e l'eventuale approvazione

delle richieste. Si evidenzia che la normativa, civile e penale, impone la presenza di software regolarmente licenziato o libero (quindi non protetto dal diritto d'autore).

3.7 Salvo preventiva espressa autorizzazione del personale del servizio Sistemi Informativi, non è consentito all'utente modificare le caratteristiche impostate sul proprio PC né procedere ad installare dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, …).

3.8 Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il personale del servizio Sistemi Informativi nel caso in cui siano rilevati virus ed adottando quanto previsto dal successivo punto 7 del presente Regolamento relativo alla cyber security.

3.9 Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio o in caso di suo inutilizzo, salvo indicazioni contrarie da parte dei responsabili del servizio stesso o del Sistemi Informativi. In ogni caso lasciare un personal computer acceso e con l'utente loggato può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso. Durante l'allontanamento, anche di breve durata, l'utente deve bloccare la propria postazione per consentirne l'accesso unicamente mediante l'immissione della password.

3.10 L'utente è responsabile del PC portatile assegnatogli dal servizio Sistemi Informativi e deve custodirlo con diligenza durante gli spostamenti, nella sede di lavoro e/o in modalità di lavoro agile.

3.11 Ai PC portatili si applicano le regole di utilizzo previste dal presente regolamento, con particolare attenzione alla rimozione di eventuali file elaborati prima della riconsegna.

3.12 I PC portatili utilizzati all'esterno, in caso di allontanamento, devono essere custoditi con diligenza, adottando tutti i provvedimenti che le circostanze rendono necessari per evitare danni o sottrazioni.

3.13 Tali disposizioni si applicano anche nei confronti di incaricati esterni quali consulenti, collaboratori, ecc.

3.14 I PC portatili devono essere restituiti al servizio Sistemi Informativi al termine del rapporto di lavoro.

3.15 Tutti i supporti magnetici rimovibili forniti dall'Azienda ULSS7 PEDEMONTANA (CD e DVD riscrivibili, supporti USB, hard disk esterni, ecc.), contenenti dati sensibili nonché informazioni costituenti patrimonio aziendale, devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto o, successivamente alla cancellazione, recuperato.

3.16 Al fine di assicurare la distruzione e/o inutilizzabilità di supporti magnetici rimovibili contenenti dati sensibili, ciascun utente dovrà contattare il personale dei Sistemi Informativi e seguire le istruzioni da questo impartite.

3.17 In ogni caso, i supporti magnetici contenenti dati sensibili devono essere dagli utenti adeguatamente custoditi.

3.18 È vietato l'utilizzo di supporti rimovibili personali, salvo i casi espressamente autorizzati dal Responsabile del servizio.

3.19 L'utente è responsabile della custodia dei supporti e dei dati aziendali in essi contenuti.

3.20 **Il telefono aziendale affidato all'utente è uno strumento di lavoro.** L'uso deve essere esclusivamente per lo svolgimento dell'attività lavorativa, non essendo quindi consentite comunicazioni a carattere personale o comunque non strettamente inerenti l'attività lavorativa stessa. La ricezione o l'effettuazione di telefonate personali è consentita solo nel caso di comprovata necessità ed urgenza, mediante il telefono fisso aziendale a disposizione.

L'assegnazione del telefono cellulare aziendale è autorizzata dal Direttore / Responsabile dell'U.O. di appartenenza dell'utente che sarà responsabile del suo utilizzo e della sua custodia. Al cellulare aziendale si applicano le medesime regole sopra previste per l'utilizzo del telefono fisso aziendale: in particolare è vietato l'utilizzo del telefono cellulare messo a disposizione per inviare o ricevere SMS o MMS di natura personale o comunque non pertinenti rispetto allo svolgimento dell'attività lavorativa. L'eventuale uso promiscuo (anche per fini personali) del telefono cellulare aziendale è possibile soltanto in presenza di preventiva autorizzazione scritta e se previsto, in conformità delle istruzioni al riguardo impartite digitando il prefisso per l'addebito delle chiamate personali.
Per motivi di sicurezza è fatto obbligo di impostare un tipo di blocco schermo (segno, impronta digitale..).

3.21 È vietato l'utilizzo dei fax aziendali per fini personali, tanto per spedire quanto per ricevere documentazione.

3.22 È vietato l'utilizzo delle fotocopiatrici aziendali per fini personali.

3.23 È vietato l'utilizzo di scanner aziendali per fini personali.

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

3.25 Protezione contro furti e danneggiamenti

Tutte le postazioni di lavoro portatili e i dispositivi mobili devono essere custoditi in luogo sicuro, adottando le opportune precauzioni contro il furto delle strumentazioni informatiche e/o dei dati in esse contenuti.
L'Utente è tenuto a informare immediatamente il dirigente responsabile, il Servizio Sistemi Informativi e, qualora vi sia la possibilità di una violazione di dati personali, anche il RPD di qualsiasi danno, furto o perdita di strumentazioni informatiche, software e/o dati in proprio possesso, fermo restando gli obblighi di denuncia alle autorità competenti.

## 4- Utilizzo della rete

4.1 Per l'accesso alla rete dell'Azienda ULSS7 PEDEMONTANA ciascun utente deve essere in possesso della specifica credenziale di autenticazione.

4.2 È assolutamente proibito entrare nella rete e nei programmi con un codice d'identificazione utente diverso da quello assegnato. Le parole chiave d'ingresso alla rete ed ai programmi sono personali e vanno tenute segrete.

4.3 Le cartelle utenti presenti nei server dell'Azienda ULSS7 PEDEMONTANA sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto qualunque file che non sia legato all'attività lavorativa non può essere allocato, nemmeno per brevi periodi, in queste unità. Su queste unità vengono svolte regolari attività di controllo, amministrazione e back up da parte del personale del servizio Sistemi Informativi.

4.4 Il personale del servizio Sistemi Informativi può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la Sicurezza sia sui PC degli incaricati sia sulle unità di rete.

4.5 Risulta opportuno che, con regolare periodicità (almeno ogni tre mesi), ciascun utente provveda alla pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati, essendo infatti necessario evitare un'archiviazione ridondante.

## 5- Uso della posta elettronica

5.1 **La casella di posta elettronica assegnata all'utente e/o al servizio è uno strumento di lavoro aziendale.** Nell'Intranet aziendale è presente il manuale descrittivo delle relative funzionalità. L'assegnatario della casella di posta elettronica è responsabile del corretto utilizzo. Al fine di aumentare il livello di sicurezza, l'Azienda ha scelto di implementare un sistema di Multi Factor Authentication (MFA), richiedendo all'Utente di dimostrare la propria identità attraverso una seconda forma di verifica al momento dell'accesso.

5.2 È fatto divieto di utilizzare le caselle di posta elettronica ***nome.cognome@aulss7.veneto.it*** [1] per motivi diversi da quelli strettamente legati all'attività lavorativa, salvo le indicazioni presenti nel successivo punto 6.
In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare la

posta elettronica per:

- l'invio e/o il ricevimento di allegati contenenti filmati o brani musicali (es.mp3) non legati all'attività lavorativa;
- l'invio e/o il ricevimento di messaggi personali o per la partecipazione a dibattiti, aste on line, concorsi, forum o mailing-list;
- la partecipazione a catene telematiche (o catene di Sant'Antonio);
- gli allegati non potranno avere dimensioni maggiori di 25 Mbyte.

[1] Ovvero potrà essere realizzato un sistema di indirizzi di posta elettronica condivisi tra più utenti (ad es. *segdipalgot@aulss7.veneto.it* al posto di un sistema basato sull'identità personale).

5.3 La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti. La conservazione on line delle mail in tale casella è a tempo indeterminato mentre per i documenti messi nel Cestino è di 30 giorni.

5.4 Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali per l'Azienda ULSS7 PEDEMONTANA ovvero contenga documenti da considerarsi riservati in quanto contraddistinti dalla dicitura "strettamente riservati" o da analoga dicitura, deve essere visionata od autorizzata dal Responsabile d'ufficio.

5.5 È possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario. Si evidenzia che le comunicazioni ufficiali, da inviarsi mediante gli strumenti tradizionali (fax, posta, …), devono essere autorizzate e firmate dalla Direzione Generale e/o dai Responsabili di ufficio, a seconda del loro contenuto e dei destinatari delle stesse. Sono state attivate delle caselle di posta certificata (PEC) dalle quali è possibile trasmettere e ricevere documenti ufficiali in sostituzione della posta cartacea.

5.6 È obbligatorio porre la massima attenzione nell'apertura delle email, verificandone l'attendibilità ed il mittente, in particolare per quelle contenenti file allegati oppure link a siti web esterni.

5.7 Al fine di garantire la funzionalità del servizio di posta elettronica aziendale e di ridurre al minimo l'accesso ai dati, nel rispetto del principio di necessità e di proporzionalità, in caso di assenze programmate (ad es. per ferie o attività di lavoro fuori sede dell'assegnatario della casella) l'utente deve attivare le funzionalità di risponditore automatico, con le indicazioni su caselle o numeri di telefono alternativi da contattare.

5.8 Sarà comunque consentito al superiore gerarchico dell'utente, preventivamente sentito l'utente, o comunque a persona individuata dall'azienda, accedere alla casella di posta elettronica dell'utente per ogni ipotesi in cui si renda necessario (ad es.: mancata attivazione della funzionalità di cui al punto 5.7 o assenza non programmata).

5.9 Il personale del servizio Sistemi Informativi o altro personale esterno a ciò incaricato, nell'impossibilità di procedere come sopra indicato e nella necessità di non pregiudicare la necessaria tempestività ed efficacia dell'intervento, potrà accedere alla casella di posta elettronica per le sole finalità indicate al punto 3.3.

5.10 Alla data di cessazione del rapporto professionale con l'Azienda le credenziali di accesso alla posta dell'utente vengono disattivate automaticamente. L'utente dovrà provvedere al trasferimento di proprietà di eventuali documenti condivisi prima della cessazione, altrimenti non saranno più recuperabili. Dopo 30 giorni dalla disattivazione, durante i quali non sarà comunque possibile accedere, viene effettuata l'eliminazione definitiva.

## 6- Navigazione in Internet (e uso per finalità non istituzionali)

6.1 **Il PC assegnato al singolo utente ed abilitato alla navigazione in Internet costituisce uno strumento aziendale utilizzabile esclusivamente per lo svolgimento della propria attività lavorativa**. È quindi assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa, salvo le indicazioni presenti nel successivo punto 6.5.

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

- l'upload o il download di software, nonché di documenti provenienti da siti web non verificati in quanto sussiste il grave pericolo di introdurre virus informatici;
- l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, fatti salvi i casi direttamente autorizzati dal Responsabile d'ufficio e/o del servizio Sistemi Informativi e comunque nel rispetto delle normali procedure di acquisto;
- ogni forma di registrazione a siti i cui contenuti non siano strettamente legati all'attività lavorativa; la partecipazione a forum non professionali, l'utilizzo di chat (esclusi gli strumenti autorizzati), o social web non espressamente autorizzati dal Responsabile d'ufficio.

L'accesso, tramite internet, a caselle webmail di posta elettronica personale è consentito solo nel rispetto di quanto riportato al punto 6.5.

6.3 Al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa, l'Azienda ULSS7 PEDEMONTANA rende peraltro nota l'adozione di uno specifico sistema di blocco o filtro automatico che prevengano determinate operazioni quali l'upload o l'accesso a determinati siti inseriti in una black list. L'azienda si attiverà nell'individuazione di categorie di siti considerati correlati con la prestazione lavorativa e compatibili con le finalità non istituzionali di cui al successivo punto 6.5.

6.4 Gli eventuali controlli, compiuti dal personale incaricato del servizio Sistemi Informativi ai sensi del precedente punto 3.3, avverranno mediante sistemi SIEM come meglio specificato al successivo punto 7.5. Il controllo sui file di log non è continuativo ed i file stessi vengono conservati non oltre 6 mesi, ossia il tempo indispensabile per il corretto perseguimento delle finalità organizzative e di sicurezza dell'azienda.

6.5 La Direzione Aziendale, potrà consentire la consultazione di determinati siti internet e l'accesso a caselle webmail di posta elettronica personale laddove le modalità di consultazione siano compatibili con le misure di sicurezza implementata a protezione

del sistema informatico. Tale modalità non deve in ogni caso avvenire in misura eccedente e pregiudizievole rispetto agli obblighi che l'utente ha nei confronti dell'ente. Al fine di contemperare le rispettive esigenze l'uso di internet per tali finalità è consentito da postazioni dedicate, individuate dalle Direzioni di Area con la collaborazione del servizio Sistemi Informativi.

## 7- Cyber security

7.1 Il sistema informatico dell'Azienda ULSS7 PEDEMONTANA è protetto da software antivirus/anti malware aggiornato quotidianamente. Ogni utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale mediante virus o mediante ogni altro software aggressivo.

7.2 Nel caso il software antivirus rilevi la presenza di malware, l'utente dovrà immediatamente sospendere ogni elaborazione in corso senza spegnere il computer nonché segnalare prontamente l'accaduto al personale del servizio Sistemi Informativi.

7.3 Ogni dispositivo magnetico di provenienza esterna all'Azienda dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, dovrà essere prontamente consegnato al personale del servizio Sistemi Informativi.

7.4 È obbligatorio attenersi alle disposizioni in materia di Privacy e di misure minime di sicurezza, come indicato nella lettera di designazione ad incaricato del trattamento dei dati ai sensi del G.D.P.R. (REG UE 679/2016) con successive modifiche e integrazioni.

7.5 L'azienda al fine di migliorare la sicurezza ha attivato un servizio SOC alimentato dal SIEM Aziendale per la raccolta e la correlazione degli eventi sui sistemi per garantire migliore sicurezza dei servizi e delle risorse aziendali, monitorare le risorse, individuare e reagire tempestivamente attività anomale e indizi di possibili attacchi cyber.

7.6 L'azienda al fine di migliorare la sicurezza ha attivato un servizio sperimentale PAM di gestione credenziali amministrative, destinato agli amministratori di sistema, ed oltre a firewall perimetrali ha attivato sistemi WAF per la messa in sicurezza degli applicativi WEB.

7.7 In caso di anomalie, rilevate da SIEM o altri fonti, il personale incaricato dei Sistemi Informativi effettuerà controlli che si concluderanno con avvisi generalizzati diretti ai dipendenti dell'area o del settore in cui è stata rilevata l'anomalia, nei quali verrà evidenziato l'utilizzo irregolare degli strumenti aziendali e si inviteranno gli interessati ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite. Controlli su base individuale potranno essere compiuti solo in caso di successive ulteriori anomalie e per i casi di particolare gravità solo su autorizzazione della Direzione. Tutti coloro che utilizzano le strumentazioni informatiche e telematiche devono sempre considerare che le apparecchiature utilizzate immagazzinano una serie di informazioni inerenti il loro uso: numero di mail inviate e ricevute; cronologia siti web visitati (url); pagine visualizzate; durata delle connessioni a internet; materiale scaricato.

In particolare, il sistema informativo fornisce una serie di informazioni inerenti l'utilizzo dei software e/o dell'hardware di ciascuna postazione di lavoro (log), quali:

- i log di accesso a internet;
- i log inerenti la posta elettronica; i log relativi ai virus rilevati;
- i log inerenti l'accesso alle banche dati e gli applicativi;
- log degli applicativi installati sulla propria postazione di lavoro.

Tutte le suddette informazioni potrebbero servire all'azienda, per poter salvaguardare il proprio patrimonio informativo e tecnologico o per rispondere a richieste dall'autorità giudiziaria.
I controlli verranno posti in essere solo per gruppi aggregati.

Nel caso in cui si riscontrassero comportamenti potenzialmente dannosi e comunque non conformi alle suddette linee guida, la Direzione aziendale provvederà a informare il dirigente responsabile del servizio. Nel caso in cui vi siano sospetti di illeciti di rilevanza penale si provvederà a denunciare il fatto all'autorità giudiziaria.
A seguito di comportamenti potenzialmente dannosi, l'Amministrazione si riserva di adottare le contromisure ritenute idonee per limitare i possibili effetti.

7.8 In alcun caso verranno compiuti controlli prolungati, costanti o indiscriminati senza autorizzazione.

## 8- Sanzioni

È fatto obbligo a tutti gli utenti di osservare le disposizioni portate a conoscenza con il presente regolamento. Il mancato rispetto o la violazione delle regole sopra ricordate è perseguibile nei confronti del personale dipendente con provvedimenti disciplinari e risarcitori previsti dal vigente CCNL nonché con tutte le azioni civili e penali consentite.