Sistema Socio Sanitario

Regione Lombardia

ASST Fatebenefratelli Sacco

Regolamento per la sicurezza del trattamento dei dati nell'ambito dell'uso dei sistemi informatici

(approvato con deliberazione n. 1049 del 24/07/2024)

Redatto da: dr. Enrico Cuoco - Direttore SC Sistemi Informativi Aziendali
DPO aziendale LTA Advisor Srl

Sommario

Art. 1 - Premessa

La ASST Fatebenefratelli Sacco riconosce quale valore imprescindibile la sicurezza delle informazioni in particolare nell'ambito dei sistemi informatici.

A tal fine il presente documento regolamenta l'utilizzo degli strumenti elettronici atti a rendere la prestazione lavorativa in conformità:

- all'art. 4 comma 2 della Legge 20.5.1970 n. 300 così come modificata dal D.lgs n 151/2015;
- al Regolamento Europeo 679/16 "General Data Protection Regulation" (d'ora in avanti Reg. 679/16 o GDPR);
- alle "Linee Guida del Garante per posta elettronica e Internet" del 10.3.2007.

Scopo del presente Regolamento è quello di indicare i limiti entro cui i fruitori possono legittimamente usare gli strumenti elettronici messi a disposizione dall'ASST al fine di uno svolgimento proficuo e più agevole della propria attività (personal computer, smartphone, tablet, etc.).

Il Regolamento è stato implementato per tutelare la sicurezza dei sistemi informativi dell'ASST, assicurando la disponibilità delle risorse informative e dei dati, l'integrità dei sistemi e dei dati e la riservatezza delle informazioni.

Il Regolamento, oltre a dettare una disciplina per l'utilizzo degli strumenti aziendali, è da considerarsi uno strumento di formazione e sensibilizzazione per il personale nell'ambito degli obiettivi e delle politiche di sicurezza delle informazioni adottate dall'ASST.

L'ASST ha ritenuto inoltre di porre in essere adeguati e commisurati sistemi di controllo sul corretto utilizzo degli strumenti e delle risorse informatiche e telematiche, in una prospettiva di reciproca correttezza e trasparenza, senza che ciò possa in alcun modo invadere e violare la sfera personale del lavoratore e quindi il suo diritto alla riservatezza ed alla dignità.

Art. 2 - Oggetto e campo di applicazione

Il presente regolamento disciplina le modalità di utilizzo di qualsiasi dotazione informatica per il trattamento dei dati messa a disposizione dall'ASST, atta a rendere la prestazione lavorativa, che ciascun utilizzatore è tenuto ad osservare.

Il Regolamento si applica a tutti i dipendenti, senza distinzione di ruolo e/o livello e a tutti i collaboratori dell'ASST, a prescindere dal rapporto contrattuale con la stessa intrattenuto e a chiunque abbia in dotazione, anche temporaneamente, risorse informatiche e telematiche di proprietà dell'ASST o ad essa affidate. Tali soggetti, nell'ambito del presente Regolamento, sono indicati nel seguito anche come "Utente", "Utilizzatore" o "Incaricato".

Il presente Regolamento si applica a qualsiasi dotazione ICT intesa come risorsa informatica e/o telematica (a titolo esemplificativo e non esaustivo: computer, notebook, server, software, rete, utenza, file, cartella di rete, internet key, telefono, tablet, smartphone, modem, pen drive, router,

ecc..), di seguito indicata anche come “strumento elettronico”, messa a disposizione dall’ASST all’Utente per rendere la prestazione lavorativa.

Art. 3 - Politiche generali

Tutti gli strumenti elettronici affidati all’Utente sono da considerarsi uno strumento di lavoro. Possono pertanto essere utilizzati solo per fini professionali (in relazione alle mansioni assegnate) e non a fini personali; ogni utilizzo non inerente l'attività lavorativa è vietato in quanto può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza aziendale. Al dipendente è consentito l’utilizzo degli strumenti informatici forniti dall’amministrazione per poter assolvere alle incombenze personali senza doversi allontanare dalla sede di servizio purché l’attività sia contenuta in tempi ristretti, senza alcun pregiudizio per i compiti istituzionali e a condizione che non venga in alcun modo messa a rischio l’infrastruttura informativa aziendale.

Tutti gli strumenti elettronici affidati all’Utente non possono essere utilizzati per scopi illeciti e devono essere custoditi con cura ed in modo appropriato evitando ogni possibile forma di danneggiamento.

Gli strumenti elettronici devono essere spenti al termine della propria sessione lavorativa giornaliera, in caso di assenze prolungate dall'ufficio o in caso di loro inutilizzo.

Qualora lo strumento elettronico sia utilizzato da più incaricati, alla conclusione dei lavori è necessario disconnettere il proprio account dal sistema. Prima di effettuare la disconnessione chiudere i programmi rimasti eventualmente aperti. In questo modo la persona che utilizzerà il suddetto strumento in seguito potrà comunque effettuare la procedura di autenticazione. Lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso.

Si fa presente che tutti i dischi o altre unità di memorizzazione locali NON sono soggetti a salvataggio da parte dei sistemi informativi dell’ASST. Pertanto gli Utenti sono tenuti a memorizzare la documentazione lavorativa esclusivamente sui server dell’ASST (cd. “*file sharing*” o “cartelle condivise”).

Si precisa che è assolutamente vietato il trasferimento di file e/o documenti aziendali presso aree di storage esterne al perimetro aziendale (es: Google drive, Microsoft onedrive, Amazon drive, whatsapp, telegram, ecc). Tale comportamento espone infatti l’ASST a rilevanti rischi di violazione di dati personali e sensibili; inoltre, qualora le piattaforme di sotarage esterno fossero condivise con soggetti non designati al trattamento di dati, l’attività si configurerebbe a tutti gli effetti come un *DATA BREACH.*

È indispensabile che nessun dato personale degli Utenti non inerente l’attività lavorativa sia presente sulle risorse informatiche dell’ASST neppure provvisoriamente.

Per i PC operanti al di fuori del dominio della ASST, non avendo accesso diretto ai server e di conseguenza ai salvataggi periodici, i dati devono essere conservati sul disco locale e periodicamente

salvati secondo le istruzioni impartite dall'Amministratore di sistema o dal Responsabile IT; per lo scopo si precisa che l'ASST consente di accedere alle cartelle condivise aziendali sia per mezzo di credenziali vpn, sia per mezzo di infrastruttura tecnologica VDI (virtualizzazione della postazione di lavoro).

Ogni Utente è responsabile:

- della propria postazione informatica sia fissa che mobile, della propria casella di posta elettronica e del contenuto dei messaggi da essa inviati.
- della segretezza delle credenziali di accesso alla rete e ai software al cui utilizzo è stato autorizzato.

Ogni Utente è tenuto ad osservare tutte le misure di protezione e sicurezza atte ad evitare rischi di distruzione o perdita accidentale dei dati, accesso non autorizzato, trattamento non consentito o non conforme alle finalità della raccolta.

Gli Utenti sono tenuti a mantenersi aggiornati, prendendo visione delle eventuali disposizioni emanate e divulgate tramite pubblicazione in area dedicata intranet nella rete informatica dell'ASST, tramite posta elettronica o tramite altro strumento cartaceo (avviso, disposizione, regolamento, ecc.).

L'ASST garantisce, all'interno del perimetro aziendale, per tutte le postazioni operanti in rete, la presenza di strumenti antivirus costantemente aggiornati, la presenza di strumenti antispam a bordo dei sistemi di gestione della posta elettronica, la presenza di strumenti di protezione perimetrale con I quali vengono impediti tentativi di intrusione a seguito di attacchi esterni.

Resta inteso che tutte le risorse informative, sia in termini di strumenti che in termini di dati, rimangono di proprietà dell'ASST e che l'Utente è tenuto a restituire la totalità delle risorse utilizzate nel momento in cui dovesse cessare il rapporto con la stessa o nel caso in cui gli venisse richiesto da quest'ultima.

Gli Utenti sono tenuti a dare tempestiva comunicazione, preferibilmente in forma scritta, di qualsiasi anomalia relativa al sistema informativo aziendale al Titolare o suo delegato immediatamente dopo la sua scoperta, affinché la stessa venga valutata dal personale all'uopo incaricato e gestita nel rispetto delle procedure di sicurezza dell'ASST.

3.1 - Server di rete per file sharing e cartelle condivise

Presso la ASST sono operativi server di rete sui quali è possibile depositare file in cartelle di rete condivise tra gli utenti che, ancorchè operanti presso sedi fisiche diverse, hanno la necessità di condividere documenti e file di varia natura.

Ogni Responsabile definisce l'albero documentale su cui far confluire i documenti prodotti dalla propria struttura, definendo anche per ciascun Utente i privilegi da assegnare allo stesso (sola lettura, scrittura, cancellazione).

In occasione di eventuali assunzioni o trasferimenti di personale tra strutture, ogni Responsabile provvede a rivedere, modificare, revocare i privilegi concessi a ciascuno dei propri collaboratori dandone evidenza alle strutture Sistemi Informativi.

Ogni Responsabile, quando lo ritiene opportuno, può chiedere di eseguire una verifica per monitorare i livelli di visibilità oltre che I privilegi degli utenti che accedono alle cartelle condivise, che sono anche fruibili dagli Utenti che operano in regime di Smart Working dall'esterno della ASST.

Il patrimonio informativo custodito sui server adibiti a file sharing viene messo in regime di sicurezza per mezzo di procedure di backup.

Sul file sharing aziendale sono attivi controlli sui tipi di dati che vengono depositati sullo stesso, oltre che sui limiti dimensionali massimi consentiti. In caso di rilevazione di formati non compatibili con le estensioni aziendali (es. file MP3, file audio, file video, ecc) viene notificata una mail ad Utente per evidenziare uso anomalo dello strumento.

Per ogni cartella di rete condivisa possono essere definite una o più quote indicanti la dimensione massima che la cartella stessa potrà raggiungere, al fine di gestire ed ottimizzare al meglio le capacità di memorizzazione offerte dal file sharing aziendale. Nel caso gli utilizzatori dovessero raggiungere o superare la soglia di occupazione definita da una delle quote, viene notificato l'evento attraverso una mail all'utente che lo ha provocato, oltre che una mail agli amministratori di sistema.

Tra le misure di sicurezza che potranno essere attivate, vi è anche l'ipotesi di blocco dell'utilizzo di dispositivi di memorizzazione removibili (hard disk, pen drive, ecc.).

3.2 - Infrastruttura per la virtualizzazione dei Personal Computer

L'ASST è da anni dotata di una infrastruttura tecnologica denominata VDI (Virtual Desktop Infrastructure) che ha consentito di procedere gradualmente alla sostituzione dei dispositivi "Personal Computer" con dispositivi "Thin Client". Tale processo, che continuerà progressivamente in futuro, consente alla ASST di accrescere in modo rilevante gli aspetti legati alla sicurezza poiché tale dispositivo:

- non è dotato di hard disk e non contiene patrimonio informativo di nessun tipo, tutelando pertanto in caso di furto o di danneggiamento l'ASST da potenziali rischi di asportazioni o perdita di patrimonio informativo riservato o sensibile;
- il ciclo di vita di tali dispositivi è estremamente superiore a quello di un tradizionale Personal Computer e pertanto, poiché gestito centralmente, non è sottoposto ai fisiologici processi di invecchiamento che ne devono prevedere la sostituzione periodica;
- la continuità di servizio di tali dispositivi è estremamente superiore rispetto a quella offerta da un Personal Computer poiché il numero di guasti che possono coinvolgere un Thin Client sono estremamente inferiori, anche per l'assenza di componenti meccaniche in movimento come gli hard disk tradizionali;

- consente all'Utente di utilizzare il proprio desktop e tutte le caratteristiche del proprio profilo, indipendentemente dal dispositivo che sta utilizzando in quel momento e indipendentemente dal luogo in cui lo sta utilizzando;
- per le caratteristiche del precedente punto può essere utilizzato anche dall'esterno dell'ASST ricorrendo ad un qualsiasi dispositivo informatico dotato di browser (PC desktop, portatile, smartphone, tablet) attraverso cui l'Utente, preventivamente abilitato, potrà accendere remotamente la sua postazione di lavoro; tale caratteristica si è dimostrata fondamentale per la diffusione massiva dell'attività lavorativa in regime di Smartworking, che ha consentito al personale dipendente di utilizzare in modo agevole, anche con strumenti informatici propri, la postazione aziendale dal proprio domicilio.

Gli Utenti possono utilizzare, se autorizzati, la postazione virtualizzata anche dall'esterno dell'ASST garantendo le seguenti osservanze:

- la postazione va utilizzata solo ed esclusivamente durante l'orario di lavoro e solo per scopi lavorativi;
- durante l'utilizzo della postazione l'Utente NON deve essere affiancato da familiari o conoscenti che potrebbero prendere visione di informazioni riservate legate alla sfera lavorativa aziendale.

Art. 4 - Regole per gli accessi

L'accesso alla rete informatica dell'ASST e l'utilizzo degli strumenti elettronici dati in affidamento all'Utente è consentito solo attraverso specifiche credenziali di autenticazione, che consistono in un codice per l'identificazione (username) dell'incaricato associato a una parola chiave (password) riservata conosciuta solamente dal medesimo. Il sistema richiede periodicamente all'utente di modificare la propria password seguendo i medesimi principi del "primo accesso" (vedi sotto). Per l'accesso dall'esterno, per alcuni sistemi aziendali, è operativa modalità di autenticazione a 2 fattori che prevede, oltre alle tradizionali utenza e password, anche un codice OTP rilasciato da una app installata su proprio smartphone.

Gli accessi ed i permessi degli Utenti garantiscono i profili di autorizzazione degli incaricati in ambito di trattamento dei dati, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento. Ne consegue che gli Utenti possono effettuare esclusivamente i trattamenti di dati personali che rientrano nel proprio ambito lavorativo e per i quali hanno ricevuto specifico incarico.

Tali trattamenti devono essere effettuati esclusivamente in conformità alle finalità previste e alle informazioni comunicate agli Interessati.

L'Utente è tenuto a modificare la parola chiave (password) assegnatagli al primo accesso tenendo conto di quanto segue:

- la password deve essere complessa (a titolo esemplificativo: deve contenere lettere e numeri e/o simboli, minimo 10 caratteri, minuscole, maiuscole);
- la password non deve essere agevolmente riconducibile all'Utente (a titolo esemplificativo non deve essere identica allo username, non deve essere la data di nascita, ecc.);
- la sequenza delle password non può essere la medesima di quelle scadute ed utilizzate in precedenza;
- le credenziali di autenticazione non utilizzate da almeno sei mesi sono automaticamente disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica che rimangono nella disponibilità esclusiva degli Amministratori di Sistema e di eventuali sistemi automatizzati che ne fanno uso per l'erogazione di servizi;
- le credenziali sono disattivate anche in caso di perdita delle qualità che consentono all'Utente, incaricato, l'accesso al sistema informatico e ai dati personali in esso custoditi o all'area ad accesso ristretto; in caso di cessazione del rapporto di lavoro, per mezzo di un automatismo, le credenziali cessano dopo 30 giorni, per consentire accesso al portale dipendente per recupero ultima busta paga. Casi che richiedano l'immediata disattivazione delle utenze dovranno essere comunicati tempestivamente ai Sistemi Informativi;
- è vietato affidare al sistema operativo la memorizzazione automatica delle password e l'Utente è tenuto a digitare la password ad ogni accesso;
- Il browser di navigazione (es. Mozilla Firefox, Google Chrome, Edge) deve essere impostato in modo tale che non memorizzi le credenziali di accesso inserite dall'utente, per accedere agli applicativi web aziendali;
- il sistema richiede la modifica della parola chiave (password) ogni 90 giorni.

Il codice di identificazione non deve essere comunicato ad alcuno e deve essere custodito dall'Utente con la massima diligenza e non divulgato.

È assolutamente proibito accedere alla rete e ai programmi con un codice di identificazione Utente diverso da quello assegnato.

L'Utente è tenuto ad avvisare prontamente l'ufficio competente al riguardo nell'ipotesi di smarrimento dei dati di accesso.

In caso di prolungata assenza o impedimento di un Utente che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema, il responsabile IT (o l'Amministratore di sistema o l'incaricato alla custodia delle credenziali, se designati), su indicazione della Direzione, al fine di assicurare la disponibilità dei dati e/o degli strumenti elettronici, potrà resettare la componente riservata della credenziale di autenticazione, per consentire l'accesso ad un altro Utente indicato dalla Direzione. In tale circostanza l'utente riceve una mail in cui viene avvisato dell'avvenuta forzatura delle proprie credenziali.

L'Utente, terminato il periodo di assenza o impedimento, sarà immediatamente informato in merito all'intervento effettuato e, in occasione del primo login, dovrà cambiare la password di primo accesso.

Le credenziali amministrative locali (Administrator) delle postazioni di lavoro vengono gestite centralmente attraverso specifico tool (Microsoft LAPS) parametrizzato da criteri di dominio. La password viene continuamente modificata a intervalli regolari ed è generata casualmente con criteri di elevata complessità (lunghezza di 15 caratteri, maiuscole, minuscole, numeri). Tutti gli amministratori di sistema dei Sistemi Informativi possono conoscere la password attualmente configurata per una determinata postazione di lavoro e impostarne una nuova scadenza.

Art. 5 - Divieti

È vietato, salvo preventiva ed espressa autorizzazione dell'ASST:

- l'uso di programmi diversi da quelli ufficialmente installati;
- installare, modificare e aggiornare i software autonomamente, se non inclusi nell'elenco software autorizzati;
- modificare le caratteristiche impostate sul proprio personal computer e procedere ad installare dispositivi di memorizzazione, di comunicazione, di stampa o altro;
- utilizzare strumenti software e/o hardware atti ad intercettare, falsificare, alterare o eliminare il contenuto di comunicazioni e/o documenti informatici;
- utilizzare e conservare sul sistema informatico dell'ASST file non attinenti l'attività lavorativa;
- violare l'integrità di dati personali;
- compromettere l'integrità dei sistemi;
- saturare le risorse in misura tale da compromettere l'efficienza del sistema informativo dell'ASST;
- compiere atti di criminalità informatica;
- consentire l'accesso alla rete e/o condividere la rete con soggetti non autorizzati;
- usare false identità;
- violare la sicurezza, trasferire, comunicare, diffondere, intercettare, accedere a dati per i quali non si ha specifica autorizzazione;
- collegare alla rete aziendale computer personali o computer non assegnati dall'ASST, anche in modalità Wi-Fi;
- accedere ad aree, chiaramente definite e segnalate dall'ASST, che contengono informazioni sensibili o critiche e strutture di elaborazione delle informazioni, se non specificatamente autorizzati;
- consentire l'accesso alle aree in cui si esegue il trattamento dei dati a personale esterno non autorizzato;
- trasferire all'esterno del perimetro aziendale, anche fisicamente, le apparecchiature, informazioni, file, documenti o software senza preventiva autorizzazione.

Si evidenzia che alcune delle violazioni di cui sopra sono sanzionabili anche penalmente.

Art. 6 - Politiche di “schermo pulito”

Al fine di ridurre il rischio di accesso non autorizzato ad informazioni aziendali, è necessario che l’Utente segua delle politiche di “schermo pulito”.

In particolare è fondamentale che presti particolare attenzione alle schermate a video contenenti informazioni non pubbliche.

Il desktop della postazione di lavoro può contenere solamente i collegamenti ai principali software di produttività e non deve per alcuna ragione essere utilizzato per il salvataggio di documenti.

È quindi opportuno che tali schermate siano mantenute solo per il tempo strettamente necessario.

Art. 7 - Supporti rimovibili

I supporti rimovibili contenenti dati personali, se non utilizzati, devono essere distrutti o resi inutilizzabili prima di procedere al loro smaltimento.

Tali supporti possono essere utilizzati da altri Incaricati se le informazioni precedentemente in essi contenute sono inintelligibili e tecnicamente in alcun modo ricostruibili.

E’ disabilitata attraverso criteri globali di sicurezza, l’esecuzione automatica di programmi presenti su supporti di origine esterna. Alla prima connessione di tali dispositivi, il software preinstallato di Endpoint Security provvede inoltre ad una scansione in real-time dei contenuti ed elimina o isola gli oggetti ritenuti pericolosi.

In ogni caso, i supporti magnetici contenenti dati particolari devono essere dagli Utenti adeguatamente custoditi in locali o in soluzioni di stoccaggio ad accesso ristretto e controllato (a titolo esemplificativo, armadi o cassetti chiusi a chiave, casseforti e simili).

L'uso di supporti removibili (hard disk, pen drive, ecc) è vietato; in circostanze tecniche limitate l’attività viene consentita al solo personale tecnico autorizzato dai Sistemi Informativi.

Art. 8 - Dispositivi portatili

L'Utente è responsabile dei dispositivi portatili assegnatigli dall’ASST (PC, smartphone, tablet, ecc) e deve custodirli con diligenza, adottando tutti i provvedimenti che le circostanze rendono necessari per evitare danni o sottrazioni.

I dispositivi portatili, proprio per le loro intrinseche caratteristiche, sono più vulnerabili dei dispositivi fissi. Per tale motivo, oltre alle politiche adottate per gli strumenti informatici fissi, occorrono accorgimenti aggiuntivi.

Quindi, al fine di minimizzare il rischio associato al furto, all’uso fraudolento e all’accesso di persone non autorizzate alle informazioni presenti sui dispositivi, l’Utente viene abilitato ad accedere ad infrastruttura aziendale da remoto per mezzo di VPN o di virtual desktop, potendo pertanto utilizzare

una normale connettività ad internet in modo sicuro e con traffico dati cifrato, così da consentire una comunicazione sicura della postazione di lavoro con l'infrastruttura tecnologica della ASST.

I dispositivi portatili, al fine di garantire il controllo, l'aggiornamento e l'allineamento alle politiche di sicurezza dell'ASST, devono essere periodicamente connessi (almeno una volta alla settimana), direttamente o tramite connessione protetta, alla rete dell'ASST, per la durata necessaria.

Si evidenzia inoltre che le reti Wi-Fi non protette espongono i dispositivi aziendali a potenziali rischi di intercettazione di traffico dati, oltre di credenziali, in modo fraudolento; è per tale motivo che è vietato accedere a reti Wi-Fi che non offrano idonee misure di sicurezza (evitare categoricamente le connessioni presso dispositivi a libero accesso presso bar, ristoranti, negozi, stazioni, centri commerciali, distributori di carburante, ecc.).

Art. 9 - Utilizzo della rete Internet e dell'account di posta elettronica

La navigazione in Internet ed il sistema di posta elettronica sono mezzi di comunicazione, informazione e trasmissione.

L'uso della posta elettronica e della rete Internet, nelle sue numerose funzionalità, è consentito esclusivamente per gli scopi attinenti alle mansioni lavorative assegnate.

I metadati di posta elettronica sono di proprietà dell'ASST.

La casella di posta elettronica è uno strumento di lavoro e gli utenti assegnatari delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

È fatto divieto di utilizzare le caselle di posta elettronica assegnate e/o messe a disposizione dall'ASST per motivi diversi da quelli strettamente legati all'attività lavorativa e per motivi non attinenti allo svolgimento di mansioni lavorative assegnate. La "personalizzazione" dell'indirizzo di posta elettronica, ovvero la possibilità che esso contenga riferimenti al nome e cognome dell'utente, non comporta il fatto che la stessa venga considerata "privata", in quanto si tratta comunque di uno strumento di esclusiva proprietà dell'Azienda, messo a disposizione di dipendenti e collaboratori a vario titolo al solo fine dello svolgimento delle proprie mansioni lavorative. Si chiarisce pertanto che non è possibile avanzare richieste di esportazione del proprio database di posta elettronica al momento della cessazione del rapporto di lavoro.

Al momento della cessazione del rapporto di lavoro, la casella di posta viene chiusa e conservata sui server di posta elettronica dell'Azienda. Per un periodo di 6 mesi è ancora possibile all'utente cessato fare richiesta di accesso alla propria casella. Se la richiesta viene approvata dalla Direzione Aziendale, le credenziali di accesso vengono ripristinate per il periodo di tempo autorizzato dalla Direzione.

Trascorso un periodo di 6 mesi dalla chiusura definitiva, la casella di posta viene archiviata e rimossa dai server di posta per consentire il riutilizzo della licenza e liberare spazio utile. La casella archiviata viene conservata per 1 anno off line su storage dedicato.

La casella di posta elettronica deve essere mantenuta in ordine, cancellando periodicamente documenti inutili, messaggi pubblicitari, mail non rilevanti e soprattutto allegati ingombranti, limitandone la sua dimensione complessiva. Per lo scopo si ricorda che sono operativi in Azienda strumenti di chat che agevolano e semplificano le comunicazioni di carattere estemporaneo tra gli Utenti e che questi sono da preferire alle mail, quando le conversazioni hanno carattere informale.

Prima di aprire i file allegati ai messaggi di posta elettronica, è necessario identificare il mittente e porre particolare attenzione alla tipologia del file stesso, in caso in cui non si conosca il mittente è consigliabile cancellare tutto, messaggio ed allegato oppure identificarlo autonomamente come SPAM utilizzando gli appositi strumenti messi a disposizione dal sistema di gestione della posta elettronica. In presenza di messaggi di origine o contenuto sospetto, l'Utente può sempre contattare il supporto tecnico dei Sistemi Informativi che procederà ad una verifica approfondita.

Si porta anche all'attenzione la pericolosità di eventuali allegati relativi a suite di Office Automation (Microsoft Office oppure LibreOffice) capaci di ospitare funzioni Macro che possono contenere codice malevolo in grado di violare la sicurezza della postazione e, quindi, dell'intera rete; si suggerisce pertanto di tenere tali funzioni disabilitate all'interno delle citate suite ed abilitarle solo quando si è certi della provenienza del documento ricevuto.

Al fine di ribadire agli interlocutori la natura della casella di posta elettronica assegnata dall'ASST, i messaggi devono contenere, in calce, un avvertimento standardizzato nel quale sia dichiarata la natura non personale dei messaggi stessi.

Nei messaggi di posta elettronica è inserita, per mezzo di un automatismo, la seguente dicitura:

> "*Questa comunicazione e ogni eventuale documento allegato sono ad uso esclusivo del destinatario e contengono informazioni riservate. Il messaggio ed eventuali documenti allegati non hanno natura personale e le eventuali risposte alla presente potranno essere conosciute da più soggetti e unità operative all'interno della Azienda Socio Sanitaria Territoriale Fatebenefratelli - Sacco, che a vario titolo abbiano interesse ad assolvere le specifiche richieste o esigenze oggetto della comunicazione. Se non siete l'effettivo destinatario della consegna della comunicazione e se l'aveste ricevuta per errore, ci scusiamo per l'accaduto e vi invitiamo cortesemente ad eliminarla in maniera definitiva senza possibilità alcuna di recupero e di comunicare immediatamente l'accaduto ai nostri uffici. Qualsiasi modifica o distribuzione a terzi è assolutamente vietata. Vi ricordiamo, inoltre, che la comunicazione, la diffusione, l'utilizzo e/o la conservazione dei dati ricevuti per errore, costituiscono violazioni alle disposizioni del Regolamento generale sulla protezione dei dati personali 679/2016 dell'Unione Europea e sono sanzionabili ai sensi dell'art. 616 del Codice Penale*."

In caso di violazione o inadempimento di quanto riportato al presente paragrafo in merito all'utilizzo della posta elettronica, l'ASST procederà ad impedire all'Utente la possibilità di collegamento alla casella di posta elettronica assegnata e si procederà per eventuale accertamento di responsabilità disciplinari, in caso di personale dipendente, o contrattuali in caso di professionisti e/o collaboratori.

L'ASST mette a disposizione di ciascun lavoratore, con modalità di agevole esecuzione, apposite funzionalità di sistema che consentano di inviare automaticamente, in caso di assenze programmate, messaggi di risposta che contengano le "coordinate" di altro soggetto o altre utili modalità di contatto.

La ASST, quando rileva utilizzi anomali di una casella mail aziendale (ad esempio spedizione massiva di mail da parte di un utente), che sono il risultato di una violazione delle credenziali di autenticazione, procede al cambio forzoso della password per impedire il protrarsi della situazione di rischio; in tale modo l'utente che ha subito la violazione della propria casella viene riportato in stato di sicurezza.

È assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati allo svolgimento delle mansioni lavorative assegnate.

È assolutamente proibita la navigazione in Internet qualora il contenuto dei siti sia di natura oltraggiosa e discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.

Il sistema di sicurezza adottato e interposto tra la rete dell'ASST e la rete Internet potrà impedire l'accesso a siti web indesiderati, attraverso la valutazione del contenuto o per l'appartenenza ad una "black list".

Per ridurre il rischio di attacchi informatici durante la navigazione, posizionare il cursore del mouse sul link interessato, osservandone il percorso sulla barra del browser: se è un file eseguibile potrebbe trattarsi di un programma malevolo (ad esempio di un programma che potrebbe collegare l'Utente a un altro indirizzo internet, non sicuro). Nel caso il software antivirus rilevi la presenza di un virus, l'Utente dovrà immediatamente sospendere ogni elaborazione in corso, senza spegnere il computer e segnalare tempestivamente l'accaduto al personale del Servizio IT.

All'interno del perimetro aziendale è presente un servizio di Wi-Fi per gli ospiti che, previa registrazione, consente la libera navigazione in internet senza restrizioni del traffico.

L'Utente è direttamente e totalmente responsabile dell'uso di Internet, delle informazioni che immette, delle modalità con cui opera, dei siti web o pagine internet ai quali abbia stabilito collegamento tramite link. Qualora vengano attivati eventuali controlli da parte dell'ASST, tenuto conto degli strumenti elettronici installati, avverranno come di seguito indicato:

- gli apparati in uso, (ad esempio tramite un sistema proxy server) tracceranno in modo anonimo la navigazione effettuata dagli utenti in merito ai siti rilevati;
- tale tracciamento potrà essere visualizzato solo dall'Amministratore di sistema.

A seguito di eventuali segnalazioni provenienti dagli strumenti automatizzati di monitoraggio delle minacce informatiche o di generalizzate campagne di attacchi informatici in essere, L'ASST per garantire la sicurezza della propria infrastruttura, potrà effettuare controlli a campione sugli accessi internet interessati dalla segnalazione, effettuati dai dipendenti/collaboratori stessi nel periodo segnalato.

Si rende noto che l'ASST è autorizzata al trattamento in forma anonima, tale da precludere l'immediata identificazione degli utenti, dei dati relativi al "traffico" internet. I file di LOG verranno

conservati per il tempo strettamente necessario al perseguimento di finalità organizzative, produttive e di sicurezza.

Verranno prolungati i tempi di conservazione (limitatamente comunque alle sole informazioni indispensabili per perseguire finalità preventivamente determinate) solo in caso di:

- esigenze tecniche o di sicurezza del tutto particolari;
- indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;
- obbligo di custodire o conservare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria.

Il controllo anonimo potrebbe concludersi con un avviso generalizzato relativo ad un rilevato utilizzo anomalo degli strumenti aziendali e con l'invito ad attenersi scrupolosamente a compiti assegnati e istruzioni impartite. Si ribadisce che i controlli rispettano i principi di pertinenza e di non eccedenza. In nessun caso verranno compiuti controlli prolungati, costanti o indiscriminati. I controlli saranno svolti in conformità alla legge, sia per eseguire verifiche sulla funzionalità e sicurezza del sistema, sia per verificare il corretto utilizzo da parte degli utenti (dipendenti, collaboratori etc.) tanto della rete Internet che della posta elettronica. Nell'esercizio del potere di controllo l'ASST si atterrà al principio generale di proporzionalità e non eccedenza delle attività di controllo.

Art. 10 - Principali minacce

Al fine di sensibilizzare gli utenti ad un uso diligente delle risorse messe a disposizione dall'ASST, vengono indicate di seguito alcune minacce (*Malware*) che rappresentano una fonte di rischio per l'intero sistema informativo.

Nella sicurezza informatica il termine *Malware* indica genericamente un qualsiasi software creato con il solo scopo di causare danni più o meno gravi ad un computer, ai dati degli utenti del computer, o a un sistema informatico su cui viene eseguito. Il termine deriva dalla contrazione delle parole inglesi malicious e software e ha dunque il significato letterale di "programma malvagio"; in italiano è detto anche codice maligno. Si distinguono molte categorie di *Malware*, anche se spesso questi programmi sono composti di più parti interdipendenti e rientrano pertanto in più di una classe. Vista inoltre la rapida evoluzione in questo campo, la classificazione presentata di seguito non è da ritenersi esaustiva:

Virus: sono parti di codice che si diffondono copiandosi all'interno di altri programmi, o in una particolare sezione del disco fisso, in modo da essere eseguiti ogni volta che il file infetto viene aperto. Si trasmettono da un computer a un altro tramite lo spostamento di file infetti ad opera degli utenti.

Worm: questi Malware non hanno bisogno di infettare altri file per diffondersi, perché modificano il sistema operativo della macchina ospite in modo da essere eseguiti automaticamente e tentare di replicarsi sfruttando per lo più Internet. Per indurre gli utenti ad eseguirli utilizzano tecniche di ingegneria sociale, oppure sfruttano dei difetti (bug) di alcuni programmi per diffondersi automaticamente. Il loro scopo è rallentare il sistema con operazioni inutili o dannose.

Trojan horse: software che oltre ad avere delle funzionalità "lecite", utili per indurre l'utente ad utilizzarli, contengono istruzioni dannose che vengono eseguite all'insaputa dell'utilizzatore. Non possiedono funzioni di auto-replicazione, quindi per diffondersi devono essere consapevolmente inviati alla vittima. Il nome deriva dal famoso cavallo di Troia.

CryptoLocker: una forma di ransomware infettante i sistemi Windows e che consiste nel criptare i dati della vittima, richiedendo un pagamento per la decriptazione. CryptoLocker generalmente si diffonde come allegato di posta elettronica apparentemente lecito e inoffensivo che sembra provenire da mittenti legittimi.

Backdoor: letteralmente "porta sul retro". Sono dei programmi che consentono un accesso non autorizzato al sistema su cui sono in esecuzione. Tipicamente si diffondono in abbinamento ad un trojan o ad un Worm, oppure costituiscono una forma di accesso lecita di emergenza ad un sistema, inserita per permettere ad esempio il recupero di una password dimenticata.

Spyware: software che vengono usati per raccogliere informazioni dal sistema su cui sono installati e per trasmetterle ad un destinatario interessato. Le informazioni carpite possono andare dalle abitudini di navigazione fino alle password e alle chiavi crittografiche di un utente.

Hijacker: questi programmi si appropriano di applicazioni di navigazione in rete (soprattutto browser) e causano l'apertura automatica di pagine web indesiderate.

Rootkit: i rootkit solitamente sono composti da un driver e, a volte, da copie modificate di programmi normalmente presenti nel sistema. I rootkit non sono dannosi in sé, ma hanno la funzione di nascondere, sia all'utente che a programmi tipo antivirus, la presenza di particolari file o impostazioni del sistema. Vengono quindi utilizzati per mascherare spyware e trojan.

Scareware: sono così chiamati quei programmi che ingannano l'utente facendogli credere di avere il proprio PC infetto, allo scopo di fargli installare dei particolari malware, chiamati in gergo rogue antivirus, caratterizzati dal fatto di spacciarsi per degli antivirus veri e propri, talvolta spacciati anche a pagamento.

Rabbit: i rabbit sono programmi che esauriscono le risorse del computer creando copie di sé stessi (in memoria o su disco) a grande velocità.

Adware: programmi software che presentano all'utente messaggi pubblicitari durante l'uso, a fronte di un prezzo ridotto o nullo. Possono causare danni quali rallentamenti del pc e rischi per la privacy in quanto comunicano le abitudini di navigazione ad un server remoto.

Batch: i Batch sono i cosiddetti "virus amatoriali". Non sono sempre dei file pericolosi in quanto esistono molti file batch tutt'altro che dannosi, il problema arriva quando un utente decide di crearne uno che esegua il comando di formattare il pc (o altri comandi dannosi) dell'utente a cui viene mandato il file. Non si apre automaticamente, deve essere l'utente ad aprirlo, perciò dato che l'antivirus non rileva i file Batch come pericolosi è sempre utile assicurarsi che la fonte che vi ha mandato il file sia attendibile oppure aprirlo con blocco note per verificare o meno la sua pericolosità. Bisogna però anche dire che esistono modi per camuffare i Batch e farli sembrare dei file exe,

aumentandone anche il peso per sedare ogni sospetto. L'utilizzo di questo particolare "malware" è spesso ricorrente nel Cyberbullismo.

Keylogger: i Keylogger sono dei programmi in grado di registrare tutto ciò che un utente digita su una tastiera o che copia e incolla rendendo così possibile il furto di password o di dati che potrebbero interessare qualcun altro. La differenza con gli Adware sta nel fatto che il computer non si accorge della presenza del Keylogger e il programma non causa rallentamento del pc, passando così totalmente inosservato. Generalmente i Keylogger vengono installati sul computer dai trojan o dai Worm, in altri casi invece il Keylogger viene installato sul computer da un'altra persona che può accedere al pc o attraverso l'accesso remoto (che permette a una persona di controllare un altro pc dal suo stesso pc attraverso un programma) oppure in prima persona, rubando così dati e password dell'utente.

Rogue antispyware: malware che si finge un programma per la sicurezza del PC, spingendo gli utenti ad acquistare una licenza del programma.

Bomba logica: è un tipo di malware che "esplode" ovvero fa sentire i suoi effetti maligni al verificarsi di determinate condizioni o stati del PC fissati dal cracker stesso.

Zip Bomb: è un file che si presenta come un file compresso. Deve essere l'utente ad eseguirlo. All'apparenza sembra un innocuo file da pochi Kilobyte ma, appena aperto, si espande fino a occupare tutto lo spazio su disco rigido. Nell'uso comune il termine virus viene utilizzato come sinonimo di malware e l'equivoco viene alimentato dal fatto che gli antivirus permettono di rilevare e rimuovere anche altre categorie di software maligno oltre ai virus propriamente detti.

Intercettazioni delle comunicazioni: possono comportare l'accesso non autorizzato alle banche dati per consultazione e copia di dati personali da parte di persone non autorizzate.

Attacchi alle password: questi attacchi effettuati in varia forma sono dei tentativi per venire a conoscenza e quindi rubare le password degli utenti, di programmi e di accesso a siti Internet. Alcuni esempi sono i seguenti:

- Brute Force: un apposito programma prova tutte le possibili combinazioni di chiavi per decrittare il file protetto.
- Attacco a Dizionario: prova lunghissimi elenchi di parole, nomi e sigle di uso comune in una data lingua.
- Attacco all'Algoritmo: prevede la possibilità di intervenire su particolari debolezze matematiche o computazionali dell'algoritmo utilizzato.
- Password Sniffing: ruba la password - sniff - con qualche trucco, carpendola con un inganno ad esempio fingendosi responsabili di un servizio assistenza clienti o della sicurezza.

Crimini informatici: i sistemi informatici potrebbero essere utilizzati per compiere crimini informatici con implicazioni di tipo civile e penale (spamming, tentativi di intrusione, trattamento di testi o immagini proibite, violazione della corrispondenza, scaricamento di software o file non autorizzato o coperti da diritto d'autore, etc.).

Danni all'hardware: l'elemento più delicato dell'elaboratore è la memoria di massa. Se si dovesse danneggiare, a meno di ricorrere a pratiche costosissime sviluppate da centri specializzati, tutti i dati andrebbero persi. Quindi è fondamentale la centralizzazione di tutti i dati sul server, anche di quelli relativi a documenti estemporanei (documenti di testo, fogli di calcolo, presentazioni, ecc) che vanno conservati su file sharing aziendale e per nessun motivo vanno conservati sul proprio desktop

Usurpazione di identità: al momento di stabilire un collegamento alla rete o di ricevere dati, l'utente deduce l'identità del suo interlocutore in funzione del contesto in cui avviene la comunicazione e potrebbe scaricare un software maligno da un sito web che si fa passare per fonte affidabile per cui si potrebbero anche rivelare informazioni riservate alla persona sbagliata.

IP spoofing: l'autore dell'attacco sostituisce la propria identità a quella di un utente legittimo del sistema. Viene fatto non per generare intrusione in senso stretto, ma per effettuare altri attacchi. Lo spoofing si manifesta come attività di "falsificazione" di alcuni dati telematici, come ad esempio di un indirizzo IP o dell'indirizzo di partenza dei messaggi di posta elettronica.

Spamming: saturazione di risorse informatiche a seguito dell'invio di un elevato numero di comunicazioni tali da determinare l'interruzione del servizio. Ad esempio l'invio di molti messaggi di posta elettronica con allegati provoca la saturazione della casella e la conseguente non disponibilità a ricevere ulteriori messaggi.

Incidenti ambientali e eventi imprevisti: calamità naturali (tempeste, inondazioni, incendi e terremoti); guasti dell'hardware o del software dei componenti o dei programmi utilizzati; errore umano dell'operatore (compresi i fornitori di servizi) o dell'utente (ad esempio problemi di gestione della rete, installazione errata del software).

Art. 11 - Comportamento da tenere in caso di rilevazione anomalia o punto di debolezza del sistema informativo o indisponibilità dei dati

In caso di rilevazione di un'anomalia o punto di debolezza del sistema informativo, soprattutto se impatta o può potenzialmente impattare sulla sicurezza dei dati personali intesa come integrità, disponibilità e riservatezza, l'Utente è tenuto a darne tempestiva comunicazione, possibilmente scritta, al Responsabile opportunamente individuato. L'utente deve inoltre collaborare attivamente con quest'ultimo, in base alle indicazioni ricevute, per la tempestiva risoluzione e per la verifica del ripristino delle condizioni di normalità. E' altresì importante che l'Utente comunichi tempestivamente ai Sistemi Informativi per il tramite degli strumenti aziendali (apertura ticket), eventuali anomalie quali ad esempio: calo notevole delle prestazioni della propria postazione, frequenti messaggi di errore, comparsa di una nuova home page e/o di un nuovo motore di ricerca predefinito nel proprio browser di navigazione.

In caso si verifichi una violazione dei dati personali (Data Breach), ossia una 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 è necessario darne immediata comunicazione al Responsabile del Trattamento o al Responsabile della Protezione dei Dati – DPO o al Titolare del Trattamento (Direttore Generale), affinché possano attivare le procedure di notifica previste dalla legge.

Il Responsabile della Protezione dei dati (DPO) individuato dall'ASST è il seguente soggetto:
Società LTA Advisor Srl
E-mail: consulenza@ltadvisors.it

Art. 12 - Utilizzo di fax, stampanti e fotocopiatrici, telefoni, tablet, smartphone

Il telefono o qualsiasi strumento di telefonia (fisso o mobile, fisico o virtuale) o connettività mobile affidato all'Utente è uno strumento di lavoro. Ne viene concesso l'uso 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 consentito solo nel caso di comprovata necessità ed urgenza.

L'eventuale uso promiscuo (anche per fini personali) del telefono cellulare aziendale o di qualsiasi strumento di telefonia o connettività mobile affidato all'Utente è possibile soltanto in presenza di preventiva autorizzazione scritta e in conformità alle istruzioni al riguardo impartite dall'ASST ovvero nel caso di attivazione di contratti personali su dispositivi aziendali (servizi di dual billing con fatturazione diretta sul proprio conto corrente delle chiamate personali).

È vietato l'utilizzo delle fotocopiatrici e delle stampanti per fini personali. La ASST si riserva la facoltà di impedire l'invio di scansioni documentali dai fotocopiatori multifunzione ad indirizzi mail caratterizzati da un dominio diverso da quello aziendale.

E' fatto divieto all'utente utilizzatore di dispositivi smartphone o tablet aziendali di installare qualsiasi applicazione che non sia strettamente legata allo svolgimento dell'attività professionale e che non sia stata preventivamente autorizzata dai Sistemi Informativi.

I dispositivi smartphone e tablet aziendali sono controllati e amministrati da specifico impianto MDM (*Mobile Device Management*) gestito dai Sistemi Informativi che limita l'utilizzo dei dispositivi per i soli scopi aziendali e impedisce l'installazione di ulteriori applicazioni.

In caso di furto o smarrimento di dispositivo mobile, si procede al blocco e alla cancellazione (wipe) del medesimo attraverso le funzioni erogate dal software MDM.

Art. 13 - Accesso ai dati trattati dall'Utente

È facoltà dell'ASST, tramite il personale incaricato della gestione del sistema informatico o addetti alla manutenzione, accedere direttamente, nel rispetto della normativa sulla privacy, a tutti gli strumenti informatici e ai documenti ivi contenuti. Le informazioni raccolte mediante tali operazioni di accesso, sulla base del presente regolamento che funge anche da strumento informativo, possono essere utilizzate a tutti i fini connessi al rapporto di lavoro ai sensi dell'art. 4, comma 3, Legge 300/1970 (come modificato dal D. Lgs. 151/2015).

Art. 14 - Controlli

Al fine di verificare il corretto utilizzo degli strumenti come da prescrizioni esplicitate nel presente paragrafo potranno essere svolti dei controlli sia "remoti" (attraverso sistemi software all'uopo deputati) che "fisici" presso le singole postazioni o i singoli strumenti, senza entrare nel merito dei contenuti o delle attività svolte dall'utente.

Gli operatori dei Sistemi Informativi autorizzati allo svolgimento dei controlli, utilizzeranno specifico software di remote inventory che analizza in maniera trasparente all'utenza tutti i software installati sulla postazione di lavoro e può effettuare installazioni, aggiornamenti o rimozione di pacchetti software secondo le esigenze tecniche o di sicurezza richieste al corretto svolgimento dell'attività professionale.

Gli operatori dei Sistemi Informativi autorizzati allo svolgimento dei controlli, possono collegarsi alle postazioni di lavoro (sino esse fisiche o virtuali) attraverso specifico software di amministrazione remota che richiede un esplicito consenso da parte dell'utente utilizzatore della postazione. Ogni accesso in modalità controllo remoto da parte degli Amministratori di Sistema viene tracciata e conservata.

In nessun caso verranno compiuti controlli prolungati, costanti o indiscriminati.

I controlli saranno svolti in conformità alla legge, sia per eseguire verifiche sulla funzionalità e sicurezza del sistema, sia per verificare il corretto utilizzo da parte degli utenti (dipendenti, collaboratori, etc.). Nell'esercizio del potere di controllo l'ASST si atterrà al principio generale di proporzionalità e non eccedenza delle attività di controllo.

Il personale tecnico specificatamente incaricato è autorizzato a compiere interventi nel sistema informatico dell'ASST ed ha la facoltà di collegarsi alle singole postazioni di lavoro al fine di garantire l'assistenza tecnica, la normale attività operativa e la sicurezza e salvaguardia del sistema stesso.

Il personale incaricato della gestione del sistema informatico può in qualunque momento procedere alla rimozione di ogni file o applicazioni installati in violazione delle prescrizioni di cui al presente regolamento.

Il personale incaricato della gestione del sistema informatico può in qualunque momento eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.

14.1 - Sistemi di controllo graduali

L'ASST informa circa la necessità di porre in essere adeguati sistemi di controllo sull'utilizzo degli strumenti di cui al presente Regolamento nel rispetto dei criteri e dei principi stabiliti dal Garante per la protezione dei dati personali (provvedimento n. 13 del 01/03/07) e di valutare conseguentemente gli usi scorretti che, oltre ad esporre l'ASST stessa a rischi, tanto patrimoniali quanto penali, possono di per sé considerarsi contrari ai doveri di diligenza e fedeltà previsti dagli artt. 2104 e 2105 del Codice Civile.

I controlli sull'uso degli strumenti informatici/telefonici tuttavia garantiranno tanto il diritto di proteggere la propria ASST , essendo strumenti di lavoro la cui utilizzazione personale è preclusa, quanto il diritto del lavoratore a non vedere invasa la propria sfera personale, e quindi il diritto alla riservatezza ed alla dignità come sanciti dallo Statuto dei lavoratori (legge n. 300/1970) e D.Lgs. n.165/2001.

e ss.mm.ii. (testo unico del Pubblico impiego) ed ai CCNL di settore dal General Data Protection Regulation - GDPR (Regolamento 679/2016/UE).

Il Regolamento, essendo rilevante ai fini delle eventuali azioni disciplinari attivabili dal datore di lavoro nei confronti del dipendente, è stato redatto tenendo opportunamente conto altresì delle disposizioni contenute nella Legge. n. 300/1970 e D.Lgs. n.165/2001 e ss.mm.ii. (testo unico del Pubblico impiego) ed ai CCNL di settore in tema di provvedimenti disciplinari.

Nel rispetto della normativa in tema di protezione dei dati personali, l'attività di controllo espletata dall'ASST garantisce il rispetto dei principi fondamentali di "proporzionalità", i diritti e le libertà fondamentali, nonché la dignità dell'interessato e soprattutto prevede la fornitura di un'adeguata e preventiva informativa.

Si comunica pertanto che in caso di anomalie, il personale incaricato dalla Direzione potrà effettuare controlli anonimi, che si concluderanno con avvisi generalizzati diretti ai dipendenti dell'area / settore in cui è stata rilevata l'anomalia, nei quali si evidenzierà l'utilizzo irregolare degli strumenti aziendali e si inviteranno gli interessati ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite.

In nessun caso verranno compiuti controlli prolungati, costanti o indiscriminati.

Art. 15 - 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 C.C.N.L. applicabile, nonché con tutte le azioni civili e penali consentite anche nei confronti di collaboratori e professionisti.

Art. 16 - Entrata in vigore, riesame e aggiornamento

Il presente regolamento entra in vigore a partire dall'adozione dello specifico atto deliberativo.

Il Regolamento viene riesaminato ed eventualmente aggiornato con cadenza periodica annuale o nel caso in cui si siano verificati cambiamenti significativi, al fine di garantirne sempre l'idoneità, l'adeguatezza e l'efficacia.