
	Regolamento interno ICT	Rev. 1.0 Pag. 1/22 Regolamento-ICT_ASFLG
---	--------------------------------	--

REGOLAMENTO PER L'UTILIZZO E LA GESTIONE DELLE RISORSE STRUMENTALI INFORMATICHE E TELEMATICHE AZIENDALI


ASL FOGGIA

1.0	09/05/2024	M. De Matteis - C. A. Di Matteo	T. Petrosillo	A. Nigri	Nuova emissione
Rev.	Data	Redatto	Verificato	Approvato	Descrizione

 ASL Foggia PugliaSalute	MODULO Regolamento ICT	<i>Rev. 1.0</i> <i>Pag. 2/22</i> Regolamento-ICT-ASLFG
--	---	--

SOMMARIO

1. Premessa	3
2. Campo di applicazione	4
3. Utilizzo del personal computer	5
4. Hardware e Software.....	7
5. Utilizzo di PC dedicati alla strumentazione	8
6. Computer portatili e dispositivi mobili.....	9
7. Stampanti e Fotocopiatori.....	9
8. Credenziali di accesso.....	10
9. Utilizzo della rete e accessi da remoto.....	12
10. Supporti rimovibili	13
11. Social Media	13
12. Posta elettronica.....	14
13. Navigazione internet.....	17
14. Protezione da virus	18
15. Salvataggio dati.....	18
16. Teleassistenza	19
17. Monitoraggio.....	19
18. Controlli.....	21
19. Sanzioni	22
20. Aggiornamento e revisione	22

 <p>ASL Foggia PugliaSalute</p>	<p>MODULO Regolamento ICT</p>	<p><i>Rev. 1.0</i> <i>Pag. 3/22</i> Regolamento-ICT-ASLFG</p>
--	---	---

1. Premessa

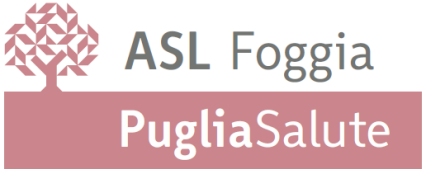
Premesso che l'utilizzo delle risorse informatiche e telematiche deve sempre ispirarsi, in applicazione di quanto disposto dagli artt. 2104 e 2105 c.c., al **principio della diligenza, fedeltà e correttezza, comportamenti che normalmente si adottano nell'ambito dei rapporti di lavoro**, adottando, quindi, tutte le cautele e le precauzioni necessarie per evitare le possibili conseguenze dannose alle quali un utilizzo non avveduto di tali strumenti può produrre, anche in considerazione della difficoltà di tracciare una netta linea di confine tra l'attività lavorativa e la sfera personale e la vita privata del lavoratore e di terzi che interagiscono con quest'ultimo.

La progressiva diffusione delle nuove tecnologie informatiche, le maggiori possibilità di interconnessione tra computer e l'aumento di informazioni trattate con strumenti elettronici aumentano i rischi legati alla sicurezza e all'integrità delle informazioni oltre alle conseguenti responsabilità previste dalla normativa vigente in materia.

L'Azienda Sanitaria Locale della provincia di Foggia (d'ora in avanti "ASL FOGGIA") con il presente atto adotta un Regolamento interno diretto ad evitare che comportamenti inconsapevoli possano innescare problemi alla gestione della Rete informatica aziendale e/o minacce alla sicurezza nel trattamento dei dati personali di qualsivoglia tipo (personale, sensibile e giudiziario) e per richiamare le indicazioni e le misure necessarie ed opportune per il corretto utilizzo, nel rapporto di lavoro, dei personal computer (fissi e portatili), dei dispositivi elettronici aziendali in genere, della posta elettronica e di internet, **definendone le modalità di utilizzo nell'ambito dell'attività lavorativa.**

La progressiva diffusione delle nuove tecnologie informatiche ed, in particolare, il libero accesso alla rete Internet dai Personal Computer, espone la Rete **dell'ASL FOGGIA** a rischi di natura patrimoniale, oltre alle responsabilità penali conseguenti alla violazione di specifiche disposizioni di legge, creando evidenti problemi alla sicurezza e all'immagine **di questa ASL. Pertanto le prescrizioni di seguito previste si aggiungono ed integrano le specifiche istruzioni già fornite a tutti i Responsabili, Delegati e Soggetti autorizzati al trattamento dei dati in attuazione del D.Lgs. 30 giugno 2003 n. 196, così come modificato dal D.Lgs. 101/2018 ed in osservanza del Regolamento UE 2016/679.**

L'ASL FOGGIA necessita di garantire un servizio continuativo, nel suo stesso interesse, ed assicurare la riservatezza delle informazioni e dei dati, in maniera tale da evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla sicurezza nel trattamento dei dati o diminuire l'efficienza delle risorse informatiche. L'ASL FOGGIA riconosce il valore fondamentale dell'utilizzo di strumenti di comunicazione sia nella comunicazione interna che con l'utenza esterna, anche al fine di ridurre i tempi di risposta e di migliorare pertanto l'efficienza del proprio operato.

	MODULO Regolamento ICT	<i>Rev. 1.0</i> <i>Pag. 4/22</i> Regolamento-ICT-ASLFG
---	---	--

2. Campo di applicazione

Il presente Regolamento si applica a tutti i dipendenti, senza distinzione di ruolo o livello, nonché a tutti i collaboratori dell'ASL FOGGIA a prescindere dal rapporto contrattuale con lo stesso intrattenuto (consulenti, tirocinanti, borsisti, volontari, ditte esterne autorizzate, ecc.). Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche e telematiche, per "utente" deve intendersi ogni soggetto, in possesso di specifiche credenziali di autenticazione, operante su computer in rete aziendale. Tale figura si configura quale "persona autorizzata al trattamento" ai sensi del Regolamento UE 2016/679. **Il presente Regolamento contiene le disposizioni relative alle corrette modalità di utilizzo della rete informatica dell'ASL FOGGIA e di tutte le risorse aziendali, in conformità e nel rispetto di quanto previsto dalla specifica normativa di settore e dalle ulteriori disposizioni emanate.**

Gli strumenti informatici oggetto del presente Regolamento sono di proprietà dell'ASL FOGGIA e sono messi a disposizione degli Utenti al fine di permettere il quotidiano svolgimento delle proprie prestazioni lavorative. Essi sono essenzialmente individuabili nei computer, negli apparati removibili, nei sistemi di identificazione e di autenticazione informatica, Internet e negli strumenti di scambio di comunicazioni e file, nella posta elettronica e in qualsiasi altro programma e apparecchiatura informatica destinata a memorizzare o a trasmettere dati e informazioni.

E' responsabilità di tutti i soggetti che utilizzano gli strumenti informatici messi a disposizione, di applicare e rispettare puntualmente le disposizioni del presente Regolamento.


Sono esentati dall'applicazione del presente Regolamento, e limitatamente a quanto necessario per il corretto svolgimento delle proprie funzioni, gli Amministratori di Sistema formalmente nominati.

Per qualsiasi dubbio relativo all'applicazione pratica ed all'interpretazione autentica delle disposizioni contenute nel presente Regolamento, è possibile rivolgersi al Responsabile della S.S. Sistemi Informativi Aziendali o direttamente al Responsabile della protezione dei dati dell'ASL di Foggia.

Per **Amministratore di Sistema** si intende il soggetto cui è conferito il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di base dati e di consentirne l'utilizzazione.

Devono essere nominati Amministratori di Sistema tutti coloro che, nell'espletamento delle loro consuete attività tecniche, sono "Responsabili" di fasi lavorative che possono comportare elevate criticità rispetto alla protezione dei dati, quali:

- gestione dei sistemi di autenticazione e di autorizzazione;
- custodia delle credenziali di autenticazione e di autorizzazione;
- salvataggio dei dati (backup/recovery);
- organizzazione dei flussi di rete;

 ASL Foggia PugliaSalute	MODULO Regolamento ICT	<i>Rev. 1.0</i> <i>Pag. 5/22</i> Regolamento-ICT-ASLFG
--	---	--

- gestione dei supporti di memorizzazione;
- manutenzione hardware.

Possono dunque qualificarsi quale Amministratori di sistema i seguenti soggetti:

- amministratori di sistemi di autenticazione e di autorizzazione;
- amministratori di server e pc;
- amministratori di apparati di rete;
- amministratori di base di dati;
- amministratori di apparati di sicurezza;
- amministratori di applicazioni.

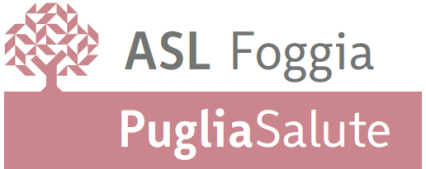
Nel caso di servizi di amministrazione di sistema affidati in outsourcing, quale Responsabile esterno del trattamento, l'ASL FOGGIA dovrà impegnarsi a conservare direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema. Qualora l'attività degli amministratori di sistema riguardi servizi o sistemi che trattano informazioni di carattere personale di dipendenti, l'ASL FOGGIA è tenuto a rendere nota o conoscibile l'identità degli Amministratori di sistema nell'ambito della propria organizzazione.

3. Utilizzo del personal computer

Il personal computer affidato all'Utente è uno strumento di lavoro. Ogni utilizzo non inerente all'attività lavorativa è vietato perché può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. Il PC deve essere custodito con cura evitando ogni possibile forma di danneggiamento.

Il personal computer dato in affidamento all'Utente permette l'accesso alla rete aziendale solo attraverso specifiche credenziali di accesso ed autenticazione.

L'ASL FOGGIA rende noto che l'attuale società affidataria del servizio di assistenza e manutenzione della rete informatica, nella qualità di Responsabile esterno del trattamento e nella fattispecie in qualità di Amministratore di Sistema, è autorizzato a compiere interventi nel sistema informatico, diretti a garantire la sicurezza e la salvaguardia del sistema stesso, nonché per ulteriori motivi tecnici e/o manutentivi. Detti interventi potranno anche comportare l'accesso in qualunque momento, ai dati trattati da ciascuno, ivi compresi gli archivi su PC e Server, nonché alla verifica sui siti internet acceduti dagli utenti abilitati. La stessa facoltà, sempre ai fini della sicurezza del sistema e per garantire

	MODULO Regolamento ICT	<i>Rev. 1.0</i> <i>Pag. 6/22</i> Regolamento-ICT-ASLFG
---	---	--

la normale operatività dell'ASL FOGGIA, si applica anche in caso di assenza prolungata od impedimento del dipendente.


La società di cui sopra ha la facoltà di collegarsi, previa autorizzazione dell'Utente, e visualizzare in remoto il desktop delle singole postazioni PC al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza contro virus informatici in genere. L'intervento viene effettuato esclusivamente su chiamata dell'utente o, in caso di oggettiva necessità, a seguito della rilevazione tecnica di problemi nel sistema informatico e telematico. In quest'ultimo caso, e sempre che non si pregiudichi la necessaria tempestività ed efficacia dell'intervento, verrà data formale comunicazione della necessità dell'intervento stesso.

Il personal computer viene fornito con configurazione software predefinita che non può essere per alcun motivo modificata da parte dell'utente. Le richieste di installazione di nuovo software o di modifica della configurazione devono essere inviate sul sistema di trouble ticketing al link <https://helpdesk.aslfg.it>.

L'utente non può modificare le impostazioni del PC autonomamente.

Di conseguenza:


- non saranno forniti privilegi di "amministratore" ad eccezione di specifiche e motivate esigenze avanzate formalmente da parte del Responsabile della Struttura interessata e dietro specifica autorizzazione rilasciata dal **Responsabile della S.S. Servizi Informativi Aziendali**;
- non è consentita l'installazione di mezzi di comunicazione personali (come ad esempio modem e dispositivi bluetooth, smartphone, chiavette per l'accesso ad internet etc.);
- non è consentito utilizzare strumenti software e/o hardware atti a intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici;
- non è consentito copiare sul proprio computer file contenuti in supporti magnetici, ottici e dispositivi usb non aventi alcuna attinenza con la propria prestazione lavorativa;
- il computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio o in caso di suo inutilizzo;
- qualora ci si allontani dalla propria postazione, occorre bloccare il computer o disconnettersi (per il sistema operativo windows premendo contemporaneamente i tasti Alt+Ctrl+Canc e cliccando su blocca computer o in alternativa attivando la protezione sul proprio screen saver); 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.
- non è consentito utilizzare strumenti potenzialmente in grado di consentire accessi non autorizzati alle risorse informatiche (es.: programmi di condivisione quali IRC, ICQ, o software di monitoraggio della rete in genere);

 <p>ASL Foggia PugliaSalute</p>	<p>MODULO Regolamento ICT</p>	<p><i>Rev. 1.0</i> <i>Pag. 7/22</i> Regolamento-ICT-ASLFG</p>
--	---	---

- non è consentito configurare o utilizzare servizi diversi da quelli messi a disposizione da parte dell'ASL FOGGIA (quali DNS, DHCP, server internet Web, FTP,...);
- non è consentito intercettare pacchetti sulla rete (sniffer) o software dedicati a carpire, in maniera invisibile, dati personali, password e ID dell'utente oppure a controllare ogni attività, ivi inclusa la corrispondenza e i dati personali;
- non è consentito impostare password nel bios;
- non è consentito disassemblare il computer, asportare, scollegare, aggiungere, spostare o semplicemente scambiare tra un PC e l'altro qualsiasi apparecchiatura in dotazione all'Utente salvo diretta e specifica indicazione del personale tecnico della P.O. SIA;
- non è consentito avviare il personal computer con sistemi operativi diversi da quello installato dal personale autorizzato;
- non è consentito utilizzare connessioni in remoto per l'accesso alle risorse aziendali, al di fuori del perimetro aziendale e fatte salve le connessioni realizzate e autorizzate da parte del **Responsabile della S.S. Servizi Informativi Aziendali**;
- salvo preventiva espressa formale autorizzazione del **Responsabile della S.S. Sistemi Informativi Aziendali** tramite <https://helpdesk.aslfg.it> non è consentito l'uso di programmi diversi da quelli ufficialmente installati, né viene consentito agli utenti di installare autonomamente programmi provenienti dall'esterno, sussistendo infatti il grave pericolo di introdurre virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti. L'inosservanza della presente disposizione espone l'ASL FOGGIA a gravi responsabilità civili; si evidenzia inoltre, che le violazioni della normativa a tutela dei diritti d'autore sul software, che impone la presenza nel sistema di software regolarmente licenziato o comunque libero e quindi non protetto dal diritto d'autore, saranno sanzionate anche penalmente;
- ogni Utente deve prestare la massima attenzione ai supporti di origine esterna, sottoponendoli sempre a scansione antivirus ed avvertendo immediatamente il personale tecnico preposto nel caso in cui siano rilevati virus di qualsivoglia natura.
- **Non è consentito collegare alla rete informatica Personal Computer o PC Portatili personali e, più in generale, qualsiasi dispositivo hardware senza la autorizzazione del Responsabile della S.S. Servizi Informativi Aziendali, su esplicita richiesta motivata del Direttore della struttura interessata.**

4. Hardware e Software

Tutto l'hardware ed il software collegato ai sistemi in rete, potrà essere acquistato solo previa richiesta di parere tecnico favorevole al Responsabile della S.S. Servizi Informativi Aziendali, che

 <p>ASL Foggia PugliaSalute</p>	<p align="center">MODULO Regolamento ICT</p>	<p><i>Rev. 1.0</i> <i>Pag. 8/22</i> Regolamento-ICT-ASLFG</p>
--	--	---

controllerà le richieste di acquisto al fine di valutarne la compatibilità e programmare l'applicazione delle misure di sicurezza informatica aziendali.

A tal fine le richieste particolari di acquisto dell'hardware e del software dovranno essere indirizzate al Responsabile della S.S. Sistemi Informativi Aziendali per la verifica tecnica di compatibilità o per la proposizione di soluzioni alternative. I supporti originali dei software acquistati e le relative licenze devono essere custoditi presso la S.S. Sistemi Informativi, così da consentire le operazioni di verifica della disponibilità di licenze e l'eventuale reinstallazione delle procedure.


Il software per elaboratori è considerato opera di ingegno e come tale è tutelato dalle Leggi sul diritto di autore. L'utilizzo del software è regolamentato da licenze d'uso che devono essere assolutamente rispettate da tutti (Dlgs. 518/92 sulla tutela giuridica del software, L. 633/41 e L. 248/2000 "nuove norme di tutela del diritto d'autore" e s.m.i.). È vietato provare ad installare arbitrariamente il software scaricato da Internet o contenuto nei vari supporti distribuiti con le riviste, con i libri e con i quotidiani anche se si tratta di software allegato a riviste del settore. Prima di installare questi programmi, qualora l'uso fosse collegato ad esigenze lavorative, sarà necessario il benestare del **Responsabile della S.S. Servizi Informativi Aziendali**.

5. Utilizzo di PC dedicati alla strumentazione

Il collegamento alla rete aziendale di computer dedicati alla strumentazione deve essere richiesto e concordato con la **S.S. Sistemi Informativi Aziendali** che provvederà alla verifica della fattibilità e della compatibilità tecnica del collegamento. In caso di interventi di manutenzione effettuati da Ditte esterne su computer strumentali collegati alla rete aziendale, questi devono essere preventivamente valutati e concordati. Al fine di evitare il rischio di alterazione dei risultati delle analisi non sono permessi utilizzi differenti allo scopo cui sono dedicate tali risorse. Eventuali installazioni di ulteriori programmi devono essere preventivamente assoggettate a verifica di compatibilità e autorizzazione da parte dei **Sistemi Informativi**.

L'esecuzione dei backup dei dati residenti sui computer strumentali deve essere effettuata a cura del personale della Struttura che ha in carico l'apparecchiatura strumentale, in particolare come di seguito specificato:

- computer in rete con salvataggio dei dati sul server: il backup viene eseguito automaticamente secondo le modalità definite dai **Sistemi Informativi Aziendali** ;
- computer non in rete o in rete senza salvataggio dei dati sul server: il backup viene effettuato dal personale del laboratorio previa verifica preliminare da parte dei **Sistemi Informativi**

 <p>ASL Foggia PugliaSalute</p>	<p>MODULO Regolamento ICT</p>	<p><i>Rev. 1.0</i> <i>Pag. 9/22</i> Regolamento-ICT-ASLFG</p>
--	---	---

Aziendali che ne valuta la modalità più idonea (salvataggio su CD/DVD, su pen-drive e altri supporti esterni);

- computer che non permettono alcun tipo di backup: in questo caso i **Sistemi Informativi Aziendali**, in collaborazione con la ditta esterna incaricata della manutenzione, valuteranno l'investimento tecnologico necessario per rendere il computer idoneo all'esecuzione del backup dei dati.

6. Computer portatili e dispositivi mobili

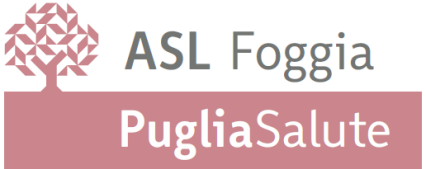
L' Utente è responsabile dell'integrità del computer portatile e dei dispositivi mobili (tablet, smartphone, router portatili, etc.) affidatigli dall'ASL FOGGIA e dei dati ivi contenuti. L'Utente è tenuto a custodirli con diligenza sia durante l'utilizzo nel luogo di lavoro sia durante i suoi spostamenti. A tali dispositivi si applicano le regole di utilizzo previste per i personal computer. Nel caso di utilizzo condiviso con altri Utenti, prima della riconsegna occorre provvedere alla rimozione definitiva di eventuali file elaborati. I dischi rigidi, se contenenti dati sensibili, dovranno essere criptati al fine di evitare, in caso di furto o di smarrimento, l'accesso a dati riservati e/o personali da parte di soggetti non autorizzati. Tutti i dispositivi portatili dovranno essere inviati alla **S.S. Sistemi Informativi Aziendali** che provvederà all'applicazione di tutte le misure di sicurezza previste da disciplinare interno e dalla normativa vigente.

Per quanto concerne l'utilizzo degli Smartphone, Tablet, Router portatili e in generale per tutti quei dispositivi ove è previsto il possibile inserimento di una SIM aziendale, si rimanda all'allegato (Regolamento-MOBILE-ASL-FG).

7. Stampanti e Fotocopiatori

Per quanto concerne l'utilizzo delle stampanti, l'Utente è tenuto a:

- stampare documenti e atti solo se strettamente necessari per lo svolgimento delle proprie funzioni lavorative;
- prediligere le stampanti di rete in luogo di quelle locali al fine di ridurre l'utilizzo di materiali di consumo (toner, cartucce, ...);
- prediligere le stampanti laser in luogo di quelle che prevedono consumi maggiori, quali stampanti a getto di inchiostro; stampare in bianco/nero e fronte/retro al fine di ridurre i costi, laddove possibile.

	MODULO Regolamento ICT	<i>Rev. 1.0</i> <i>Pag. 10/22</i> Regolamento-ICT-ASLFG
---	---	---

Le stampanti locali devono essere spente ogni sera prima di lasciare gli uffici o in caso di loro inutilizzo.

Qualora il dipendente dovesse stampare documenti contenenti dati o informazioni riservate, dovrà aver cura di monitorare la stampante e preservare, limitatamente alle oggettive possibilità, la conoscibilità di tali dati o informazioni da parte di terzi non autorizzati. Pertanto si raccomanda di non lasciare documenti incustoditi nei fax, nei fotocopiatori e nelle stampanti condivise.

Eventuali fotocopie o stampe mal riuscite di documenti contenenti dati personali devono essere distrutte.

Il trasferimento di ogni documento contenente dati sensibili o giudiziari deve avvenire adottando rigorose misure di garanzia, tali da impedire che allo stesso accedano estranei: buste chiuse, documenti sigillati, non abbandono durante i trasferimenti. Ogni dispositivo idoneo a stampare documenti deve essere collocato in modo che la visione dei documenti in uscita sia possibile solo da parte del personale incaricato al trattamento dei dati.

In caso di accessi da parte di estranei il personale incaricato deve prestare particolare attenzione affinché questi ultimi non vengano in contatto con dati in uscita da stampanti e fax eventualmente posizionati in corridoi in comune tra gli uffici.

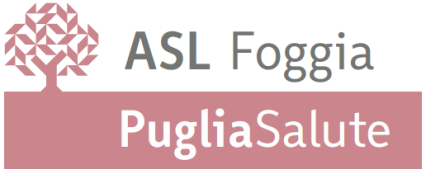
Il personale incaricato ha il dovere di sincerarsi che al momento dello spegnimento dei computer non vi siano documenti in coda di stampa.

La documentazione contenente dati sensibili o giudiziari (dati appartenenti a categorie particolari di cui agli artt. 9-10 del Regolamento UE 2016/679) deve essere trasferita, anche all'interno dell'Azienda, in busta chiusa, in modo da assicurare la protezione della riservatezza sia del documento che dei dati contenuti. Per dare garanzia della non apertura della busta e della integrità del contenuto sarebbe opportuno che i lembi della busta fossero sigillati. In alternativa è comunque opportuno piegare il documento spillandone i lati.

8. Credenziali di accesso

I sistemi di controllo degli accessi in rete informatica assolvono il compito di prevenire che persone non autorizzate possano accedere a un sistema informatico ed alle relative applicazioni. Lo scopo è di cautelare l'ASL FOGGIA e i suoi dipendenti da ogni tipo di manomissione, furto o distruzione di dati oltre che di limitare l'accesso a specifici dati da parte di personale non autorizzato.

Le credenziali di autenticazione nell'intranet (accesso rete aziendale), vengono inizialmente assegnate dai **Sistemi Informativi Aziendali** e successivamente obbligatoriamente reimpostate dal dipendente stesso secondo criteri prestabiliti dalla normativa vigente e con modalità operative di seguito meglio specificate. Non sono ammesse impostazioni autonome della password al Bios del computer onde evitare impedimenti all'accesso in caso di prolungata assenza o impedimento dell'incaricato e

	MODULO Regolamento ICT	<i>Rev. 1.0</i> <i>Pag. 11/22</i> Regolamento-ICT-ASLFG
---	---	---

considerata la necessità dell'ASL FOGGIA di garantire in ogni caso la continuità dei servizi istituzionali.

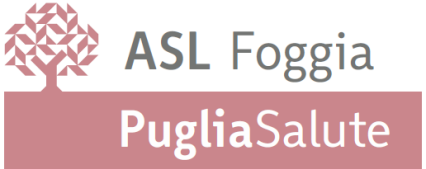
Le credenziali di autenticazione per l'accesso alla rete informatica e per l'utilizzo del servizio di posta elettronica vengono assegnate dalla **S.S. Sistemi Informativi Aziendali** previa formale richiesta da effettuarsi attraverso la compilazione dell'apposito modulo "MOD-01-RM", sottoscritta dal Dirigente Responsabile della Struttura presso la quale l'Utente dovrà operare ed inserita su <https://helpdesk.aslfg.it>.

Nel caso di collaboratori a progetto e coordinati e continuativi quali borsisti, tirocinanti, volontari etc. la preventiva richiesta, se necessaria, verrà inoltrata direttamente dalla Direzione Aziendale (ovvero dal Dirigente Responsabile della Struttura con la quale il collaboratore si coordina nell'espletamento del proprio incarico). Sarà cura del Responsabile dare tempestiva comunicazione al Responsabile della S.S. Servizi Informativi Aziendali, apertura di un ticket su <https://helpdesk.aslfg.it>", nell'eventualità che il collaboratore cessi o abbia cessato il rapporto con l'ASL FOGGIA prima del tempo indicato nel modulo di richiesta, al fine di evitare un possibile uso illecito dei servizi forniti. Stesso onere di comunicazione spetta al Responsabile nel caso in cui il collaboratore si trasferisca in altre U.O. o Sedi diverse.

La credenziale di autenticazione (login) consiste in un codice per l'identificazione dell'Utente (user id), assegnato dal personale tecnico autorizzato **dal Responsabile della S.S. Sistemi Informativi Aziendali** ed associato ad una parola chiave (password) riservata e modificata dall'Utente al primo accesso. Essa dovrà essere memorizzata, custodita con la massima diligenza e non divulgata (ad es.: non scrivere la password su carta o post-it lasciandoli sulla scrivania o attaccati al monitor; non comunicare o condividere con altri colleghi la propria password); durante la digitazione della propria password, assicurarsi che nessuno stia osservando la tastiera con l'intenzione di memorizzarla.

La password deve essere composta da almeno otto caratteri e deve essere "robusta". Una password si dice robusta quando è difficile ricostruirla e cioè quando risponde ad alcuni principi quali:

- all'aumentare della sua lunghezza, aumenta la difficoltà a carpirla;
- include cifre, lettere e caratteri speciali;
- non contiene il proprio nome o cognome, il soprannome, la data di nascita, il nome di persone familiari, parole comuni, nomi di paesi, animali e così via;
- non contiene parole che si trovano nei dizionari di qualsiasi lingua, anche se digitate al contrario, in quanto esistono software in grado di individuarle;
- non sono composte da semplici sequenze di tasti, come ad esempio "qwerty", o da ripetizioni del proprio nome utente (ad es. se il proprio utente è rossi; la password "rossi rossi" sarebbe inopportuna);
- è composta con più parole contenenti errori ortografici o con sillabe combinate costituite da parole non correlate tra loro.

	MODULO Regolamento ICT	<i>Rev. 1.0</i> <i>Pag. 12/22</i> Regolamento-ICT-ASLFG
---	---	---

La password di accesso di ciascun Utente di rete sarà automaticamente reimpostata ogni 90 giorni. In base a tale procedura automatica, l'Utente, mediante idoneo avviso a video, dovrà inserire una nuova password, diversa dalla precedente, pena il blocco del computer con conseguentemente inibizione dell'accesso alla rete aziendale.

L'Utente potrà richiedere la modifica della password al personale tecnico **della S.S. Servizi Informativi Aziendali**, per decorrenza del termine sopra previsto in via eccezionale e/o in via ordinaria in caso questi ravveda una perdita della riservatezza. Qualsiasi azione svolta sotto l'autorizzazione offerta dalla coppia userid e password sarà attribuita in termini di responsabilità all'utente titolare del codice userid, salvo che l'utente dia prova di illecito utilizzo della sua autorizzazione da parte di terzi.

9. Utilizzo della rete e accessi da remoto

Per l'accesso alla Rete (intranet aziendale) ciascun Utente deve essere in possesso delle specifiche credenziali sopra descritte.

È assolutamente vietato accedere alla rete informatica aziendale e/o nei programmi con un codice d'identificazione Utente di un altro operatore.


La presenza di eventuali cartelle di rete condivise sono da considerarsi strumento di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi.

Si ricorda che tutti i dischi rigidi o altre unità di memorizzazione locali (es. dischi fissi interni o esterni al PC) non sono soggette a salvataggio da parte del personale incaricato **della S.S. Servizi Informativi Aziendali**. La responsabilità del salvataggio dei dati ivi contenuti è pertanto a carico del singolo Utente.

Il personale tecnico **della S.S. Sistemi Informativi Aziendali** può in qualunque momento, senza preavviso, procedere alla rimozione dai computer in rete di ogni file e/o applicazione che riterrà essere pericolosi per la sicurezza dei dati e della rete.

Non è consentito collegare alle prese di rete apparecchiature non autorizzate da parte **della S.S. Servizi Informativi Aziendali**, quali: hub, switch, access point o similari. Non è inoltre consentito installare o utilizzare qualsiasi altra apparecchiatura atta a gestire comunicazioni, salvo specifica autorizzazione rilasciata dal Responsabile **della S.S. Servizi Informativi Aziendali**, quali, a titolo esemplificativo: modem, router, Internet key,... Non è inoltre consentito effettuare spostamenti o modifiche di risorse collegate alla rete aziendale (es.: pc, stampanti, fotocopiatori e altro) senza una preventiva autorizzazione.

I tecnici delle ditte esterne (fornitori applicativi, sistemisti etc.) dovranno richiedere l'autorizzazione del Responsabile **della S.S. Sistemi Informativi Aziendali** prima di collegarsi fisicamente alla rete

 <p>ASL Foggia PugliaSalute</p>	<p>MODULO Regolamento ICT</p>	<p><i>Rev. 1.0</i> <i>Pag. 13/22</i> Regolamento-ICT-ASLFG</p>
--	---	--

aziendale con dispositivi personali. Quest’ultimi saranno sottoposti alle politiche di sicurezza di ASL FOGGIA al fine di garantire la sicurezza generale della rete informatica.

Gli accessi da remoto verso la rete aziendale potranno essere effettuati solo previa autorizzazione del **Responsabile della S.S. Sistemi Informativi Aziendali** che rilascerà apposite credenziali per l’autenticazione sicura a doppio fattore **dopo la compilazione di specifico** modulo “MOD-02-VPN” inserito su <https://helpdesk.aslfg.it>. Tutti gli accessi saranno monitorati e registrati. Non sono ammessi accessi di tipologia differente da quella VPN (IPSEC o SSL) definita dalla **S.S. Servizi Informativi Aziendali**.

10.Supporti rimovibili

Eventuali supporti magnetici contenenti dati sensibili devono essere adeguatamente custoditi dall’Utente in armadi o cassette chiudibili a chiave. **È vietato l’utilizzo di supporti rimovibili personali** (dischi rigidi e penne USB) compreso qualsiasi altro punto di memorizzazione tramite internet (c.d. “remote storage”) nel caso si voglia trattare dati personali, sensibili e/o giudiziari. In caso di trasferimento di dati sensibili tra computer in rete, si devono necessariamente utilizzare “cartelle di lavoro condivise” e protette da password note solo agli utenti a ciò interessati. L’Utente è responsabile della custodia dei supporti e dei dati in essi contenuti.

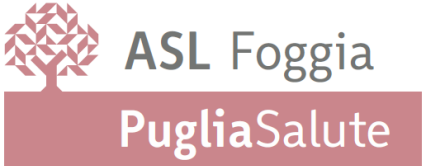
11.Social Media

L’ eventuale utilizzo di Facebook, Twitter, LinkedIn, WhatsApp, dei blog e dei forum, anche professionali (ed altri siti o social media) è gestito ed organizzato esclusivamente dall’ASL di Foggia attraverso specifiche direttive ed istruzioni operative al personale a ciò espressamente addetto, rimanendo escluse iniziative individuali da parte dei singoli utenti o collaboratori.

Fermo restando il diritto della persona alla libertà di espressione, l’ASL di Foggia ritiene comunque opportuno indicare agli utenti alcune regole comportamentali, al fine di tutelare tanto la propria immagine ed il patrimonio aziendale, anche immateriale, quanto i propri dipendenti, i propri fornitori oltre che gli stessi utilizzatori dei social media, fermo restando che è vietata la partecipazione agli stessi social media durante l’orario di lavoro.

Il presente articolo deve essere osservato dall’Utente sia che utilizzi dispositivi messi a disposizione dall’Ente, sia che utilizzi propri dispositivi, sia che partecipi ai social media a titolo personale, sia che lo faccia per finalità professionali, come dipendente dell’ASL di Foggia.

La condivisione dei contenuti nei social media deve sempre rispettare e garantire la segretezza sulle informazioni dell’ASL FOGGIA, nel rispetto del segreto d’ufficio, segreto professionale e della protezione dei dati. È vietato l’utilizzo di dispositivi di proprietà personale (tablet, smartphone etc..) per

	MODULO Regolamento ICT	<i>Rev. 1.0</i> <i>Pag. 14/22</i> Regolamento-ICT-ASLFG
---	---	---

la trasmissione e condivisione, tramite ad es WhatsApp, Telegram etc., di documenti ed informazioni aziendali, in particolar modo se riconducibili agli assistiti.

12. Posta elettronica

Il servizio di posta elettronica è un mezzo istituzionale di comunicazione aziendale e il suo utilizzo deve avvenire nel rispetto delle norme in materia di protezione dei dati personali.

La casella di posta elettronica assegnata all'Utente è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

Su richiesta del Responsabile della Struttura richiedente, la S.S. Sistemi Informativi Aziendali può assegnare due tipologie di account di posta elettronica aziendale:

1. account di posta elettronica di "servizio" (casella di gruppo condivisa), il cui nome richiama il Servizio in cui lavora il richiedente;
2. account di posta elettronica "individualizzata" legata al nominativo del dipendente (casella nominativa personale).

L'account di posta elettronica di "servizio", gestito mediante casella di posta condivisa, deve comunque essere associato ad almeno un account nominativo.

Il personale dipendente autorizzato all'accesso alla posta elettronica di servizio dovrà risultare formalmente autorizzato dal superiore gerarchico, ai sensi dell'art. 29 del Reg. UE 2016/679 e dell'art. 2-quatercedies c.1 del d.lgs 196/03. Il Responsabile di Struttura è tenuto a comunicare tempestivamente al Responsabile del Sistemi Informativi Aziendali qualsiasi variazione dei permessi di accesso al fine di proteggere i dati sensibili e riservati dall'accesso non legittimato.


L'accesso alla casella di posta elettronica avviene tramite interfaccia web senza nessuna installazione sulle postazioni di lavoro e dispositivi aziendali.

Per la sicurezza è di norma attivo un servizio di sandboxing che analizza i collegamenti presenti nelle mail per individuare URL malevoli.

È fatto divieto di utilizzare le caselle di posta elettronica per motivi diversi da quelli strettamente legati all'attività lavorativa.

In questo senso, a titolo puramente esemplificativo, l'Utente non potrà utilizzare la posta elettronica ordinaria e certificata per:

- l'invio e/o il ricevimento di allegati contenenti filmati o brani musicali (es. mp3) non legati all'attività lavorativa;
- l'invio e/o il ricevimento di messaggi personali o per la partecipazione a dibattiti, sondaggi e aste on-line;

 <p>ASL Foggia PugliaSalute</p>	<p>MODULO Regolamento ICT</p>	<p><i>Rev. 1.0</i> <i>Pag. 15/22</i> Regolamento-ICT-ASLFG</p>
--	---	--

- la partecipazione a catene di Sant'Antonio; non si dovrà in alcun caso procedere all'apertura degli allegati a tali messaggi.

La casella di posta elettronica deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti (in termini di centinaia di MB e, ancor più di GB).

È obbligatorio porre la massima attenzione nell'aprire i file allegati alle e-mail prima del loro utilizzo.

In linea di massima non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti, altrimenti, se obbligati sottoporre necessariamente detti file ad una "scansione approfondita" dell'antivirus prima del loro utilizzo.


L'Utente assegnatario della casella di posta elettronica istituzionale è il diretto responsabile del corretto utilizzo della stessa e risponde personalmente dei contenuti trasmessi. In particolare, l'Utente è tenuto a rispettare quanto segue:

- non utilizzare il servizio per scopi illegali o non conformi al presente Regolamento o in maniera tale da recar danno o pregiudizio all'ASL FOGGIA o a terzi;
- non utilizzare il servizio in modo da danneggiare, disattivare, sovraccaricare, pregiudicare o interferire con la fruibilità del servizio da parte degli altri utenti;
- non utilizzare la posta elettronica per inviare, anche tramite collegamenti o allegati in qualsiasi formato (testo, fotografico, video, grafico, audio, codice, ecc.), messaggi che contengano o rimandino ad esempio a: pubblicità non istituzionale, manifesta o occulta;

In nessun caso l'Utente potrà utilizzare la posta elettronica per diffondere codici dannosi per i computer quali virus e simili.

Di seguito si elencano alcune norme di comportamento che ciascun Utente è tenuto ad osservare al fine di preservare l'efficienza del servizio di posta elettronica e delle comunicazioni con esso veicolate:

- l'Utente è tenuto a visionare regolarmente la casella di posta elettronica di propria competenza;
- i messaggi devono essere preferibilmente di solo testo, evitando ove possibile ogni formattazione e inserzione di immagini;
- è buona norma inviare messaggi sintetici che descrivano in modo chiaro il contenuto;
- è necessario indicare sempre chiaramente l'oggetto, in modo tale che il destinatario possa immediatamente individuare l'argomento del messaggio ricevuto, facilitandone la successiva ricerca per parola chiave;
- non superare la dimensione complessiva di 10 Megabyte degli allegati inviati con un singolo messaggio;

 <p>ASL Foggia PugliaSalute</p>	<p>MODULO Regolamento ICT</p>	<p>Rev. 1.0 Pag. 16/22 Regolamento-ICT-ASLFG</p>
--	---	--

- limitare l'invio di messaggi di posta elettronica a indirizzi plurimi (decine di destinatari) e trasmetterli solo in casi motivati da esigenze di servizio;
- non aprire allegati con estensione .zip, .rar, .exe e similari se la provenienza risulti dubbia.


L'Utente, infine, si impegna a non inviare messaggi di natura ripetitiva (*c.d.* catene di Sant' Antonio) anche quando il contenuto sia volto a segnalare presunti o veri allarmi (esempio: segnalazioni di virus).

In caso di assenza prolungata programmata del dipendente, si consiglia e si raccomanda al dipendente di attivare il sistema di risposta automatica ai messaggi di posta elettronica ricevuti indicando, nel messaggio di accompagnamento, le coordinate di un collega o della struttura di riferimento che può essere contattata in sua assenza e/o altre modalità utili di contatto della Struttura organizzativa presso cui presta la propria attività lavorativa.

Nell'ipotesi di assenza o impossibilità, temporanea o protratta nel tempo, del dipendente, qualora per ragioni di sicurezza o comunque per garantire l'ordinaria operatività aziendale sia necessario accedere a informazioni o documenti di lavoro presenti sul personal computer del dipendente, inclusi i messaggi di posta elettronica in entrata ed in uscita, il dipendente può delegare un altro dipendente a sua scelta (fiduciario) il compito di verificare il contenuto di messaggi e inoltrare al responsabile della Struttura in cui lavora quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa.

Di tale attività deve essere redatto apposito verbale e informato il dipendente interessato alla prima occasione utile. In caso di assenza o impossibilità, temporanea o protratta nel tempo, del dipendente, qualora per ragioni di sicurezza o comunque per garantire l'ordinaria operatività aziendale sia necessario accedere a informazioni o documenti di lavoro presenti sul personal computer del dipendente, inclusi i messaggi di posta elettronica in entrata e in uscita, e il dipendente non abbia delegato un altro dipendente (fiduciario), secondo quanto sopra specificato, il Responsabile della Struttura cui afferisce il dipendente può chiedere al **Responsabile della S.S. Sistemi Informativi Aziendali** di accedere alla postazione e/o alla casella di posta elettronica del dipendente assente, in modo che si possa prendere visione delle informazioni e dei documenti necessari. Contestualmente, il Responsabile della Struttura deve informare il dipendente appena possibile, fornendo adeguata spiegazione e redigendo apposito verbale.

Le caselle di posta elettronica individuali hanno validità pari alla durata della permanenza in servizio del dipendente, fatte salve eventuali situazioni di congedo, distacco e comando. Nel caso in cui il dipendente non presti più la sua attività lavorativa presso questa ASL, la casella di posta elettronica sarà prontamente disattivata. Su richiesta dell'interessato, la casella di posta potrà restare attiva per **ulteriori tre mesi** dalla data di cessazione del rapporto di lavoro, durante il quale sarà inserita una risposta automatica d'ufficio. **Decorsi i tre mesi senza alcuna richiesta di copia delle email da parte del dipendente, questa ASL procederà con la cancellazione permanente dei dati.**

 <p>ASL Foggia PugliaSalute</p>	<p>MODULO Regolamento ICT</p>	<p><i>Rev. 1.0</i> <i>Pag. 17/22</i> Regolamento-ICT-ASLFG</p>
--	---	--

13. Navigazione internet

Il PC assegnato all'Utente ed abilitato alla navigazione in Internet costituisce uno strumento utilizzabile esclusivamente per lo svolgimento della propria attività lavorativa. È quindi assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa.

In questo senso, a titolo puramente esemplificativo, l'Utente non potrà utilizzare Internet per:


- l'upload o il download di software gratuiti se non espressamente autorizzati dal Responsabile della S.S. Servizi Informativi Aziendali;
- l'utilizzo di documenti (filmati e musica) provenienti da siti web o http, se non strettamente attinenti all'attività lavorativa;
- l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, fatti salvi i casi autorizzati e comunque nel rispetto delle normali procedure di acquisto;
- ogni forma di registrazione a siti i cui contenuti non siano strettamente legati all'attività lavorativa;
- la partecipazione a forum non professionali, a giochi on-line, l'utilizzo di chat line, di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames).

Al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa, l'ASL FOGGIA con logica preventiva, adotta uno specifico sistema di filtro automatico che impedisce determinate operazioni quali l'upload, download (illeciti o illegali) o l'accesso a determinati siti ludici (black-list). I filtri sopracitati limitano l'accesso ai siti Internet che presentano i seguenti contenuti: illegali o non etici, stupefacenti, razzismo e odio, estremismo, violenza, occultismo, plagio; materiale per adulti, nudità, pornografia; giochi, scommesse, intermediazione e trading, download software freeware; social network, radio e tv via Internet (salvo i casi espressamente autorizzati dalla Direzione Generale); peer to peer; malware, spyware, hacking, proxy anonimi, bypass proxy, phishing.

Qualsiasi altra tipologia di contenuti o siti che la Direzione Generale riterrà di non dover rendere accessibile dalla rete aziendale, verrà preventivamente comunicata agli utenti. La navigazione, ovvero l'accesso ai siti Internet, potrebbe avvenire previa autenticazione dell'Utente su di un Proxy Server.

I file contenenti le registrazioni della navigazione sul web sono conservati per il tempo strettamente necessario, determinato dalle norme in vigore e da esigenze di sicurezza.

Gli eventuali controlli per motivi di sicurezza informatica, compiuti dal personale tecnico autorizzato dalla **S.S. Servizi Informativi Aziendali**, potranno avvenire mediante un sistema di controllo dinamico dei contenuti o mediante "file di log" della navigazione svolta. Il controllo sui log, i quali sono

 <p>ASL Foggia PugliaSalute</p>	<p align="center">MODULO Regolamento ICT</p>	<p><i>Rev. 1.0</i> <i>Pag. 18/22</i> Regolamento-ICT-ASLFG</p>
--	--	--

cancellati periodicamente ed automaticamente, non è sistematico e le informazioni vengono conservate temporaneamente per finalità di sicurezza di questa ASL. Il prolungamento dei tempi di conservazione dei log potrà aver luogo solo nei seguenti casi:

- Esigenze tecniche o di sicurezza del tutto particolari;
- Indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;
- Su specifica richiesta dell'autorità giudiziaria

L'utilizzo degli strumenti aziendali può essere richiesto e concesso per svolgere attività che non rientrano tra i compiti istituzionali per assolvere incombenze amministrative e burocratiche senza allontanarsi dal luogo di lavoro (ad esempio per adempimenti nei confronti di pubbliche amministrazioni), purché contenuta nei tempi strettamente necessari allo svolgimento delle transazioni.

14. Protezione da virus

Le postazioni di lavoro sono protette da software antivirus aggiornato quotidianamente.


Ogni Utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico. Questa fattispecie può accadere mediante virus o malware, proveniente da dati e/o software importati/installati dall'Utente, che si auto-installano, all'insaputa dell'Utente, all'interno del PC, infettandolo e diffondendosi nella rete informatica aziendale.

Nel caso in cui il software antivirus rilevi e non disinfetti la presenza di un virus, l'Utente dovrà immediatamente sospendere ogni elaborazione in corso e segnalare l'accaduto al personale tecnico autorizzato dalla S.S. Servizi Informativi Aziendali.

Ogni dispositivo di memorizzazione esterna dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, dovrà essere prontamente consegnato al personale tecnico autorizzato che provvederà ad effettuare le dovute operazioni di disinfezione.

15. Salvataggio dati

Ogni Utente è responsabile della corretta conservazione dei dati e dei documenti elettronici che utilizza sul PC per motivi lavorativi, di qualsiasi tipo, formato e natura essi siano. Per questo motivo la tutela della gestione dei dati sulle postazioni di lavoro (Personal computer e PC portatili) è demandata all'Utente finale, che avrà l'obbligo di effettuare il salvataggio dei dati memorizzati sui computer in dotazione, con frequenza almeno settimanale e la conservazione degli stessi in luogo idoneo.

 ASL Foggia PugliaSalute	MODULO Regolamento ICT	<i>Rev. 1.0</i> <i>Pag. 19/22</i> Regolamento-ICT-ASLFG
--	---	---

Ove possibile, il Responsabile della S.S. Sistemi Informativi Aziendali metterà a disposizione degli Utenti che ne facessero richiesta, delle partizioni di disco su file server aziendali che l'Utente potrà utilizzare, in maniera esclusiva e riservata, per il salvataggio dei dati aziendali.

Costituisce buona regola la pulizia periodica (almeno ogni sei mesi) degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. È infatti assolutamente da evitare un'archiviazione ridondante.

16. Teleassistenza

Per lo svolgimento di normali attività di assistenza e manutenzione su personal computer connessi alla rete, il personale tecnico autorizzato dall'ASL FOGGIA potrà utilizzare specifici software di connessione remota. Tali programmi sono utilizzati per assistere l'Utente al fine di effettuare interventi di assistenza informatica e di manutenzione su applicativi e hardware in uso. L'attività di assistenza e manutenzione avviene previa autorizzazione da parte dell'Utente e mediante visualizzazione di un indicatore visivo sul monitor che segnala la connessione in remoto del tecnico informatico.


17. Monitoraggio

L'ASL FOGGIA, attraverso la S.S. Servizi Informativi Aziendali, effettuerà monitoraggi periodici su dati anonimi allo scopo di verificare l'attuazione del presente Regolamento, i possibili rischi alla sicurezza informatica e le possibili problematiche inerenti l'utilizzo degli strumenti informatici.


Questi monitoraggi si possono classificare in:

- analisi del traffico di rete: effettuati attraverso specifici log dei dispositivi di rete;
- analisi del traffico Internet: effettuati attraverso specifici log dei dispositivi di connessione ad Internet;
- inventario Hardware e Software: effettuati attraverso procedure prevalentemente automatiche per le apparecchiature collegate in rete e in maniera semiautomatica per le macchine non appartenenti al dominio.

Il monitoraggio delle risorse hardware e software non coinvolge in alcun modo i dati personali e i documenti presenti sulle singole postazioni di lavoro e viene effettuato per finalità organizzative e gestionali.

 ASL Foggia PugliaSalute	MODULO Regolamento ICT	<i>Rev. 1.0</i> <i>Pag. 20/22</i> Regolamento-ICT-ASLFG
--	---	---

I dati del traffico telematico verranno gestiti secondo le modalità e le tempistiche previste dalla normativa vigente in materia di sicurezza dei dati del traffico telefonico e telematico.

 <p>ASL Foggia PugliaSalute</p>	<p>MODULO Regolamento ICT</p>	<p><i>Rev. 1.0</i> <i>Pag. 21/22</i> Regolamento-ICT-ASLFG</p>
--	---	--

18. Controlli

L'ASL FOGGIA si riserva di effettuare controlli per verificare il rispetto del presente Regolamento.

Riguardo a tali controlli il presente Regolamento costituisce preventiva e completa informativa nei confronti dei dipendenti, in ossequio ai principi di cui all'art. 5 del Regolamento UE 2016/679.

Nel caso in cui emerga un evento dannoso, una situazione di pericolo o utilizzi non aderenti al presente Regolamento, che non siano stati impediti con preventivi accorgimenti tecnici o rilevati durante i monitoraggi o da attività di gestione degli strumenti informatici, la Direzione Generale, attraverso la **S.S. Servizi Informativi Aziendali**, potrà adottare le eventuali misure che consentano la verifica di tali comportamenti preferendo, per quanto possibile, un controllo preliminare su dati aggregati riferiti all'intera Struttura organizzativa o a sue articolazioni.

Il controllo su dati anonimi si concluderà con una comunicazione al Responsabile della Struttura analizzata che si preoccuperà di inviare un avviso generalizzato relativo a un utilizzo non corretto degli strumenti aziendali, invitando i destinatari ad attenersi scrupolosamente al presente Regolamento.

Qualora le anomalie e irregolarità dovessero persistere, si procederà circoscrivendo l'invito al personale afferente alla Struttura in cui è stata rilevata l'anomalia.


In caso di reiterate anomalie o irregolarità, saranno effettuati controlli su base individuale.

In nessun caso, a eccezione di specifica richiesta da parte dell'Autorità Giudiziaria, verranno poste in essere azioni sistematiche quali:

- la lettura e la registrazione dei messaggi di posta elettronica (al di là di quanto tecnicamente necessario per lo svolgimento del servizio di gestione e manutenzione della posta elettronica);
- la riproduzione ed eventuale memorizzazione delle pagine web visualizzate dal lavoratore;
- la memorizzazione di quanto visualizzato sul monitor.

Oltre a ciò, l'ASL FOGGIA si riserva di effettuare specifici controlli sui software caricati sui personal computer utilizzati dai dipendenti al fine di verificarne la regolarità sotto il profilo delle autorizzazioni e delle licenze, nonché, in generale, la conformità degli stessi alla normativa vigente e, in particolare, alle disposizioni in materia di proprietà intellettuale.

Oltre a tali controlli di carattere generale, l'ASL FOGGIA si riserva comunque le facoltà previste dalla normativa vigente di effettuare specifici controlli ad hoc nel caso di segnalazioni di attività che hanno causato danno, che ledono diritti di terzi o che, comunque, risultino illegittime.

 <p>ASL Foggia PugliaSalute</p>	<p align="center">MODULO Regolamento ICT</p>	<p><i>Rev. 1.0</i> <i>Pag. 22/22</i> Regolamento-ICT-ASLFG</p>
--	--	--

19.Sanzioni

È fatto obbligo a tutti i Dipendenti e Collaboratori dell'ASL FOGGIA di osservare le disposizioni portate a conoscenza con il presente Regolamento. Il mancato rispetto o la violazione delle regole sopra ricordate è perseguibile con provvedimenti disciplinari e/o risarcitori previsti dalla vigente normativa, nonché con tutte le azioni civili e penali consentite.

20.Aggiornamento e revisione

Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni motivate al presente documento. Le proposte saranno esaminate dai Responsabili Competenti ed inoltrate alla Direzione Generale.

Il presente Regolamento è soggetto a revisione come per Legge o qualora se ne ravveda la necessità.

Copia del presente documento verrà consegnata a ciascun dipendente aziendale ovvero messo a disposizione per ogni Utente autorizzato all'utilizzo della rete aziendale.

Con l'entrata in vigore del presente Regolamento, tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi sostituite dalle presenti.