REGOLAMENTO
PER L'UTILIZZO DELLE RISORSE E DEI SERVIZI INFORMATICI AZIENDALI

ASL TERAMO
www.aslteramo.it

Sommario

REDAZIONE			VERIFICA			APPROVAZIONE		
Data	*Funzione*	*Cognome/Nome*	*Data*	*Funzione*	*Cognome/Nome*	*Data*	*Funzione*	*Cognome/Nome*
24.11.2023	UOC SISTEMI INFORM	Dott. Luca Fidanza	24.11.2023	DPO UOSD SEGRETERIA DIREZIONE	Dott. Davide De Luca Dott. Valeria Adriana Violante	30.11.2023	DG	Dott. Maurizio Di Giosia

ELENCO DELLE REVISIONI

Paragrafo	Descrizione Modifica	Rev. N.	Data Rev.
		1	

INDICE PER ARGOMENTI

PREMESSA

La progressiva diffusione delle nuove tecnologie ICT ed in particolare l'utilizzo della posta elettronica ed il libero accesso alla rete Internet, espone l'Azienda Sanitaria Locale di Teramo e gli utenti (dipendenti e collaboratori della stessa) a rischi di natura tecnica, patrimoniale e reputazionale, oltre alle responsabilità legali conseguenti alla violazione di specifiche disposizioni di legge (diritto d'autore, privacy, ecc.), creando evidenti problemi alla sicurezza ed all'immagine dell'Azienda stessa.

Premesso quindi che l'utilizzo delle risorse informatiche e telematiche deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito dei rapporti di lavoro, l'ASL ha predisposto il presente Regolamento Informatico Aziendale per il corretto utilizzo di apparecchiature e servizi informatici, allo scopo di evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla sicurezza nel trattamento dei dati.

Considerato inoltre che l'Azienda, nell'ottica di uno svolgimento proficuo e più agevole della propria attività, mette a disposizione dei propri dipendenti e collaboratori apparecchiature informatiche e mezzi di comunicazione efficienti (Personal Computer, Notebook, casella di posta elettronica, accesso alla rete Internet, etc.), sono stati inseriti nel regolamento alcuni articoli relativi alle modalità ed alle regole che ciascun utente deve osservare nell'utilizzo delle apparecchiature informatiche.

Quanto riportato nel presente regolamento non è valido per le apparecchiature informatiche collegate a strumentazioni elettromedicali, la cui gestione è demandata all'UO Ingegneria Clinica.

Art. 1 - Campo di Applicazione

1.1 Il presente 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 (consulenti, lavoratori somministrati, collaboratori a progetto, in stage, volontari, tirocinanti, ditte esterne autorizzate, ecc.).

Art. 2 - Definizioni ed Acronimi

2.1 Ai fini dell'applicazione del presente Regolamento si forniscono le seguenti definizioni:

- per "***utente***", si intende ogni dipendente, collaboratore–etc. che utilizza le risorse informatiche (hardware, software, rete, ecc.) messe a disposizione dall'Azienda, in possesso o meno di specifiche credenziali di autenticazione per l'utilizzo delle procedure aziendali;
- "***S.I.A.***", è l'acronimo di Sistema Informativo Aziendale; è costituito dall'insieme delle informazioni utilizzate, prodotte e trasformate da un'azienda durante l'esecuzione dei processi aziendali, dalle modalità in cui esse sono gestite e dalle risorse, sia umane, sia tecnologiche, coinvolte. Il sistema informatico, che indica una porzione di sistema informativo, è la componente del S.I.A. che fa uso di tecnologie informatiche e automazione.
- "***S.I.***" è l'acronimo di U.O.C. Sistemi Informativi; è la struttura aziendale preposta al corretto funzionamento delle risorse informatiche aziendali (vedi art.3). Per "*Tecnici dei S.I.*" si intende il personale della suddetta articolazione o altra persona da essa temporaneamente delegata (ad es. consulenti, società esterna addetta alla manutenzione, ecc.).

Art. 3 - Competenze

3.1 Nell'ambito della gestione delle risorse e dei servizi informatici aziendali risultano essere direttamente coinvolte determinate UU.OO., ciascuna con specifiche competenze.

Al fine di agevolare l'utente nella risoluzione delle problematiche relative all'utilizzo dei servizi summenzionati, si riporta un elenco di tali strutture, con le singole specifiche competenze:

- UOC Acquisizione Beni e Servizi: è l'unica articolazione aziendale, fatte salve eventuali deroghe che possono essere concesse di volta in volta, preposta all'acquisto di hardware, software e servizi di natura informatica previo parere tecnico rilasciato dalla UOC Sistemi Informativi.
- UOC Patrimonio, Lavori e Manutenzioni: è l'articolazione aziendale che ha in carico la predisposizione e la gestione, diretta o indiretta, di tutte le infrastrutture necessarie alla gestione ed al funzionamento degli impianti tecnologici (es. lavori edili, impianto elettrico e di condizionamento, ecc. ecc.).
- UOC Sistemi Informativi: è l'articolazione aziendale preposta a garantire il corretto funzionamento del S.I.A. e le cui principali competenze possono essere sintetizzate come segue:
  - fornire parere tecnico e consulenza in merito ad acquisto e gestione di software ed apparecchiature informatiche fatta eccezione per i dispositivi elettromedicali la cui competenza è in capo alla UO Ingegneria Clinica;
  - fungere da interfaccia tecnica fra gli utenti del S.I.A. e le ditte fornitrici;

- garantire il corretto funzionamento delle Postazioni di Lavoro;
- fornire a tutti gli utenti, durante il normale orario di lavoro, un Call Center di primo livello per la segnalazione di malfunzionamenti delle apparecchiature;
- gestire gli utenti del S.I.A. con i dovuti criteri di sicurezza e riservatezza;
- gestire e monitorare la rete aziendale;
- assegnare le apparecchiature informatiche disponibili in magazzino;
- formare il personale sul corretto uso delle risorse e delle procedure di Office Automation utilizzate.

Si precisa che l'U.O.C. Sistemi Informativi non è in alcun caso proprietaria dei dati gestiti dal S.I.A. e che pertanto eventuali statistiche o report dovranno essere richiesti alle UU.OO. di competenza (Controllo di Gestione, Ufficio del Personale, Ragioneria, Ufficio Statistica, ecc.). Analogamente, il corretto utilizzo delle procedure applicative (contabili, sanitarie, gestione del personale, ecc.) è di competenza delle diverse articolazioni aziendali che utilizzano il software.

Art. 4 - Finalità

4.1 Le apparecchiature informatiche, gli applicativi ed in generale tutte le risorse informatiche che l'ASL di Teramo mette a disposizione dei suoi utenti, ivi compresi i servizi di internet e posta elettronica, devono essere utilizzati esclusivamente per fini lavorativi e non personali e nel pieno rispetto della normativa vigente, nonché del presente Regolamento Aziendale. Ciò al fine di evitare possibili danni erariali, finanziari e di immagine all'Ente stesso.

4.2 Tutto il personale interessato dalle disposizioni del presente Regolamento è tenuto a contattare l'U.O.C. Sistemi Informativi prima di intraprendere qualsiasi attività tecnica non esplicitamente compresa nel presente regolamento, al fine di garantire che tali attività non siano in contrasto con gli standard di sicurezza informatica stabiliti dall'Ente.

HARDWARE E SOFTWARE

Art. 5 - Acquisto di hardware e software

5.1 Tutto l'hardware ed il software potrà essere acquistato solo previa richiesta di parere tecnico favorevole da parte dell'U.O.C. Sistemi Informativi, che controllerà le richieste di acquisto al fine di valutare la compatibilità e prevenire la compromissione della sicurezza del S.I.A..

Tutto il software in uso presso l'ASL Teramo deve essere ottenuto seguendo le procedure e le linee guida dell'Ente e deve essere registrato a nome dell'ASL di Teramo.

A tal fine le richieste di acquisto dell'hardware e del software dovranno essere redatte su apposito modulo disponibile nel sito aziendale nella sezione modulistica. Tale modulo dovrà essere inviato a mezzo e-mail all'indirizzo *"acquisti.informatici@aslteramo.it"*. Le richieste incomplete o compilate in modo errato **non potranno essere prese in considerazione** e verranno restituite al mittente.

All'U.O.C. Sistemi Informativi spetta la verifica tecnica della compatibilità degli strumenti richiesti con l'infrastruttura dell'Ente. Nel caso in cui gli strumenti proposti non possano - per ragioni tecniche - essere installati, verranno individuate - ove possibile - soluzioni alternative, d'intesa tra l'U.O.C. Sistemi Informativi ed il servizio richiedente.

In ogni caso, prima dell'acquisizione di nuovi software e/o hardware verrà sempre effettuata un'analisi del relativo rischio, tendente a valutare l'impatto potenziale della modifica richiesta sulla sicurezza delle informazioni e a pianificare le necessarie azioni di ripristino, subordinando l'acquisizione all'esito positivo della predetta analisi.

I supporti originali dei software acquistati e le relative licenze devono essere conservati presso l'U.O.C. Sistemi Informativi, così da consentire le operazioni di verifica della disponibilità di licenze e l'eventuale re-installazione delle procedure.

L'acquisto e la gestione dei materiali di consumo (carta, toner, etichette, CD/DVD, ecc.ecc.) non sono di competenza dell'U.O.C. Sistemi Informativi.

Art. 6 - Utilizzo dei software

6.1 Il software per elaboratori è considerato opera di ingegno e come tale è tutelato dalle Leggi sul diritto di Autore. L'utilizzo del software è regolamentato da licenze d'uso che devono essere rispettate da tutti gli utenti. (DLG. 518/92 sulla tutela giuridica del software e L. 248/2000 "*nuove norme di tutela del diritto d'autore*"). Pertanto, il personale è tenuto al rispetto delle leggi in materia di tutela della proprietà intellettuale (*copyright*) e non può in alcun caso installare, duplicare od utilizzare software ottenuto illegalmente o comunque sprovvisto delle necessarie licenze.

6.2 Non è consentito in alcun caso installare ed utilizzare programmi[1] diversi da quelli ufficialmente installati dai tecnici dell'U.O.C. Sistemi Informativi per conto dell'Azienda, salvo specifiche deroghe che dovranno essere preventivamente richieste, giustificate ed autorizzate, nonché concretamente gestite e monitorate dalla U.O.C. Sistemi Informativi.

6.3 Al fine di proteggere l'integrità del S.I. dell'ASL di Teramo, al personale non è consentito nemmeno installare ed utilizzare eventuale software di proprietà personale. Tale principio vincolante si applica anche alle applicazioni regolarmente acquistate e registrate, programmi shareware e/o freeware, eventuale software scaricato da Internet o proveniente da CD/DVD allegati a riviste e/o giornali o altro software posseduto a qualsiasi titolo.

6.4 L'utente è responsabile del software installato sul proprio PC e di come lo utilizza; se ne raccomanda pertanto un uso diligente ed accorto.

6.5 Non è in alcun caso consentita la disinstallazione/rimozione dei software presenti sui sistemi. I suddetti interventi saranno effettuati, in caso di necessità, solo a cura dei tecnici dell'U.O.C. Sistemi Informativi dietro segnalazione dell'utente e relativa approvazione.

6.6 In particolare, non è consentito in alcun caso rimuovere, disinstallare o disabilitare - anche temporaneamente - il software antivirus presente sui computer, oppure compiere qualsiasi altra azione comunque tendente ad impedirne l'aggiornamento automatico o la piena funzionalità.

Nell'eventualità di PC non collegati alla rete aziendale e/o la cui gestione, per svariati motivi, non sia a carico dell'U.O.C. Sistemi Informativi, sarà cura del fornitore procedere al regolare aggiornamento del software.

6.7 Rientra nelle facoltà dell'U.O.C. Sistemi Informativi bloccare automaticamente il download - da siti non istituzionali o non affidabili - di software potenzialmente infetto. Nel caso in cui sia ritenuto necessario "scaricare" determinati files dalla rete ed il relativo download risulti bloccato, l'utente dovrà formulare una richiesta. L'U.O.C. Sistemi Informativi,

[1] Con ciò intendendosi software installabili, portabili, driver, screen saver etc…

previe le verifiche tecniche del caso, provvederà ad autorizzare il download. Nel caso in cui la richiesta di download sia legata alla necessità di installazione di un software non ricompreso tra quelli aziendali, il richiedente dovrà fare inoltrare dal proprio responsabile una richiesta ai Sistemi Informativi che procederanno dopo valutazione tecnica.

6.8 Gli utenti devono essere consapevoli che l'inosservanza delle disposizioni sopra elencate potrebbe esporre l'Azienda a gravi ripercussioni in sede di giustizia civile; si evidenzia altresì come le violazioni della normativa a tutela del diritto d'Autore vengano sanzionate anche penalmente.

Si richiede pertanto agli utenti di tenere sempre un comportamento diligente ed attento nell'utilizzo del software, in modo da rendere sicuro il proprio lavoro e tutelare altresì l'Ente.

Art. 7 - Utilizzo del Personal Computer

7.1 La postazione di lavoro (PC, Stampante, Monitor, Scanner, ecc.ecc.) affidata all'utente é uno strumento di lavoro che deve essere custodito con cura ed adottando ogni precauzione necessaria ad evitare qualsiasi possibile forma di danneggiamento. L'utilizzo non inerente all'attività lavorativa è vietato, poiché può comportare disservizi e - soprattutto - minacce alla sicurezza, ad eccezione di quanto previsto dal Codice di Comportamento Aziendale sull'utilizzo di strumenti informatici forniti dall'Azienda.

Gli utenti, nel compimento delle normali attività mediante gli strumenti informatici:

- devono accedere con ed utilizzare esclusivamente l'account del quale sono stati forniti, identificandosi con il nome utente assegnato e la relativa password. I lavoratori che hanno necessità di utilizzare, per determinate finalità, un account dotato di maggiori privilegi ed hanno le necessarie competenze a tal fine, ricevono dall'U.O.C. Sistemi Informativi un account privilegiato che dovrà comunque essere utilizzato solamente quando necessario per la realizzazione delle specifiche e limitate attività che lo richiedono. Al contrario, per le operazioni ordinarie anche tali utenti dovranno utilizzare l'account non amministratore;
- non devono in alcun modo modificare, rimuovere e/o disattivare le misure di sicurezza predisposte nel dispositivo, né compiere azioni di modifica dei sistemi (ad esempio: disattivare gli aggiornamenti del sistema operativo, la protezione in tempo reale dell'antivirus o il suo aggiornamento automatico, il firewall del sistema operativo ecc.ecc.);
- non devono utilizzare account diversi da quello assegnato.

Gli utenti dovranno prestare la massima attenzione nell'apertura di documenti che richiedono l'attivazione di particolari funzionalità (ad esempio le c.d. macro nei file excel e word). Le stesse dovranno essere consentite esclusivamente quando l'utente è certo della provenienza legittima del documento e, in caso di minimo dubbio, non dovrà mai consentire l'esecuzione del codice, dovendosi piuttosto rivolgere per la necessaria consulenza ai Tecnici dell'U.O.C. Sistemi Informativi. La stessa regola di prudenza vale altresì per l'apertura di link inviati mediante e-mail od altre forme di comunicazione, i quali dovranno prima essere vagliati circa la loro provenienza ed apparente sicurezza.

Le credenziali di accesso al sistema non vanno in alcun modo riportate in fogli od altri supporti cartacei, né vanno salvate in file di testo sul computer od altri documenti digitali ovunque riposti. Inoltre le stesse non devono in alcun caso essere comunicate (a voce o in altre forme) ad altri collaboratori e/o terzi.

Nel modificare la password di accesso, dovranno essere sempre rispettati i necessari parametri di sicurezza, ovvero:

- lunghezza minima di 12 caratteri;
- divieto di utilizzo di parole di senso comune od informazioni relative alla persona (data di nascita ecc.ecc.);
- utilizzo di caratteri sia minuscoli che maiuscoli e di numeri;
- utilizzo di almeno un carattere speciale;

Le postazioni di lavoro fisse devono essere mantenute in ordine, pulite e prive di pericoli per i sistemi informatici.

7.2 I tecnici dell'U.O.C. Sistemi Informativi sono autorizzati a compiere interventi nel sistema informatico aziendale diretti a garantirne la manutenzione e la sicurezza. Nel rispetto della normativa Europea e Nazionale in tema di protezione dei dati personali, detti interventi potranno anche comportare - ove necessario - l'accesso ai dati trattati dal sistema, ivi compresi gli archivi di posta elettronica.

I tecnici dell'U.O.C. Sistemi Informativi potranno in qualunque momento procedere alla rimozione di file ed applicativi ritenuti non sicuri.

7.3 Il personale incaricato dell'U.O.C. Sistemi Informativi ha la facoltà - in caso di richiesta o di stretta necessità - di collegarsi da remoto al desktop delle singole postazioni PC, al fine di garantire l'assistenza tecnica necessaria nonché la sicurezza contro eventuali malware.

Qualora sul PC in dotazione venissero trattati dati sensibili, in base alla normativa vigente, la password di accesso dovrà essere modificata ogni 3 mesi.

7.4 È fatto assoluto divieto all'utente di intervenire in qualunque modo sull'hardware in dotazione. In caso di malfunzionamento delle apparecchiature assegnate, l'utente è tenuto a darne tempestiva segnalazione al personale dell'U.O.C. Sistemi Informativi. La manutenzione delle apparecchiature pertanto è di assoluta pertinenza dei tecnici dell'U.O.C. Sistemi Informativi.

7.5 Il Personal Computer deve essere spento al termine dell'utilizzo od in caso di assenze prolungate dall'ufficio. Inoltre, lo stesso va sospeso non appena ci si allontana dalla postazione di lavoro, in modo da impedirne l'utilizzo ad opera di terzi.

7.6 È vietato agli utenti l'utilizzo di PC personali salvo casi espressamente autorizzati dalla Direzione Generale.

7.7 Il corretto smaltimento del materiale di consumo sarà a carico dell'utente, che dovrà rispettare la normativa vigente ed eventuali direttive aziendali, con relative sanzioni in caso di inosservanze.

7.8 È necessario inoltre, mantenere il desktop più pulito possibile, lasciando soltanto i collegamenti e le cartelle condivise strettamente necessarie.

Art. 8 - Utilizzo di PC portatili

8.1 Considerati i maggiori rischi di sicurezza derivanti dall'utilizzo di dispositivi mobili, l'Ente potrà assegnare all'utente un PC portatile solamente nel caso di effettiva necessità e previa ed esauriente relazione sottoscritta dal Direttore del Dipartimento o Responsabile della Struttura e parere favorevole dell'U.O.C. Sistemi Informativi.

8.2 L'utente è responsabile del PC portatile assegnatogli e **deve custodirlo con la massima diligenza possibile**, sia durante gli spostamenti che durante l'utilizzo sul luogo di lavoro, evitando di esporre lo stesso al rischio di manomissioni e furto.

8.3 Ai PC portatili si applicano le medesime regole di utilizzo previste dal presente regolamento per i Personal Computer. Particolare attenzione deve essere rivolta all'utilizzo temporaneo del PC portatile, essendo necessario rimuovere - prima della riconsegna - eventuali file salvati.

8.4 Eventuali connessioni di rete, dirette verso la rete aziendale o verso la rete esterna, possono essere configurate esclusivamente seguendo le medesime procedure previste per l'accesso alla rete intranet/internet nel successivo art.12.

8.5 Tutti i notebook sono protetti da crittografia del disco e la chiave di ripristino è conservata presso i SI.

Art. 9 – Utilizzo dei telefoni cellulari

9.1 Il telefono cellulare affidato all'utente è uno strumento di lavoro che deve essere custodito con cura, adottando ogni precauzione necessaria ad evitare il danneggiamento e la perdita. È lecito installare applicazioni non aziendali sul telefono ma solo se necessarie per lo svolgimento dell'attività lavorativa. È necessario ricordare che in caso di richiesta da parte di autorità di polizia tutti i log dell'attività svolta con l'uso di strumenti informatici potranno essere oggetto di attività di indagine.

Art. 10 - Trattamento e conservazione dei dati

10.1 Ciascun utente è responsabile del corretto trattamento e dell'archiviazione sicura dei dati e delle informazioni utilizzate (documenti informatici, database ecc.ecc.). A tal fine, gli utenti devono conservare i file, i documenti informatici ed in generale tutte le informazioni digitali create/utilizzate, unicamente nel File Server (cartelle condivise) a tal uopo rese disponibili dall'Ente a mezzo dell'U.O.C. Sistemi Informativi. Il salvataggio dei dati e dei documenti nelle apposite cartelle condivise e non in locale sul proprio PC - o su altri dispositivi - deve considerarsi attività vincolante, in quanto finalizzata ad evitare perdite di dati derivanti dal mancato backup dei dati conservati al di fuori del File Server.

10.2 Ai dipendenti che trattano dati personali e/o informazioni aziendali riservate è richiesto di prestare la massima diligenza possibile – ed imposta dal rispettivo ruolo – nel trattamento dei predetti dati.

In particolare, gli utenti sono tenuti al riserbo sulle informazioni di cui vengono a conoscenza e tale obbligo si traduce altresì nell'utilizzo corretto e attento degli strumenti informatici che contengono quei dati.

Pertanto i dipendenti dovranno attenersi alle misure di sicurezza indicate e fare quanto in loro potere per proteggere la riservatezza, l'integrità e la disponibilità dei dati aziendali, senza duplicarli, trasferirli, distruggerli e modificarli indebitamente.

I dipendenti dovranno altresì segnalare prontamente qualsiasi vulnerabilità di cui vengono a conoscenza, nonché l'utilizzo improprio dei dispositivi e dei software da chiunque posto in essere.

Agli utenti è altresì richiesto di impegnarsi attivamente nella formazione offerta dall'Azienda e/o da fornitori terzi, in modo da acquisire e rinforzare le competenze necessarie a trattare in sicurezza i dati personali e/o comunque riservati.

10.3 In caso di cessazione del rapporto di lavoro gli account utente vengono disattivati e i dati delle cartelle condivise restano sul server aziendale. Nel caso in cui l'utente avesse in uso un PC portatile, lo stesso viene restituito al proprio dirigente responsabile che provvederà a riassegnarlo ad altra unità di personale oppure a restituirlo ai Sistemi Informativi. Per i dispositivi oggetto di rottamazione si procede con l'estrazione delle memorie di massa che vengono conservate in

un luogo sicuro e sottochiave, trascorsi sei mesi tali memorie vengono smaltite in maniera tale da non poter più accedere ai dati che vi erano memorizzati.

ACCESSO INTERNET/INTRANET, POSTA ELETTRONICA E GESTIONALI

Art. 11 - Internet e Posta Elettronica

11.1 Le credenziali di autenticazione per l'accesso alla rete e per l'utilizzo del servizio di Posta Elettronica vengono assegnate dal personale dell'U.O.C. Sistemi Informativi, previa formale richiesta da effettuare mediante la compilazione dell'apposita modulistica disponibile nel sito web aziendale sottoscritta, qualora previsto, dal Dirigente Responsabile della struttura presso la quale l'utente opera o dovrà operare.

Nel caso di collaboratori a progetto e coordinati e continuativi, stagisti, etc., la richiesta preventiva verrà inoltrata direttamente dal Dirigente Responsabile della struttura con la quale il collaboratore si coordina nell'espletamento del proprio incarico.

Nel caso in cui il dipendente/collaboratore/stagista cessi o abbia cessato il rapporto con l'Azienda; sarà cura del Responsabile dell'U.O. di appartenenza dare tempestiva comunicazione all' U.O.C. Sistemi Informativi al fine di evitare un possibile uso illecito dei servizi forniti e delle credenziali di autenticazione.

La modulistica relativa alla concessione dei privilegi di accesso agli applicativi aziendali sarà da utilizzare anche nei casi di trasferimento/spostamento dei dipendenti presso UU.OO. diverse da quelle nelle quali il soggetto prestava servizio al momento della concessione.

Sarà quindi cura del precedente Responsabile dell'U.O. di appartenenza comunicare il trasferimento del dipendente e quindi la cessazione all'utilizzo del servizio; un eventuale riattivazione sarà successivamente possibile previa nuova autorizzazione concessa dal Responsabile dell'U.O. presso cui opererà il dipendente.

11.2 Le credenziali di autenticazione consistono in un nome utente o *userid* volto ad identificare univocamente il soggetto ed assegnato dall'U.O.C. Sistemi Informativi, associato ad una password che dovrà essere custodita dall'utente e da questi mantenuta riservata.

Non è ammesso in alcun caso l'accesso a servizi e sistemi senza previa autenticazione con le predette credenziali identificative.

11.3 Al primo accesso, sarà necessario procedere alla modifica della password e, successivamente, variarla ogni sei mesi (tre mesi nel caso di accesso a sistemi afferenti a dati sensibili) senza utilizzare password già impiegate ed attenendosi strettamente ai requisiti di robustezza indicati nell'art. 7. La password dovrà essere immediatamente modificata nel caso in cui si sospetti che la stessa sia stata violata, comunicando l'anomalia all'U.O.C. Sistemi Informativi.

11.4 Qualora la password venisse dimenticata e l'utente non avesse eseguito la registrazione al software per il recupero della password, si procederà alla sua sostituzione d'intesa con il personale dell'U.O.C. Sistemi Informativi che provvederà, in seguito alla segnalazione, a fornire direttamente all'interessato le nuove credenziali di autenticazione; resta inteso che sarà cura dell'utente modificare la password al primo accesso.

Art. 12 - Programmi Gestionali

12.1 È possibile ottenere l'assegnazione di specifiche credenziali di autenticazione a programmi gestionali specifici dietro compilazione - a cura del Dirigente Responsabile - di apposita modulistica presente nell'area modulistica del sito della ASL, ovvero da richiedere all'U.O.C. Sistemi Informativi.

12.2 Qualora l'utente sia in possesso di credenziali che gli consentano l'accesso a procedure gestionali (es. Accesso al sistema AMC, Accesso sistema Rilevazione Presenze, Gestione Tessera Sanitaria, Archiflow, etc.) o a dati sensibili, il sopraindicato modulo dovrà essere compilato a cura del dirigente Responsabile ed inviato all'U.O.C. Sistemi Informativi, anche in caso di trasferimento del dipendente ad altra struttura o eventuale cessazione del rapporto di lavoro con l'Azienda.

12.3 In caso di cessazione del rapporto di lavoro agli utenti, viene mantenuto l'acceso al portale dei dipendenti per ulteriori 3 mesi (per la consultazione di cedolini, CUD, …), successivamente ci sarà la disattivazione al servizio e l'utente potrà rivolgersi direttamente all'ufficio del personale.

Art. 13 - Raccolta dei log

13.1 Gli utenti sono resi edotti del fatto che i sistemi e gli apparati di rete utilizzati a fini lavorativi registrano le attività in essi eseguite mediante generazione e conservazione dei c.d. *log* di sistema.

Tali log contengono informazioni quali data ed ora dell'evento, id dell'utente, nome del computer, software avviato od installato, file creati ecc.ecc.

La raccolta di tali log non è in alcun modo legata ad attività di controllo degli utenti, essendo gli stessi unicamente finalizzati a garantire la sicurezza dei sistemi e delle reti. Difatti, l'analisi e la correlazione degli eventi permettono di rilevare anomalie e possibili incidenti di sicurezza, in tal modo permettendo il contenimento dei danni e - soprattutto - il rispetto di tutte quelle normative (in primis il Regolamento Europeo sulla protezione dei dati personali) che richiedono la predisposizione di misure tecnico-organizzative finalizzate alla protezione dei dati.

Pertanto i log saranno raccolti, correlati e periodicamente analizzati al fine di rilevare eventi pericolosi, vulnerabilità ed attività sospette o condotte in violazione delle politiche aziendali. I log conservati potranno altresì costituire oggetto di ulteriori attività di indagine, anche a richiesta delle Autorità esterne competenti.

13.2 I tempi di conservazione dei log sono di 180 giorni.

Art. 14 - Utilizzo della rete Aziendale

14.1 È fatto assoluto divieto, agli utenti, di connettere alla rete aziendale dispositivi non autorizzati e preventivamente configurati dall'U.O.C. Sistemi Informativi, essendo quest'ultimo l'unico soggetto abilitato a provvedere alla connessione di apparati di rete (router, switch, ecc.ecc.) e dispositivi (PC, stampanti di rete, ecc.ecc.) e configurarli. Non sarà pertanto possibile provvedere autonomamente a configurazioni manuali diverse da quelle impostate dall'U.O.C. Sistemi Informativi, come ad esempio modificare l'indirizzo ip statico del pc, l'indirizzo ip del server dns da contattare ecc.ecc..

Qualsiasi eventuale richiesta di modifica della configurazione di rete dovrà essere avanzata e giustificata all'U.O.C. Sistemi Informativi.

14.2 È fatto assoluto divieto all'utente di intercettare, analizzare, modificare in qualsiasi modo od ostacolare il traffico sulla rete aziendale.

14.3 L'utilizzo di reti Wireless deve essere autorizzato dall'U.O.C. Sistemi Informativi e, nel caso di installazione nelle vicinanze di apparecchiature medicali, comunicato al Servizio di Ingegneria Clinica che dovrà valutare la compatibilità con le apparecchiature esistenti.

14.4 Le cartelle utenti, o cartelle dei dipartimenti presenti nei server dell'Azienda 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 dislocato, nemmeno per brevi periodi, in queste unità.

Art. 15 – Misure di sicurezza in modalità di lavoro agile

15.1 Ogni utente coinvolto nel lavoro agile è vincolato ad applicare le norme descritte nel Regolamento Lavoro Agile settore comparto (https://www.aslteramo.it/regolamento-aziendale-per-la-disciplina-del-lavoro-agile-del-personale-del-comparto-dellazienda-2/). Inoltre, come previsto dall'art. 6 comma 2 del citato regolamento, il dipendente è responsabile della sicurezza dei dati. Il lavoro agile, per i rischi maggiori che lo stesso comporta, richiede una maggiore attenzione agli utenti, i quali dovranno attenersi scrupolosamente alle istruzioni impartite.

15.2 Il presente articolo individua le specifiche tecniche minime di custodia e sicurezza dei dispositivi elettronici e dei software, nonché le regole necessarie a garantire la protezione dei dati e delle informazioni dell'azienda. In particolare, disciplina le modalità di accesso ed utilizzo degli strumenti informatici nell'ambito della modalità di lavoro agile (in seguito anche smart working) a cui sia stato concesso l'uso di risorse informatiche di proprietà dell'azienda.

15.3 La UOC Sistemi Informativi, competente in materia di sistemi informativi (in seguito anche "Sistemi Informativi"), supporta il servizio di assistenza agli utenti (lavoratori agili), avvalendosi di personale specializzato, sia esso personale dipendente dell'azienda stessa, che personale esterno in outsourcing. L'accesso al lavoro agile può avvenire solamente per gli utenti a ciò autorizzati dall'Azienda.

15.4 Al dipendente in modalità di lavoro agile viene fornito un portatile aziendale che si collega automaticamente in VPN alla rete aziendale senza richiedere l'intervento da parte dell'utente, che quindi lavora a tutti gli effetti come se fosse in presenza.

15.5 Al dipendente in modalità di lavoro agile sono attribuite le stesse credenziali di autenticazione per l'accesso ai servizi informatici dell'azienda. L'accesso in VPN è consentito solo tramite dispositivi aziendali, pertanto i sistemi informativi non abilitano gli utenti ma abilitano i dispositivi installando il software necessario ed eseguendo le opportune configurazioni.

15.6 Il dipendente/collaboratore dovrà applicare quanto già previsto in ambito di sicurezza informatica nel presente regolamento informatico aziendale.

15.7 Le prescrizioni del presente documento si applicano ai dipendenti aziendali coinvolti nell'espletamento dell'attività lavorativa in modalità agile.

15.8 L'azienda si riserva di effettuare verifiche sul corretto utilizzo degli strumenti informatici.

15.9 La violazione da parte degli utenti delle norme contenute nel presente documento comporta l'applicazione delle sanzioni previste dalle disposizioni contrattuali vigenti in materia.

15.10 In caso di smarrimento e/o il furto di un portatile è necessario segnalarlo in maniera tempestiva ai Sistemi Informativi in quanto sarà necessario provvedere al blocco della connessione automatica in VPN.

15.11 Nelle more di completare l'approvvigionamento dei dispositivi portatili e delle licenze d'uso necessarie per lo svolgimento del lavoro agile tramite dispositivi aziendali, saranno mantenuti gli accessi VPN tramite dispositivi personali dei dipendenti.

Art. 16 - Navigazione in Internet

16.1 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.

16.2 L'accesso alla rete Internet è da intendersi quale "strumento di lavoro". In tal senso, l'utente non potrà utilizzare internet, ad esempio, per:

- caricare o scaricare software non autorizzato, audio o video od altri file comunque non attinenti alla propria attività lavorativa e/o illegali;
- visitare siti di streaming od altri espositori di contenuti di vario carattere (ludico, filmico etc…) non attinenti alle mansioni lavorative;
- 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 Dirigente Responsabile della propria U.O. 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 line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames) se non espressamente autorizzati dal Responsabile d'ufficio;
- l'accesso, tramite internet, a caselle webmail di posta elettronica personale.

16.3 Al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa, l'ASL potrà adottare uno specifico sistema di blocco o filtro automatico (sistema di Web Filtering) che prevenga determinate operazioni.

16.4 La consultazione, ai soli fini lavorativi, di specifici siti non istituzionali sarà possibile attraverso l'abilitazione all'accesso che dovrà essere richiesta compilando uno specifico modulo online; è necessario indicare l'esatto indirizzo del sito internet da abilitare ed il motivo della richiesta. Sarà facoltà dell'Azienda U.S.L. nominare un'apposita commissione per valutare l'ammissibilità della richiesta.

16.5 L'Amministrazione utilizza, attraverso personale tecnicamente competente, strumenti elettronici sia per esigenze produttive e/o organizzative (per es. per rilevare anomalie o per manutenzioni), sia per esigenze di sicurezza sul lavoro. Nelle suddette ipotesi l'Amministrazione si avvarrà legittimamente, nel rispetto dell'art. 4, comma 2, della legge 300/1970 (Statuto dei Lavoratori) di sistemi informatici ed elettronici che consentono indirettamente un controllo a distanza e

determinano un trattamento di dati personali riferiti o riferibili ai lavoratori. Ciò sarà possibile anche in presenza di attività di controllo discontinue.

L'Amministrazione, inoltre, nell'esercizio delle sue prerogative datoriali di direzione e organizzazione del lavoro, si riserva periodicamente, e almeno su base annuale, di porre in essere le seguenti attività:

- selezione del personale autorizzato alla navigazione online;
- valutazione dell'impatto dei controlli sui lavoratori;
- individuazione di categorie di siti considerati correlati o meno con la prestazione lavorativa;
- configurazione di sistemi o utilizzo di filtri che prevengano determinate operazioni – reputate incoerenti con l'attività lavorativa – quali l'upload o l'accesso a determinati siti (inseriti in una sorta di black list) e/o il download di file o software aventi particolari caratteristiche (dimensionali o di tipologia di dato);
- trattamento di dati in forma anonima o tale da precludere l'immediata identificazione di utenti mediante loro opportune aggregazioni (ad es., con riguardo ai file di log riferiti al traffico web, su base collettiva o per gruppi sufficientemente ampi di lavoratori);
- eventuale conservazione nel tempo dei dati attraverso i registri di log (almeno 90 giorni) strettamente limitata al perseguimento di finalità organizzative, produttive e di sicurezza.

Gli eventuali controlli, compiuti dal personale incaricato dell'U.O.C. Sistemi Informativi su richiesta dell'Amministrazione, potranno avvenire mediante un sistema di controllo dei contenuti (Proxy server) o mediante "file di log" della navigazione svolta. Il controllo sui file di log non è continuativo ed i file stessi vengono conservati in base alla normativa vigente.

Art. 17 - Corsi On Line

17.1 Sarà possibile per i dipendenti seguire dei Corsi On Line secondo le modalità di seguito riportate:

- preventiva autorizzazione da parte del Responsabile dell'U.O.;
- preventiva autorizzazione del Responsabile dell'Ufficio Formazione;

L'orario del Corso dovrà essere compatibile con la gestione della rete aziendale, dovrà essere svolto nella fascia oraria in cui il traffico di rete risulta minore, pertanto sarà facoltà del personale dell'U.O.C. Sistemi Informativi concedere o meno l'abilitazione.

Art. 18 - Posta Elettronica

18.1 Per lo svolgimento delle mansioni lavorative, viene attribuita, a tutti i dipendenti, una casella di posta elettronica aziendale.

Nel caso personale non dipendente, l'abilitazione alla posta elettronica deve essere preceduta da regolare richiesta del Responsabile dell'U.O. di appartenenza, tramite il medesimo modulo utilizzato per l'accesso alla rete intranet/internet, previsto nel precedente punto 11.1.

Si raccomanda di utilizzare l'e-mail esclusivamente per finalità legate all'attività lavorativa.

18.2 Le caselle di posta sono nominative e vengono assegnate utilizzando il seguente formato:

nome.cognome@aslteramo.it

Possono essere assegnate, qualora si rendesse necessario per esigenze organizzative del lavoro, dietro richiesta del Responsabile dell'U.O., delle caselle di posta istituzionali del tipo:

urp@aslteramo.it

direzione.generale@aslteramo.it

Qualora fosse necessaria una maggiore dimensione della casella di posta, farne richiesta all'U.O.C. Sistemi Informativi.

18.3 L'accesso alla casella di posta elettronica è possibile attraverso la Home Page del sito aziendale (www.aslteramo.it) utilizzando le apposite credenziali di autenticazione fornite come indicato in precedenza.

La casella di posta deve essere mantenuta in ordine, cancellando messaggi e/o allegati inutili per l'attività lavorativa e che alla lunga saturano lo spazio disponibile. Si ricorda a tal fine che sarà necessario eliminare tali messaggi/allegati inutili anche nelle cartelle POSTA INVIATA, POSTA ELIMINATA; si raccomanda inoltre di procedere all'eliminazione definitiva dei messaggi che vengono spostati nella cartella POSTA ELIMINATA.

18.4 La casella di posta, assegnata dall'Azienda all'utente, è uno strumento di lavoro in uso all'addetto solamente per la resa della prestazione lavorativa.

Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse pertanto:

- È vietato utilizzare l'indirizzo e caselle di posta elettronica aziendale, nel formato previsto nome.cognome@aslteramo.it, per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mailing-list salvo diversa ed esplicita autorizzazione.
- È vietato utilizzare la login / password di un altro utente per accedere in sua assenza alla sua posta elettronica.
- È vietato inviare catene telematiche (le cosiddette "catene di Sant'Antonio"). Se si dovessero ricevere messaggi di tale tipo, non si devono in alcun caso attivare gli allegati di tali messaggi.

18.5 Nel caso di prolungata assenza improvvisa o prolungata dell'utente o in situazioni di emergenza, qualora si renda necessario per esigenze lavorative, accedere alla posta elettronica o alla postazione di lavoro dell'utente, l'interessato dovrà esser messo in grado di delegare un altro lavoratore (fiduciario) a verificare il contenuto di messaggi e a inoltrare al titolare del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. L'utente dovrà inoltre configurare il risponditore automatico in cui comunica della momentanea indisponibilità personale.

18.6 È possibile ottenere per via informatica, nelle comunicazioni esterne ed interne all'azienda, una segnalazione di verifica sia relativamente al recapito del messaggio che all'avvenuta lettura; si ricorda però che la conferma dell'avvenuta lettura del messaggio da parte del destinatario è a sua propria discrezione, essendo il servizio di posta elettronica ordinaria in uso presso l'Azienda non certificato.

18.7 I Dirigenti Responsabili dei servizi a cui sono state assegnate caselle di Posta Elettronica Certificata (detta anche PEC) hanno l'obbligo di garantirne il controllo periodico. Tale controllo avviene, se possibile, con cadenza giornaliera.

La Posta Elettronica Certificata (detta anche PEC) è un sistema di comunicazione simile alla posta elettronica standard a cui si aggiungono delle caratteristiche di sicurezza e di certificazione della trasmissione tali da aggiungere un valore legale ai messaggi. Il valore legale è assicurato dai gestori di posta PEC del mittente e del destinatario che certificano:

a) Data e ora dell'invio del messaggio da parte del mittente;

b) Data e ora dell'avvenuta consegna del messaggio al destinatario;

c) Integrità del messaggio (ed eventuali allegati) nella trasmissione da mittente a destinatario.

La comunicazione ha valore legale solo se inviata da una casella PEC e ricevuta da un'altra casella PEC.

18.8 Si raccomanda sempre di:

- controllare il mittente dell'e-mail, nella consapevolezza che lo stesso può essere falsificato. Pertanto l'utente non dovrà mai dare per scontato che il mittente apparente corrisponda al mittente reale, dovendosi piuttosto interrogare se il resto dell'email appaia effettivamente proveniente da quel mittente o vi siano invece elementi strani che lascino presumere un pericolo di contraffazione dell'email (nel qual caso l'email dovrà essere chiusa – non cancellata - e i Tecnici dell'U.O.C. Sistemi Informativi contattati per le dovute verifiche);
- non cliccare su link contenuti nell'email, a meno che non si sia sicuri della provenienza legittima della e-mail. Anche in tal caso, comunque, se si ha il dubbio che il link abbia una forma strana oppure la sua presenza sia ingiustificata e/o fuori contesto, occorre non cliccarlo;
- non scaricare e/o aprire allegati che presentano estensioni strane, e comunque gli allegati che consistono in eseguibili (aventi estensione .exe) oppure archivi (aventi estensione .zip, .rar etc…) protetti da password;
- non utilizzare la posta elettronica per trasmettere password ed altre informazioni particolarmente sensibili;
- prestare particolare attenzione alle e-mail che giungono da mittenti sconosciuti, nonché quelle che – sebbene non bloccate dai meccanismi anti-spam – contengono inviti, pubblicità, offerte, premi ed altri contenuti non aventi carattere lavorativo;
- prestare particolare attenzione alle e-mail apparentemente legittime, che giungono ad esempio da soggetti appartenenti all'assistenza tecnica informatica, oppure da altre articolazioni non note dell'Azienda e così via, nel momento in cui avanzino delle richieste fuori dall'ordinario;
- prestare particolare attenzione e segnalare immediatamente quelle e-mail – anche se apparentemente legittime – che richiedono la trasmissione o l'inserimento in pagine web esterne (anche conosciute) di password od altri dati personali.

Come regola generale, in qualsiasi caso di sospetto od incertezza circa una e-mail, prima di scaricarne gli allegati o cliccare sui relativi link, chiedere supporto ai Tecnici dell'U.O.C. Sistemi Informativi.

18.9 L'iscrizione a "mailing list" esterne è consentita solamente per motivi professionali. Prima di iscriversi verificare sempre l'affidabilità del servizio.

18.10 Si fa presente che le e-mail trasmesse non saranno garantite da tecniche crittografiche e dunque saranno visionabili da eventuali terzi che entrassero nel possesso delle stesse. Pertanto è vietato utilizzare la posta elettronica per inviare all'esterno comunicazioni che contengono informazioni, dati sensibili e credenziali e password in chiaro.

18.11 È fatto divieto di inviare o memorizzare messaggi di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.

18.12 In caso di cessazione del rapporto di lavoro la posta elettronica sarà disattivata quando l'ufficio del personale comunicherà l'avvenuta cessazione del rapporto; dalla disattivazione, Microsoft permette il recupero della casella di posta entro 30 giorni dalla disattivazione. Trascorsi i 30 giorni il recupero delle caselle di posta elettronica – se richiesto dell'autorità giudiziaria - sarà possibile solo per alcune caselle dotate di idonea licenza disponibile in numero limitato.

Art. 19 - Osservanza della normativa aziendale

19.1 Il mancato rispetto o la violazione delle regole contenute nel presente regolamento è perseguibile con provvedimenti disciplinari nonché con le azioni civili e penali consentite.

Art. 20 - Aggiornamento e revisione

20.1 Il presente Regolamento è soggetto a revisione periodica. Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni o modifiche al presente Regolamento tramite comunicazione alla Direzione Aziendale.