Regolamento per l'utilizzo della dotazione informatica aziendale, della posta elettronica e dell'accesso a Internet

Scopo del presente Regolamento è quello di fornire le informazioni necessarie per un corretto utilizzo di Internet, delle risorse informatiche aziendali fisse e mobili e della posta elettronica da parte di tutti i dipendenti dell'Azienda Sociosanitaria Ligure Asl 3, tenuto conto che il progressivo sviluppo tecnologico e la rapida diffusione delle relative strumentazioni informatiche espone l'Azienda a problematiche che potrebbero incidere sulla sicurezza, sulla disponibilità e sull'integrità dei sistemi informativi aziendali e delle informazioni ivi gestite.

Premesso che l'utilizzo delle strumentazioni informatiche deve uniformarsi ai principi della diligenza e della correttezza, l'Asl 3, nel rispetto delle disposizioni in materia di tutela dei dati personali e sensibili e delle norme a tutela dei lavoratori, ha predisposto le seguenti disposizioni per assicurare la funzionalità e il corretto impiego dei suddetti mezzi da parte dei dipendenti, definendone le modalità d'uso nell'organizzazione dell'attività lavorativa.

L'uso di tali apparecchiature deve essere disciplinato da norme certe in quanto da comportamenti – anche inconsapevolmente non leciti – possono derivare conseguenza gravi, sia sul piano tecnico (come un blocco delle funzionalità o una perdita di dati) sia sul piano giuridico (mediante l'insorgere sia penali sia civili a carico contestualmente dell'Ente e del lavoratore).

L'S.C. Sistemi Informativi Aziendali, interpretando gli obiettivi e le competenze dell'Azienda ASL, e in accordo il mandato attribuito dalla Direzione Aziendale, ha il compito di garantire il funzionamento di un sistema di posta elettronica e di accesso alla Intranet e a Internet unicamente per gli scopi istituzionali.

Tutto il personale dell'Azienda è tenuto a osservare quanto specificato nel presente regolamento ed è invitato a segnalare tutte le violazioni alle disposizioni specificate di cui viene a conoscenza alla Direzione della propria Struttura.

Tutto ciò premesso, si ritiene utile adottare ulteriori regole interne, dirette ad evitare che comportamenti inconsapevoli e/o scorretti possano innescare problemi o minacce alla Sicurezza nel trattamento dei dati e, al fine, occorre che ciascun dipendente si uniformi al rispetto delle seguenti regole al fine di adempiere correttamente alle disposizioni legislative.

Si ricorda che per trattamento dei dati si intende "qualunque operazione o complesso di operazioni concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione dei dati". In tale ottica è indifferente che le operazioni vengano svolte con o senza l'ausilio di mezzi elettronici, o comunque automatizzati, per cui anche i trattamenti effettuati su supporto cartaceo sono assoggettati alla normativa privacy.

Pertanto le operazioni di trattamento si possono idealmente suddividere in tre macro-tipologie, in funzione del fatto che il loro fine sia:

a) Il reperimento delle informazioni

Tale fase è tecnicamente definita raccolta di dati, ovvero l'acquisizione delle informazioni, in qualunque modo essa avvenga: ad esempio, direttamente dalla persona interessata, presso terzi, o mediante consultazione di elenchi.

b) Il trattamento "interno" delle informazioni.

Si raggruppano in tale macro-tipologia le varie operazioni, poste in essere da chi raccoglie informazioni per organizzarle e renderle agevolmente usufruibili.

Esse sono:

- la registrazione dei dati, cioè il loro inserimento in supporti, automatizzati o manuali, al fine di rendere i dati disponibili per i successivi trattamenti;
- l'organizzazione dei dati in senso stretto, cioè il processo di lavorazione che ne favorisca la fruibilità attraverso l'aggregazione o la disaggregazione, l'accorpamento, la catalogazione eccetera;
- l'elaborazione, ovvero le operazioni che attribuiscono significatività ai dati in relazione allo scopo per il quale essi sono stati raccolti;
- la selezione, la estrazione ed il raffronto, specifiche che rientrano nella ipotesi più generale della elaborazione;
- la modificazione dei dati registrati, in relazione a variazioni o a nuove acquisizioni;

- l'interconnessione, ovvero la messa in relazione di banche dati diverse e distinte tra loro al fine di compiere ulteriori processi di elaborazione, selezione, estrazione o raffronto;
- il blocco, ovvero la conservazione dei dati con sospensione temporanea dei trattamenti;
- la conservazione dei dati, alla quale la legge dedica particolari attenzioni sotto il profilo della sicurezza;
- la cancellazione o la distruzione dei dati, anch'esse operazioni il cui compimento fa sorgere l'obbligo di effettuare taluni adempimenti.

c) L'uso delle informazioni nei rapporti con l'esterno.

Sono i trattamenti più delicati, in quanto è con essi che si può concretamente ledere la sfera della privacy altrui: essi vengono genericamente definiti come utilizzo, ovvero la realizzazione dello scopo per cui si è provveduto alla raccolta e ai trattamenti interni.

L'utilizzo può essere:

- diretto, instaurando cioè un rapporto con la persona sul conto della quale si sono raccolte informazioni;
- ovvero consistere nel mettere a disposizione di terzi le informazioni raccolte.

Le operazioni di utilizzo a cui la legge dedica le maggiori attenzioni, in quanto si tratta di quelle potenzialmente più lesive della privacy, sono quelle con cui si mettono a disposizione di terzi i dati personali.

Esse sono:

- la comunicazione, cioè il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- la diffusione, cioè il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

Affinché i dipendenti evitino di porre in essere inconsapevoli comportamenti incompatibili con la correttezza professionale richiesta e/o con il corretto svolgimento della prestazione lavorativa da parte degli stessi e nel pieno rispetto delle leggi regolatrici i rapporti di lavoro, si riassumono le

seguenti regole di comportamento di cui è indispensabile la conoscenza da parte di tutti i dipendenti dell'Ente.

1) Normativa di riferimento

Le norme disciplinanti la materia oggetto del presente Regolamento sono da individuare nel Regolamento U.E. 2016/679 del 27/4/2016, e norme attuative, e nel Provvedimento del Garante per la protezione dei dati personali del 1/3/2007 "Lavoro: le linee guida del Garante per posta elettronica e Internet" fatto proprio dal Titolare quale policy aziendale di sicurezza nei trattamenti di dati personali e da intendersi parte integrante del presente regolamento

2) Principi fondamentali

Nell'utilizzo delle dotazioni informatiche devono essere sempre rispettati cinque comportamenti fondamentali di seguito elencati:

RISERVATEZZA: proteggere le informazioni riguardanti il proprio lavoro e l'Azienda. Non condividere con terzi dati, idee, soluzioni, opinioni che riguardano l'attività lavorativa;

ATTENZIONE: restare concentrati sull'attività lavorativa: sui documenti, sui file, sugli strumenti di lavoro; la distrazione può facilmente provocare smarrimenti, diffusione di informazioni a soggetti non autorizzati, errori operativi che possono danneggiare i dati personali, i loro interessati e le società titolari di darti stessi;

PRECISIONE: l'accuratezza nel fare le cose consente di lavorare in modo efficace ed efficiente anche al di fuori del contesto lavorativo. E' fondamentale curare con scrupolosità le conversazioni, l'invio delle mail, il salvataggio dei dati, il ricovero temporaneo di documenti in archivi estranei al perimetro aziendale abituale;

ORDINE: la sistematica e schematica organizzazione delle risorse e degli strumenti di lavoro previene disguidi difficili da risolvere, soprattutto, quando sei fuori dalla tradizionale sede di lavoro. Ogni cosa, ogni file, ogni mezzo devono avere collocazioni e utilizzi abituali e sperimentati;

SEPARATEZZA: è opportuno separare la vita lavorativa dalla sfera privata, familiare e sociale. In questo modo si proteggono anche i propri familiari e amici. Infatti, ogni interferenza può provocare irregolarità o comportamenti non corretti, che dovranno essere oggetto di riparazione, con dispersione di energie e risorse proprie, dell'Azienda e dei terzi coinvolti.

Affinché i dipendenti evitino disporre in essere inconsapevoli comportamenti incompatibili con la correttezza professionale richiesta e/o con il corretto svolgimento della prestazione lavorativa da

parte degli stessi e nel pieno rispetto delle leggi regolatrici i rapporti di lavoro, si riassumono le seguenti regole di comportamento di cui è indispensabile la conoscenza da parte di tutti i dipendenti dell'Ente.

3) Utilizzo del Personal Computer e dei dispositivi informatici fissi e mobili

Ogni dipendente è responsabile delle dotazioni informatiche che gli sono state assegnate, tenendo conto che il personal computer, come ogni altra dotazione informatica assegnata al dipendente, è di proprietà della ASL 3 , e pertanto solo quest'ultima, attraverso le strutture operative dell'S.C. Sistemi Informativi Aziendali ne può curare l'installazione, l'assistenza, il ritiro e l'implementazione.

Non è consentito utilizzare strumenti software e/o hardware atti a intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici, nonché modificare le configurazioni impostate sul proprio PC.

È vietata l'installazione di qualsiasi mezzo di comunicazione non appartenente all'Azienda (per esempio modem, router, access-point).

Ai dipendenti non è consentita la modifica delle caratteristiche hardware e software impostate sui posti di lavoro loro assegnati né l'attivazione della password di accensione (bios), senza preventiva autorizzazione da parte delle strutture operative dell'S.C. Sistemi Informativi Aziendali.

È fatto assoluto e tassativo divieto di installazione autonoma di software, indipendentemente dalla natura e dal possesso della relativa licenza d'uso, se non dopo averne concordato le modalità con le strutture operative dell'S.C. Sistemi Informativi Aziendali.

L'utente può accedere ai servizi informatici aziendali solo utilizzando le proprie credenziali di accesso. È assolutamente vietato cedere o condividere volontariamente con altri le proprie credenziali di accesso.

L'antivirus viene distribuito ed aggiornato centralmente per tutte le postazioni installate sul dominio ASL. Nel caso in cui il software antivirus rilevi la presenza di un virus che non è riuscito a ripulire, all'utente viene notificato un messaggio di allerta. In tal caso dovrà immediatamente sospendere ogni elaborazione in corso - senza spegnere il computer - e segnalare l'accaduto alla S.C. Sistemi Informativi Aziendali.

Ogni dispositivo magnetico (CD/DVD/Chiavette) di provenienza esterna all'Azienda o i supporti di memorizzazione utilizzati sono automaticamente verificati mediante il programma antivirus prima del loro utilizzo e, nel caso venga rilevato un virus non eliminabile dal software, il sistema lo segnala e nega l'accesso alla risorsa infetta. La scansione automatica dei dispositivi non può essere disabilitata dagli utenti di dominio.

Il sistema di esecuzione automatica (autorun) di qualsiasi supporto esterno è disabilitato.

Ogni dipendente accede alla rete aziendale e al proprio personal computer mediante l'utilizzo di credenziali di autorizzazione strettamente personali (USER ID e PASSWORD). Non sono ammesse utenze generiche e condivise. In particolare, per quanto riguarda la password, questa deve essere mantenuta segreta dal dipendente e deve essere costituita da almeno 8 caratteri (o comunque dal numero massimo di caratteri consentito dal personal computer in uso). Non possono essere riutilizzate le ultime quattro password e comunque vanno modificate forzatamente ogni 3 mesi. Possono comunque essere modificate prima della suddetta scadenza. I sistemi informatici di autenticazione che lo consentono sono configurati per la verifica automatica dei requisiti di lunghezza e scadenza delle password.

Gli utenti nominati Amministratori devono impostare la lunghezza delle password di Amministratore a 14 caratteri con criteri di elevata robustezza.

Il personal computer deve essere spento o disconnesso al termine dell'orario di servizio e in caso di allontanamento dalla postazione di lavoro.

ASL 3 ha individuato nel Documento Programmatico sulla Sicurezza aziendale (D.P.S.), di cui alla deliberazione n. 130 del 14/03/2019 apposita procedura che, in caso di prolungata assenza o impedimento dell'incaricato, possa assicurare al soggetto debitamente autorizzato la disponibilità dei dati o degli strumenti elettronici, per gli interventi indispensabili ed indifferibili che si dovessero rendere necessari per ragioni di operatività o di sicurezza del sistema.

L'ASL 3, per garantire il corretto accesso ai dati durante l'eventuale assenza dell'incaricato, su richiesta scritta e motivata del Responsabile della Struttura a cui appartiene l'incaricato stesso, consente alla S.C. Sistemi Informativi Aziendali di consentire l'accesso ai dati redigendone opportuna documentazione.

Come anche riportato nel Documento Programmatico sulla Sicurezza (DPS), viene pertanto adottato il criterio in base al quale in caso di necessità, l'Amministratore di sistema preposto alla gestione delle credenziali di autenticazione degli utenti è abilitato a "rimuovere" la password dell'incaricato e

crearne una nuova da consegnare al Responsabile della Struttura che ha attivato la procedura, consentendo di accedere ai dati o allo strumento informatico per le operazioni necessarie.

L'incaricato del trattamento sarà tempestivamente informato sia della "rimozione" intervenuta delle credenziali, sia dei trattamenti effettuati dal proprio Responsabile e sarà tenuto a modificare la password al suo nuovo primo accesso. In ogni caso la password detenuta precedentemente dall'incaricato non sarà più valida.

Le informazioni archiviate sul personal computer devono essere esclusivamente quelle previste per legge o necessarie per l'esercizio dell'attività lavorativa.

È competenza dei settori tecnici della S.C. Sistemi Informativi Aziendali effettuare il periodico salvataggio dei dati gestiti dalle applicazioni dipartimentali e dei file allocati all'interno di cartelle condivise e gestite centralmente.

Ai dipendenti è demandata la gestione in locale e la relativa archiviazione dei dati che sono memorizzati sulle memorie dei propri personal computer aziendali, effettuando il backup degli stessi con la frequenza ritenuta opportuna e comunque con cadenza almeno settimanale, attraverso l'utilizzo di salvataggi in rete .

Per il salvataggio di tutti i dati per cui si renda necessaria la garanzia della conservazione, devono essere utilizzate le apposite cartelle condivise presenti sui server gestiti centralmente; è vietato mantenere tali informazioni solamente sui dischi locali, che non sono sottoposti alle procedure di backup.

Il personale tecnico interno ed esterno all'Azienda afferente alla S.C. Sistemi Informativi Aziendali, per garantire l'assistenza e il ripristino dei posti di lavoro, è in grado di accedere ai sistemi con proprie credenziali di accesso. Questo personale deve operare nella massima riservatezza e nel rispetto della normativa; eventuali comportamenti difformi alla normativa e a questo regolamento dovranno essere segnalati alla direzione della S.C. Sistemi Informativi Aziendali e annotati nei verbali d'intervento. Al fine di semplificare e migliorare l'assistenza, possono essere utilizzati sistemi di accesso remoto alle postazioni di lavoro; sarà compito del personale tecnico informare l'utente riguardo all'attivazione di queste procedure.

La S.C. Sistemi Informativi Aziendali può effettuare attraverso i propri tecnici, previa informazione ai dipendenti delle singole Strutture, ispezioni volte a verificare l'esistenza di eventuali anomalie e/o a verificare la corretta installazione di software in coerenza alle presenti disposizioni. I tecnici potranno in qualunque momento procedere alla rimozione di file o applicazioni che riterranno essere

pericolosi per la sicurezza delle reti informatiche, sia sui singoli personal computer sia sulle unità di rete.

Le regole di comportamento, finalizzate alla sicurezza dei dati personali, devono essere rispettate anche nell'utilizzo dei dispositivi mobili di servizio, compresa la telefonia.

Detti apparati, affidati al dipendente, sono strumenti di lavoro e ne è vietato ogni utilizzo non inerente all'attività lavorativa, ove non espressamente autorizzato dall'Azienda.

Considerando che con l'utilizzo degli strumenti in argomento (cellulari, smartphone, tablet, p.c. portatili, ecc) si può accedere all'e-mail, a servizi e dati personali, tali strumenti sono soggetti a rischio di violazione dei dati personali, ai sensi del Regolamento Europeo (General Data Protection Regulation, GDPR).

Per "violazione dei dati personali" (data breach) si intende "la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati" (art. 4, par. 1, n. 12 GDPR) e il Regolamento prevede l'obbligo per il Titolare del trattamento dei dati personali (Asl 3) di comunicare entro 72 ore all'Autorità di controllo (Garante) eventuali violazioni dei suddetti dati a seguito di incidenti, come attacchi informatici, accessi abusivi, incidenti o calamità naturali (ad es. incendi o alluvioni).

Anche la perdita o il furto o l'utilizzo improprio del dispositivo mobile concreta e implica una potenziale violazione dei dati personali (data breach) che con lo strumento si trattano.

Pertanto anche in riferimento al nuovo "Regolamento Europeo sulla Protezione dei Dati Personali" (GDPR-EU-2016/679) ed al fine di evitare qualsiasi accesso e utilizzo indesiderato e/o illecito, è fatto obbligo all'assegnatario del dispositivo e/o della SIM di:

- **proteggere** l'apparato attraverso un codice PIN ovvero una parola chiave (password)
- **proteggere** la SIM con apposito PIN e non rimuoverla, dall'apparato assegnato, ove non diversamente autorizzato;
- **informare** in caso di furto e/o smarrimento:
    - la Struttura competente della gestione dei dispositivo (S.C. Programmazione e Gestione delle Forniture per la telefonia mobile, e S.C. Sistemi Informativi per p.c. portatili e tablet);
    - le Forze dell'Ordine sporgendo denuncia di quanto accaduto
    - il proprio Responsabile;

- il Responsabile della Protezione dei dati Personali inviando una mail all'indirizzo rpd@asl3.liguria.it ;

Per gli apparati di Telefonia Mobile il personale della S.C. Programmazione e Gestione delle Forniture incaricato provvederà al blocco della SIM;

- **eliminare** qualsiasi informazione registrata all'interno dell'apparato al momento della restituzione del medesimo, ivi compresi, a titolo esemplificativo e non esaustivo, nomi e cognomi, numeri di telefono, messaggi, fotografie, video e quant'altro.

Quanto sopra vale anche per l'utente che utilizza la SIM aziendale oppure la posta elettronica di Asl 3 su dispositivi non aziendali. Anche per questi ultimi, in caso di furto e/o smarrimento, i dipendenti avranno l'incombenza di comunicare l'accaduto ad ASL 3 e al RPD come sopra descritto, nel più breve tempo possibile, al fine di valutare la notifica all'Autorità di controllo in caso di violazione di dati personali.

In caso di utilizzazione di dispositivi mobili e/o dotazioni informatiche personali per "Lavoro Agile" o forme assimilate, si ricorda che non possono essere effettuati salvataggi in locale di dati e/o su supporti di memorizzazione esterna. Si ricorda che anche la partecipazione alla modalità di erogazione della prestazione lavorativa "Lavoro Agile" disciplinata dalla Legge n. 81/2017 – Capo II, comporta la necessità di prestare costante attenzione alla protezione dei dati personali e adottare, in qualsiasi occasione, lavorativa e privata, un comportamento improntato alla difesa degli interessati che si relazionano con l'Ente

Per il salvataggio di tutti i dati per cui si renda necessaria la garanzia della conservazione, devono essere utilizzate le apposite cartelle condivise presenti sui server gestiti centralmente; è vietato mantenere tali informazioni solamente su supporti locali, che non sono sottoposti alle procedure di backup come riportato nel Documento Programmatico sulla Sicurezza (DPS)

Poiché in caso di violazioni contrattuali e giuridiche sia l'Azienda sia il singolo sono perseguibili con sanzioni, anche di natura penale, Asl 3 verificherà, nei limiti consentiti dalla legge, il rispetto delle regole e l'integrità del proprio patrimonio mobile.

Le presenti disposizioni sono vincolanti anche nei confronti dei lavoratori non dipendenti che collaborano con l'Azienda nell'ambito di altre forme di collaborazione professionale (contratti a termine, lavoratori somministrati, prestazione libero professionale, ecc.) o che si trovino, anche solo occasionalmente o a qualsiasi titolo, ad utilizzare dispositivi mobili di Asl 3

4) Utilizzo della rete Internet

Per ottenere l'abilitazione alla navigazione Internet dalle postazioni dell'Azienda, deve essere presentata richiesta scritta all'assistenza tecnica della S.C. Sistemi Informativi Aziendali, indicando il nome, il cognome e il servizio o struttura di appartenenza del dipendente. Tale richiesta deve essere firmata dal Direttore del servizio o dal responsabile della struttura di appartenenza.

La postazione di lavoro abilitata alla navigazione in Internet costituisce uno strumento aziendale necessario allo svolgimento della propria attività lavorativa e non è consentita la navigazione per motivi diversi da quelli strettamente legati all'attività lavorativa stessa. Inoltre non è consentito, senza autorizzazione scritta della S.C. Sistemi Informativi Aziendali, scaricare o installare software, anche se in versione gratuita o in prova, effettuare acquisti on-line o operazioni di home banking, utilizzare blog o sistemi e ambienti di comunicazione interattiva. È altresì fatto divieto il download di file musicali o di filmati.

Sono da evitare, senza esplicita autorizzazione della S.C. Sistemi Informativi Aziendali Aziendale, ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa, la partecipazione a forum non professionali, l'utilizzo di ambienti chat (esclusi strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest book, anche utilizzando pseudonimi (o nicknames).

L'Amministrazione si riserva di individuare categorie di siti Internet correlati con le prestazioni lavorative e di configurare filtri destinati a bloccare operazioni ritenute non coerenti con l'attività lavorativa, attivare "black list" e ridurre la possibilità di navigazione Internet anche senza avvisare gli utenti.

E' fatto divieto di utilizzare modem privati per il collegamento a Internet.

L'accesso ai siti consultati tramite la rete Internet viene monitorato dalle strutture tecniche dalla S.C. Sistemi Informativi Aziendali. Attraverso tale monitoraggio la S.C. Sistemi Informativi Aziendali può individuare collegamenti che mettono a rischio il sistema aziendale.

Il sistema di sicurezza del traffico Internet memorizza per una durata di 90 giorni i dati relativi al traffico effettuato dagli utenti in determinati file di log che sono accessibili, in via teorica, al personale tecnico debitamente designato quale amministratore di sistema.

Si specifica che il controllo effettuato attraverso la consultazione dei componenti di file di log registrati, potrà comportare, in caso di comportamenti non conformi al presente regolamento da parte

di singoli, in prima istanza l'inoltro di avvisi collettivi a tutti i dipendenti della specifica Struttura, e se tali abusi saranno comunque reiterati, anche ai singoli dipendenti.

Perdurando l'utilizzo non conforme, la S.C. Sistemi Informativi Aziendali potrà procedere a sospendere l'abilitazione per accedere a Internet al singolo dipendente e, ove ritenuto, il dipendente potrà essere soggetto a sanzioni disciplinari, qualora tali abusi abbiano messo a rischio il corretto funzionamento dei sistemi informativi aziendali, abbiano comportato perdita di dati o, in generale, abbiano presentato caratteristiche di particolare gravità.

All'interno dell'Azienda non è possibile, connettere alla rete aziendale apparati personali senza autorizzazione (per esempio PC portatili); è altresì vietato connettere dispositivi mobile personali alle reti wi-fi attualmente attive solo per scopi istituzionali (ad esempio, attività a letto paziente).

L'accesso alle risorse del sistema intranet dall'esterno è consentito esclusivamente tramite un collegamento che necessita di autenticazione VPN (Virtual Private Network) ovvero solo gli utenti autorizzati vi possano accedere. L'abilitazione e le credenziali di accesso vengono forniti dalla S.C. Sistemi Informativi Aziendali, previa richiesta formale con assunzione di responsabilità, verificati i requisiti di sicurezza.

L'accesso da remoto tramite VPN deve avvenire tramite apparati aziendali; nel caso si manifesti la necessita di utilizzare apparati personali (tablet, smarthphone, portatili), gli utenti devono richiederne l'autorizzazione alla S.C. Sistemi Informativi Aziendali e garantire gli standard minimi di sicurezza (antivirus) del pc, con dichiarazione esplicita.

5) Utilizzo posta elettronica

La S.C. Sistemi Informativi Aziendali ha il compito di progettare un'architettura di posta elettronica che permetta la consegna dei messaggi all'interno e all'esterno dell'Azienda e, al tempo stesso, fornisca una protezione dell'infrastruttura di rete interna adeguata allo stato tecnologico contro la minaccia di software parassiti come virus, spyware, spam, malware e/o altri programmi che hanno lo scopo di violare la privacy o provocare disfunzioni o danneggiamento dei computer e della rete aziendale.

Un messaggio di posta elettronica non rappresenta una trasmissione intrinsecamente sicura, soprattutto se inoltrato esternamente all'Azienda, e quindi veicolato su canali pubblici, e pertanto

deve essere valutata l'opportunità di inoltrare contenuti riservati, confidenziali o dati sensibili senza attivare opportuni sistemi di sicurezza.

La S.C. Sistemi Informativi Aziendali ha installato e tiene aggiornati software che controllano automaticamente ogni messaggio di posta elettronica al fine di prevenire la diffusione di virus o altri software parassiti.

I messaggi di posta elettronica devono avere dimensione non superiore a 10Mb.

La costruzione dell'indirizzo di posta elettronica garantisce che esso identifichi univocamente l'utente all'interno della rete di Internet. La casella di posta elettronica aziendale è formata per tutti i dipendenti da nome.cognome@asl3.liguria.it, salvo i casi in cui esistano omonimie, nomi composti o che utilizzano l'apostrofo o l'accento.

La denominazione delle caselle di posta elettronica istituzionali per gli indirizzari di gruppo viene creata direttamente dalle strutture tecniche della S.C. Sistemi Informativi Aziendali considerando la denominazione del servizio destinatario per semplificarne la rintracciabilità esterna e interna. A questa casella possono accedere, secondo le richieste delle Strutture, uno o più utenti in modo da consentire la continuità del servizio in caso di assenza dal lavoro.

L'utilizzo della posta elettronica aziendale è riservato al personale che per motivi inerenti la propria attività, necessita di comunicare, con continuità, all'interno/esterno dell'Azienda.

La casella di posta elettronica viene assegnata al momento dell'assunzione contestualmente alle credenziali di accesso al dominio.

Si sottolinea che la casella di posta, assegnata dall'Azienda all'utente, è uno strumento di lavoro, pertanto gli utenti del Sistema Informativo sono tenuti ad attenersi alle regole di seguito riportate:

1. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.
2. È sconsigliata la trasmissione a mezzo di posta elettronica di dati sensibili, confidenziali e personali di alcun genere.
3. Non è consentito l'uso della posta elettronica per i contatti interpersonali tra lavoratori non inerenti l'uso d'ufficio.
4. La spedizione, il ricevimento e tutti gli usi della posta elettronica sono generalmente intesi solo per scopi legati all'attività dell'Azienda; eventuali messaggi ricevuti da terzi non inerenti l'attività lavorativa devono essere immediatamente dirottati verso il corretto account personale dell'utente. Qualora il dipendente riceva messaggi di posta elettronica da indirizzi o

mittenti non conosciuti, occorrerà non aprire i suddetti messaggi e cancellarli immediatamente per non correre rischi di diffusione di virus informatici o di attacchi informatici alla rete aziendale.

5. La posta elettronica non deve essere utilizzata in modo da recare danno all'Azienda.
6. Non è consentita l'apertura di allegati ai messaggi di posta elettronica senza una verifica attraverso del software antivirus. Nel caso in cui il messaggio provenga da mittenti conosciuti ma contenga file allegati di dubbia provenienza o comunque sospetti (per esempio file eseguibili con estensione .exe .bat.), questi ultimi non dovranno essere aperti.
7. Non è consentito l'utilizzo di crittosistemi o di qualsiasi altro programma di sicurezza non previsto esplicitamente o autorizzato della S.C. Sistemi Informativi Aziendali.
8. Non è consentito inviare tramite posta elettronica e per nessun motivo, user-id, password, informazioni relative a configurazioni della rete aziendale, indirizzi e nomi dei sistemi informatici aziendali.
9. L'utente si impegna a non modificare per alcun motivo la configurazione hardware e software della propria postazione di lavoro informatica e a non utilizzare altri sistemi di posta elettronica se non espressamente autorizzato.
10. Le catene di posta elettronica, la pubblicità e gli invii generalizzati a tutto o parte dell'indirizzario aziendale sono vietati. Qualora non ci siano necessità istituzionali è vietata la diffusione di messaggi a tutti gli indirizzi contenuti nella rubrica aziendale o a consistenti parti di essa al fine di non intasare la posta elettronica con conseguente limitazione dell'efficienza della stessa.
11. Per la trasmissione di file all'interno dell'Asl 3 è possibile utilizzare la posta elettronica, prestando attenzione alla dimensione degli allegati.
12. È obbligatorio controllare i file allegati di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti). Non si devono in alcun caso attivare gli allegati di tali messaggi.
13. L'elenco degli utenti della rubrica verrà aggiornato dall'amministratore del sistema su segnalazione, da parte dell'Ufficio Personale o dai Responsabili delle Strutture, relativamente ai dipendenti cessati o trasferiti.

L'invio generalizzato a tutti gli utenti della rubrica di posta elettronica di ASL 3 è riservato esclusivamente alle segreterie di:

- Direzione Generale
- Direzione Amministrativa
- Direzione Sanitaria
- S.C. Sistemi Informativi Aziendali
- Affari del Personale
- Responsabile prevenzione corruzione e trasparenza (RPCT)
- Responsabile Protezione Dati

Potranno essere create ulteriori autorizzazioni su indicazione della Direzione Aziendale.

6) Utilizzo della Posta Certificata

In Azienda è stata istituita la casella di posta elettronica certificata (PEC) istituzionale come previsto dalla normativa (Dlgs 82/2005 e s.m.i; DPCM 06/05/2009): protocollo@pec.asl3.liguria.it.
Sono state inoltre istituite caselle pec utilizzate per servizi dedicati dalle strutture autorizzate:

- ospedalegallino@pec.asl3.liguria.it
- ospedalemicone@pec.asl3.liguria.it
- bilancio.fatture@pec.asl3.liguria.it
- ospedalevillascassi@pec.asl3.liguria.it
- proceduraordini@pec.asl3.liguria.it
- dipartimento.tecnico@pec.asl3.liguria.it
- ppigallino@pec.asl3.liguria.it
- ppimicone@pec.asl3.liguria.it
- psvillascassi@pec.asl3.liguria.it
- farmaceutica@pec.asl3.liguria.it
- refertiecg@pec.asl3.liguria.it
- ospedalecolletta@pec.asl3.liguria.it
- dipac@pec.asl3.liguria.it
- cardiologia.riabilitativa@pec.asl3.liguria.it
- penitenziaria@pec.asl3.liguria.it
- prevenzione.protezione@pec.asl3.liguria.it
- amministrazionesostegno@pec.asl3.liguria.it
- neonatologia@pec.asl3.liguria.it
- comunicazionealpersonale@pec.asl3.liguria.it

Si precisa che le caselle di posta elettronica certificata devono essere esclusivamente utilizzate per comunicazioni esterne, in quanto le comunicazioni tra strutture aziendali devono essere trasmesse solo tramite protocollo informatico.

7) Utenza da amministratore anonime

Le password per le utenze da amministratore anonime (es. root, administrator) sono conservate in busta chiusa presso la sala server del CED all'interno di armadio ignifugo.
L'utilizzo delle stesse è limitato a casi di emergenza e a personale autorizzato. L'utilizzatore è tenuto a indicare in apposito registro le seguenti informazioni relative all'accesso effettuato:

- data e ora di accesso e durata dell'intervento
- motivo
- cognome e nome
- sistema

Dopo l'effettuazione dell'intervento la password deve essere modificata secondo le regole prestabilite e deve essere aggiornata nel cartaceo conservato in busta chiusa.
Le operazioni amministrative ordinarie vengono effettuate da utenti nominativi e sono tracciate dal sistema operativo.

8) Controlli disposti dall'azienda

Ai sensi dell'art. 4 dello Statuto dei Lavoratori e del provvedimento del Garante italiano del 13 luglio 2016, fatto proprio come policy aziendale, lo strumento di lavoro non è in sé e per sé il computer, o il tablet, o lo smartphone, inteso come "scatola di plastica o metallo" contenente componenti elettronici.

Nella nozione di strumento di lavoro e con specifico riferimento ai servizi di posta elettronica e navigazione web "è da ritenere che possano ricomprendersi solo servizi, software o applicativi strettamente funzionali alla prestazione lavorativa, anche sotto il profilo della sicurezza.

Da questo punto di vista e a titolo esemplificativo, possono essere considerati "strumenti di lavoro" alla stregua della normativa sopra citata il servizio di posta elettronica offerto ai dipendenti

(mediante attribuzione di un account personale) e gli altri servizi della rete aziendale, fra cui anche il collegamento a siti internet. Costituiscono parte integrante di questi strumenti anche i sistemi e le misure che ne consentono il fisiologico e sicuro funzionamento al fine di garantire un elevato livello di sicurezza della rete aziendale messa a disposizione del lavoratore (ad esempio: sistemi di logging per il corretto esercizio del servizio di posta elettronica, con conservazione dei soli dati esteriori, contenuti nella cosiddetta "envelope" del messaggio, per una breve durata non superiore comunque ai sette giorni; sistemi di filtraggio anti-virus che rilevano anomalie di sicurezza nelle postazioni di lavoro o sui server per l'erogazione dei servizi di rete; sistemi di inibizione automatica della consultazione di contenuti in rete inconferenti rispetto alle competenze istituzionali, senza registrazione dei tentativi di accesso."

Non vengono utilizzati dall'azienda strumenti hardware e software che consentono:

1. la riproduzione e memorizzazione sistematica di tutte le pagine web visitate dal lavoratore;
2. la lettura e registrazione dei caratteri inseriti tramite la tastiera del PC

e più in generale quegli strumenti hardware e software che abbiano come precipuo fine proprio quello del controllo sistematico dell'attività espletata dal lavoratore in azienda come ad esempio il trattamento effettuato tramite sistemi software, non percepibili dall'utente (c.d. in background), ed idonei a porre in essere operazioni di "monitoraggio", "filtraggio", "controllo" e "tracciatura" costanti ed indiscriminati di tutti gli accessi a internet o al servizio di posta elettronica da parte degli utenti, quali, la registrazione sistematica dei dati relativi al MAC Address e i dati relativi alla connessione ai servizi di rete.

Secondo quanto previsto dal comma 3 dell'articolo 4 l'utilizzo delle informazioni raccolte e acquisite attraverso gli strumenti aziendali di lavoro Tablet, Pc (e anche geolocalizzazione...) e telefono indirettamente consente il controllo.

Il dipendente è edotto del fatto che il datore di lavoro può utilizzare queste informazioni.

Ad ogni modo le finalità del controllo sono esclusivamente correlate ad esigenze di:

1. tutela degli asset aziendali;
2. salute e sicurezza sul lavoro;

3. motivi organizzativo-produttivi.

L'S.C. Sistemi Informativi Aziendali, nel rispetto della normativa vigente, ha il compito di garantire il rispetto del presente Regolamento e verificare il corretto utilizzo delle apparecchiature e della Rete Aziendale, anche per prevenire utilizzi indebiti che possono essere fonte di responsabilità, ed effettuare verifiche sulla funzionalità e sicurezza dei sistemi. L'Azienda si riserva di procedere a verifiche del software installato sui personal computer, monitorare l'utilizzo delle risorse e ad attivare sistemi atti a limitare gli abusi, anche attraverso l'inoltro di preventivi avvisi collettivi e successivamente anche individuali.

9) Sanzioni disciplinari

Il mancato rispetto o la violazione delle regole contenute nel presente Regolamento è perseguibile con provvedimenti disciplinari, nonché, in relazione al tipo di infrazione, con le azioni civili e penali consentite.

10) Informativa ai dipendenti

ASL 3 nel rispetto della normativa vigente informa i dipendenti dell'Azienda che il trattamento dei dati personali raccolti in riferimento all'utilizzo della rete Internet e della posta elettronica è effettuato per le sole finalità di sicurezza e tutela dei sistemi informativi aziendali.
Il trattamento dei dati sarà effettuato utilizzando strumenti informatici e /o cartacei e conservati per un periodo non superiore ai tre mesi.
I dati personali saranno trattati da soggetti specificatamente nominati quali Responsabili esterni e/o Autorizzati al trattamento.
In qualsiasi momento potranno essere esercitati i diritti previsti Regolamento U.E. 2016/679 del 27/4/2016 e norme attuative, che riconoscono, tra gli altri, il diritto al soggetto interessato di poter accedere ai propri dati personali, di chiederne la rettifica ovvero l'integrazione, la cancellazione ("diritto all'oblio"), salvo i casi previsti all'art. 17 comma 3 del Regolamento UE 679/2016 e norme attuative ("Diritto alla cancellazione («diritto all'oblio»)- La richiesta, redatta per iscritto, potrà essere indirizzata al Titolare del Trattamento.

11) Aggiornamento e revisione

Il Presente Regolamento è soggetto a revisione con frequenza biennale e comunque in caso di introduzioni o modifiche legislative relative alla materia oggetto dello stesso.