Regione Puglia
OSPEDALI RIUNITI
Azienda Ospedaliero – Universitaria
FOGGIA

DELIBERAZIONE DEL DIRETTORE GENERALE

Nominato con Deliberazione della Giunta Regionale n. 805 del 17/4/2015

n. 64 del 11 FEB 2017

OGGETTO

Regolamento per l'utilizzo e la gestione della risorse strumentali informatiche e telematiche aziendali. Approvazione.

Struttura proponente	AFFARI GENERALI E TUTELA DELLA PRIVACY

Documenti integranti il provvedimento:

Descrizione Allegato	n. pag.
Regolamento interno ITC	19
Allegati	4

☑ **Dichiarazione di immediata esecutività**

Spese previste	
Conto Economico n.	
Descrizione conto economico	
Bilancio	
Dirigente	Dott.ssa Laura Silvestris

Destinatari dell'atto per conoscenza

☑ Direzione Amministrativa	☑ Direzione Sanitaria
☐ Struttura Controllo di Gestione	☐ Struttura Economico-Finanziaria
☑ Struttura Affari Generali e Tutela della Privacy	☐ Struttura Politiche del Personale
☐ Altro (specificare)	

La presente Deliberazione, tenuto conto delle fonti normative relative alla disciplina della privacy ovvero della tipologia degli atti allegati, è pubblicata con le seguenti modalità:

- ☐ solo frontespizio
- ☑ integrale
- ☐ solo deliberazione

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;
- il Garante della Privacy ha emanato la Deliberazione n. 13 del 1° marzo 2007 "Le linee guida del Garante per posta elettronica e internet"con la quale ha inteso prescrivere ai datori di lavoro alcune misure per conformare, alle disposizioni vigenti, il trattamento di dati personali effettuato per verificare il corretto utilizzo, nello svolgimento del rapporto di lavoro, della posta elettronica e della rete internet;
- la progressiva diffusione delle nuove tecnologie informatiche, le maggiori possibilità di interconnessione tra computer e l'aumento di informazioni trattate con strumenti elettronici aumentano infatti i rischi legati alla sicurezza e all'integrità delle informazioni oltre alle conseguenti responsabilità previste dalla normativa vigente in materia;
- l'Azienda 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;

Considerato che:

- l'Azienda Ospedaliero-Universitaria "Ospedali Riuniti" di Foggia intende adottare un Regolamento interno diretto ad evitare che comportamenti inconsapevoli possano innescare problemi di gestione della rete informatica aziendale e/o minacce alla sicurezza nel trattamento dei dati personali di qualsivoglia tipo (personale, sensibile e giudiziario);
- il Regolamento interno ITC intende richiamare, altresì, 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;

Rilevato che:

- la progressiva diffusione delle nuove tecnologie informatiche ed, in particolare, il libero accesso alla rete Internet dai Personal Computer, espone la Rete dell'Azienda 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 Azienda;
- si rende necessario, attraverso l'adottando Regolamento, prevedere specifiche prescrizioni che si aggiungono ed integrano alle specifiche istruzioni già fornite a tutti gli incaricati in attuazione del D. Lgs. 30 giugno 2003 n. 196 "Codice in materia di Protezione dei dati personali"e del Disciplinare tecnico (Allegato B al citato decreto legislativo) contenente le misure minime di sicurezza, nonché integrano le informazioni indicate nel precedente Regolamento in ordine alle ragioni ed alle modalità dei possibili controlli o alle conseguenze che possono scaturire sul piano personale in caso di violazione delle stesse;

- **Evidenziato che** l'Azienda deve provvedere a garantire un servizio continuativo volto ad 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;

Visti:

- il D. Lgs. 30 giugno 2003 n. 196 "Codice in materia di Protezione dei dati personali" ed il Disciplinare tecnico (Allegato B al citato decreto legislativo);
- la Deliberazione n. 13 del 1° marzo 2007 recante "Linee guida del Garante per posta elettronica e internet ";
- La Direttiva n.2/2009 del Ministro per la Pubblica Amministrazione e Innovazione;

Acquisito il parere favorevole del Direttore Amministrativo e del Direttore Sanitario, ciascuno per la parte di rispettiva competenza;

DELIBERA

Per le motivazioni innanzi premesse e considerate:

1. di approvare il Regolamento per l'utilizzo e la gestione della risorse strumentali informatiche e telematiche aziendali nell'allegato al presente provvedimento per formarne parte integrante e sostanziale;

2. di stabilire che copia dell'allegato Regolamento verrà trasmessa a ciascun dipendente dell'AOU di Foggia ovvero messo a disposizione per ogni Utente autorizzato all'utilizzo della rete aziendale;

3. di dare atto che, 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.

Il presente provvedimento, non essendo soggetto al controllo previsto dalla vigente normativa, è esecutivo ai sensi di legge.

Il Dirigente Proponente
dott.ssa Laura Silvestris

Il Direttore Sanitario
dott.ssa Laura Liliana Moffa

Il Direttore Amministrativo
dott. Michele Ametta

Il Direttore Generale
dott. Antonio Pedota

CERTIFICATO DI PUBBLICAZIONE

Il presente atto viene posto in pubblicazione in data odierna sull'Albo Pretorio informatico dell'Azienda Ospedaliero-Universitaria "Ospedali Riuniti" di Foggia.

Foggia, 11 FEB 2017

F.to IL FUNZIONARIO ADDETTO

Regione Puglia
OSPEDALI RIUNITI
Azienda Ospedaliero – Universitaria
FOGGIA

REGOLAMENTO

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

Anno 2017

MODULO Atto di nomina a Responsabile del Trattamento dei dati

Regolamento interno ITC

SOMMARIO

1. Premessa 3
2. Campo di applicazione 4
3. Utilizzo del personal computer 5
4. Hardware e Software 7
5. Utilizzo del Pc dedicato alla strumentazione 8
6. Computer portatili, tablet e smartphone 9
7. Stampanti e Fotocopiatori 9
8. Credenziali di accesso 10
9. Utilizzo della rete e accessi da remoto 11
10. Credenziali di accesso ai programmi gestionali 12
11. Supporti rimovibili 12
12. Posta elettronica 12
13. Navigazione internet 15
14. Protezione da virus 16
15. Salvataggio dati 16
16. Teleassistenza 17
17. Monitoraggio 17
18. Controlli 17
19. Sanzioni 18
20. Aggiornamento e revisione 19

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.
In tale contesto, il Garante ha emanato la Deliberazione n. 13 del 1° marzo 2007 "Linee guida del Garante per posta elettronica e internet"con la quale ha inteso prescrivere ai datori di lavoro alcune misure per conformare alle disposizioni vigenti il trattamento di dati personali effettuato per verificare il corretto utilizzo, nello svolgimento del rapporto di lavoro, della posta elettronica e della rete internet. La progressiva diffusione delle nuove tecnologie informatiche, le maggiori possibilità di interconnessione tra computer e l'aumento di informazioni trattate con strumenti elettronici aumentano infatti i rischi legati alla sicurezza e all'integrità delle informazioni oltre alle conseguenti responsabilità previste dalla normativa vigente in materia.
L'Azienda Ospedaliero-Universitaria "Ospedali Riuniti" di Foggia (d'ora in avanti Azienda) con il presente atto intende adottare un Regolamento interno diretto ad evitare che comportamenti inconsapevoli possano innescare problemi di 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'Azienda 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 Azienda. Pertanto, le prescrizioni di seguito previste, si aggiungono ed integrano le specifiche istruzioni già fornite a tutti gli incaricati in attuazione del D. Lgs. 30 giugno 2003 n. 196 e del Disciplinare tecnico (Allegato B al citato decreto legislativo) contenente le misure minime di sicurezza, nonché integrano le informazioni indicate nel precedente Regolamento in ordine alle ragioni ed alle modalità dei possibili controlli o alle conseguenze che possono scaturire sul piano personale in caso di violazione delle stesse.
L'Azienda deve provvedere a 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'Azienda, 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.

2. Campo di applicazione

Il presente Regolamento **si applica a tutti i dipendenti, senza distinzione di ruolo o livello, nonché a tutti i collaboratori di questa Azienda** a prescindere dal rapporto contrattuale con lo stesso intrattenuto (consulenti, tirocinanti, borsisti, volontari, ditte esterne autorizzate, ecc.). Inoltre, il presente Regolamento disciplina l'utilizzo di tutti i dispositivi collegati alla rete aziendale e quindi direttamente gestibili e controllabili a norma di legge, attraverso gli opportuni strumenti, dal personale dell'Ufficio S.I.A..
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 "Incaricato del trattamento" ai sensi dell'art. 30 del D. Lgs. n. 196/03 (Disciplina in materia di protezione dei dati personali). Il presente Regolamento contiene le disposizioni relative alle corrette modalità di utilizzo della rete informatica e di tutte le risorse aziendali, in conformità e nel rispetto di quanto previsto dalla specifica normativa di settore e dalle ulteriori disposizioni emanate dall'Azienda.
Gli strumenti informatici oggetto del presente Regolamento sono di proprietà dell'Azienda 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 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;
- 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 rete;
- amministratori di base di dati;
- amministratori di apparati di sicurezza;
- amministratori di applicazioni.

Tutti i collaboratori della P.O. dell'Ufficio S.I.A. sono nominati formalmente in qualità di Amministratori di Sistema, per ambito di competenza ed operatività.

Nel caso di servizi di amministrazione di sistema affidati in outsourcing, quale Responsabile esterno del trattamento, 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'Azienda è tenuta 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'Azienda rende noto che il personale della P.O. dell'Ufficio S.I.A. (Servizio Informativo Aziendale), in qualità di Amministratore di Sistema, individuato e nominato secondo quanto previsto dal paragrafo 2, 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 di posta elettronica, nonché alla verifica sui siti internet acceduti dagli utenti abilitati. La stessa facoltà, sempre ai fini della sicurezza del sistema e per garantire la normale operatività dell'Azienda, si applica anche in caso di assenza prolungata od impedimento del dipendente.

Il personale della P.O. dell'Ufficio S.I.A. 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 e malware 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 richieste al Responsabile della P.O. dell'Ufficio S.I.A. che provvederà ad effettuarle. L'utente non può modificare le impostazioni del PC autonomamente.

Di conseguenza:
⇒ non verranno 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 P.O. dell'Ufficio S.I.A.;
⇒ 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 spegnere o "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, AudioGalaxy o software di monitoraggio della rete in genere);
⇒ non è consentito configurare o utilizzare servizi diversi da quelli messi a disposizione da parte dell'Azienda (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 smontare il computer e/o asportare qualsiasi apparecchiatura in dotazione all'Utente;
⇒ non è consentito avviare il personal computer con sistemi operativi diversi da quello installato dal personale tecnico specializzato per conto dell'Azienda;
⇒ 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 P.O. dell'Ufficio S.I.A.;
⇒ salvo preventiva espressa formale autorizzazione del Responsabile della P.O. dell'Ufficio S.I.A., non è consentito l'uso di programmi diversi da quelli ufficialmente installati dal personale tecnico per conto dell'Azienda, 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'Azienda 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 aziendale Personal Computer o Pc Portatili e, più in generale, qualsiasi dispositivo hardware senza la formale autorizzazione del Responsabile della P.O. dell'Ufficio S.I.A.

4. Hardware e Software

Tutto l'hardware ed il software potrà essere acquistato solo previa richiesta di parere tecnico favorevole da parte della P.O. dell'Ufficio S.I.A., che 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 di acquisto dell'hardware e del software dovranno essere indirizzate al Responsabile della P.O. dell'Ufficio S.I.A. 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 conservati presso la P.O. dell'Ufficio S.I.A., così da consentire le operazioni di verifica della disponibilità di licenze e l'eventuale nuova installazione delle procedure.

Il personale non può utilizzare eventuale software di proprietà personale. Tutto ciò comprende anche le applicazioni regolarmente acquistate e registrate, programmi shareware e/o freeware, eventuale software scaricato da Internet o proveniente da CD/DVD allegati a riviste e/o giornali o altro software posseduto a qualsiasi titolo. Qualora fosse necessario per fini strettamente collegati

all'attività lavorativa, l'utilizzo di software di proprietà personale, potrà essere installato solo previa richiesta di parere tecnico favorevole da parte del Responsabile della P.O. dell'Ufficio S.I.A., che controllerà la compatibilità con le misure di sicurezza informatica aziendali.

Nell'ipotesi di utilizzo di software realizzato direttamente dall'utente finale potrà essere installato solo previa richiesta di parere tecnico favorevole da parte del Responsabile della P.O. dell'Ufficio S.I.A., che controllerà la compatibilità con le misure di sicurezza informatica aziendali e qualora vengano trattati dati sensibili, darne comunicazione anche alla Struttura Dipartimentale Affari Generali e Tutela della Privacy.

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. (D. Lgs. n. 518/92 sulla tutela giuridica del software e L. 248/2000 "Nuove norme di tutela del diritto d'autore").
E' 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 P.O. dell'Ufficio S.I.A.

5. Utilizzo del PC dedicato alla strumentazione

Il collegamento alla rete aziendale di computer dedicati alla strumentazione deve essere richiesto e concordato con il Responsabile della P.O. dell'Ufficio S.I.A. 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 unitamente al personale della P.O. dell'Ufficio S.I.A. 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 del Responsabile della P.O. dell' Ufficio S.I.A. Al fine di poter permettere l'utilizzo condiviso di una singola risorsa da parte di più Utenti è consentita la creazione e l'uso di utenze di gruppo, la cui responsabilità e assegnazione è del Responsabile della Struttura. Le utenze di gruppo non possono essere utilizzate per il trattamento di dati personali in formato digitale.

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 dalla P.O. dell'Ufficio S.I.A.;
⇒ 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 della P.O. dell'Ufficio S.I.A. 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 la P.O. dell'Ufficio S.I.A., in collaborazione con la ditta esterna incaricata della manutenzione, valuterà l'investimento tecnologico necessario per rendere il computer idoneo all'esecuzione del backup dei dati.

6. Computer portatili, tablet e smartphone

L'Utente è responsabile dell'integrità dei computer portatili, tablet e smartphone affidati dall'Azienda e dei dati ivi contenuti. L'Utente è tenuto a custodirlo 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 resi noti al Responsabile della P.O. dell'Ufficio S.I.A che provvederà all'applicazione di tutte le misure di sicurezza previste da disciplinare interno e dalla normativa vigente.

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. 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.

8. Credenziali di accesso

I sistemi di controllo degli accessi 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'Azienda 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 dal personale della P.O. dell'Ufficio S.I.A. 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 considerata la necessità di questa Azienda di garantire in ogni caso la continuità dei servizi istituzionali.

Le credenziali di autenticazione per l'accesso alla rete e per l'utilizzo del servizio di posta elettronica istituzionale (@ospedaliriunitifoggia.it) vengono assegnate dal personale della P.O. dell'Ufficio S.I.A., previa formale richiesta da effettuarsi attraverso la compilazione dell'apposito modulo "mod-utenze-rete-email" sottoscritta dal Dirigente della Struttura presso la quale l'Utente dovrà operare.
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 della struttura con la quale il collaboratore si coordina nell'espletamento del proprio incarico). Sarà cura del Dirigente dare tempestiva comunicazione al Responsabile della P.O. dell'Ufficio S.I.A, previa compilazione di apposito modulo "mod-utenze-rete-email", nell'eventualità che il collaboratore cessi o abbia cessato il rapporto con l'Azienda 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 della P.O. dell'Ufficio S.I.A. 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.

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 P.O. dell'Ufficio S.I.A., 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 P.O. dell'Ufficio S.I.A. La responsabilità del salvataggio dei dati ivi contenuti è pertanto a carico del singolo Utente.
Il personale tecnico della P.O. dell'Ufficio S.I.A. 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 Responsabile della P.O. dell'Ufficio S.I.A. 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 P.O. dell'Ufficio S.I.A. , quali, a titolo esemplificativo: modem, router, Internet key.
I tecnici delle ditte esterne (fornitori applicativi, sistemisti etc.) dovranno richiedere l'autorizzazione del Responsabile della P.O. dell'Ufficio S.I.A. prima di collegarsi fisicamente alla rete aziendale con dispositivi personali. Quest'ultimi saranno sottoposti alle politiche di sicurezza di questa Azienda al fine di garantire la sicurezza generale della rete informatica.
Gli accessi da remoto verso la rete aziendale potranno essere effettuati solo previa autorizzazione Responsabile della P.O. dell'Ufficio S.I.A. che rilascerà apposite credenziali per l'autenticazione sicura. Tutti gli accessi saranno monitorati e registrati. Non sono ammessi accessi di tipologia differente da quella VPN (Ipsec o SSL) definita dal Responsabile della P.O. dell'Ufficio S.I.A.

10. Credenziali di accesso ai programmi gestionali

E' possibile ottenere l'assegnazione di specifiche credenziali di autenticazione a programmi gestionali specifici, attraverso la compilazione dell'apposito modulo "mod-utenze-gestionali" sottoscritta dal Dirigente della Struttura presso la quale l'Utente dovrà operare.
Il sopraindicato modulo dovrà essere compilato a cura del Dirigente della Struttura anche in caso di trasferimento del dipendente ad altra struttura o eventuale cessazione del rapporto di lavoro con l'Azienda per la conseguente comunicazione di disattivazione dei profili di accesso.

11. Supporti rimovibili

Eventuali supporti magnetici contenenti dati sensibili devono essere adeguatamente custoditi dall'Utente in armadi o cassetti chiudibili a chiave. E' 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.

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 con dominio @ospedaliriunitifoggia.it è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica istituzionale sono responsabili del corretto utilizzo delle stesse.

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;
⇒ 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'Azienda 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;
- ⇒ limitare l'invio di messaggi di posta elettronica a indirizzi plurimi (decine di destinatari) e trasmetterli solo in casi motivati da esigenze di servizio.

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 dell'Azienda 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 P.O. dell'Ufficio S.I.A.
di accedere alla postazione e/o alla casella di posta elettronica istituzionale del dipendente assente mediante apposito modulo (mod-password-urgenza) in cui si evinca la richiesta.
Sarà onere del Responsabile della Struttura informare celermente il dipendente al suo rientro, fornendo adeguata spiegazione e redigendo apposito verbale.

Le caselle di posta elettronica istituzionale nominative hanno validità pari alla durata della permanenza in servizio del dipendente, fatte salve eventuali situazioni di congedo, distacco e comando. Nel caso il cui il dipendente non presti più la sua attività lavorativa presso questa Azienda, 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 l'interessato provvederà ad inserire inserita una risposta automatica d'ufficio.

13. Navigazione internet

Il Personal computer 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, all'interno dell'Azienda.
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 dalla P.O. dell'Ufficio S.I.A.;
- ⇒ 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'Azienda 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 della P.O. dell'Ufficio S.I.A., 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 cancellati periodicamente ed automaticamente, non è sistematico e le informazioni vengono conservate temporaneamente per finalità di sicurezza di questa Azienda. 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

14. Protezione da virus

Le postazioni di lavoro collegate alla rete informatica aziendale sono protette da uno stesso software antivirus (attualmente Eset Nod 32) che viene aggiornato automaticamente grazie ad una gestione centralizzata per mezzo di un server dedicato. Non e ammesso l'utilizzo di sistemi antivirus diversi.

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 della P.O. dell'Ufficio S.I.A.
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.

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. E' 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 della P.O. dell' Ufficio S.I.A. 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

La Direzione Generale, attraverso il Responsabile della P.O. dell'Ufficio S.I.A., 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.
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.

18. Controlli

L'Azienda 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 base al principio di correttezza (richiamato all'art. 5), l'eventuale trattamento deve essere ispirato ad un canone di trasparenza, come prevede anche la disciplina di settore.
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 il Responsabile della P.O. dell'Ufficio S.I.A., 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 Dirigente 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'Azienda 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, questa Azienda 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 all'Azienda, che ledono diritti di terzi o che, comunque, sono illegittime.

19. Sanzioni

È fatto obbligo a tutti i dipendenti ed utenti del sistema informativo/informatico dell'Azienda 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

Il presente Regolamento è stato redatto tenendo conto sia delle Linee guida del Garante della Privacy emanate con delibera n. 13 del 1° marzo 2007 che della direttiva n.2/2009 del Ministro per la Pubblica Amministrazione e Innovazione. Tutti gli utenti possono proporre, qualora ritenuto necessario, tramite inoltro al Dirigente della Struttura Dipartimentale Affari Generali e Tutela della Privacy, integrazioni motivate al presente documento.
Il presente Regolamento è soggetto a revisione come per Legge o qualora se ne ravveda la necessità.
Copia del presente documento verrà trasmessa a ciascun dipendente dell'AOU di Foggia ovvero messa 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.

Allegati:

1. Richiesta credenziali di accesso a programma gestionale;
2. Richiesta credenziali di accesso rete/e-mail;
3. Richiesta credenziali di accesso per casi d'urgenza;
4. Modulo richiesta VPN imprese esterne.

Allegato 1

RICHIESTA CREDENZIALI DI ACCESSO A PROGRAMMA GESTIONALE

Prot. n._____ Foggia, lì_____

Alla c.a. Responsabile della P.O. dell'Ufficio S.I.A.
Azienda Ospedaliero-Universitaria di Foggia

Struttura/Servizio richiedente: _____

Dirigente: _____

Si richiede, a far data dal_____, la

ATTIVAZIONE

DISATTIVAZIONE

delle seguenti utenze nominative per l'accesso al programma gestionale_____.

Nome	Cognome	Codice Fiscale	Data di scadenza utilizzo credenziali
La password temporanea e relative istruzioni verranno inviate via mail o con modalità differenti da concordare con il Responsabile della P.O. dell'Ufficio S.I.A.			

Si richiede, inoltre l'attivazione di:

_____.

Il Dirigente

_____

(timbro e firma)

Allegato 2

RICHIESTA CREDENZIALI DI ACCESSO RETE/E-MAIL

Prot. n._____ Foggia, lì_____

Alla c.a. Responsabile P.O. dell'Ufficio S.I.A.
Azienda Ospedaliero-Universitaria di Foggia

Struttura/Servizio richiedente: _____

Dirigente: _____

Si richiede, a far data dal_____, la

ATTIVAZIONE

DISATTIVAZIONE

delle seguenti utenze nominative per il personale autorizzato a compiere attività istituzionale presso questa Struttura/Servizio _____.

Nome	Cognome	Codice Fiscale	User ID	E.mail	Data scadenza

Si richiede inoltre l'attivazione dei profili di accesso alle banche dati come di seguito specificato:

Descrizione Banca dati	Path accesso in rete	Tipo privilegio (r,w,fc) R=lettura, W=scrittura, FC= pieno controllo
Area Contabilità	\\contabilità-srv\base	FC

Si richiede inoltre l'attivazione dei profili di accesso alle banche dati come di seguito specificato:

_____

Il Dirigente

_____

(timbro e firma)

Allegato 3

RICHIESTA CREDENZIALI DI ACCESSO PER CASI D'URGENZA

Prot. n._____ Foggia, lì_____

Alla c.a. Responsabile della P.O. Ufficio S.I.A.
Azienda Ospedaliero-Universitaria di Foggia

Struttura/Servizio richiedente: _____
Dirigente: _____
Richiedente:_____
Si richiede, a far data dal_____, la

ATTIVAZIONE
DISATTIVAZIONE

sul PC assegnato a _____
alla e.mail assegnata a _____
MOTIVAZIONE_____

Si richiede, inoltre l'attivazione di:

_____

La password temporanea e relative istruzioni verranno inviate via mail o con modalità differenti da concordare con il Responsabile della P.O. Ufficio S.I.A.

Il Dirigente

_____
(timbro e firma)

Allegato 4

MODULO RICHIESTA* ☐ **ATTIVAZIONE VPN** ☐ **DISATTIVAZIONE VPN**

Ditta esterna/Struttura/Servizio di appartenenza:_____

Richiedente:_____

Riferimento telefonico: _____

Funzione/Ruolo:_____

e-mail:_____

Si segnala che all'indirizzo indicato verrà inviata una email con le istruzioni e le credenziali necessarie alla connessione

*__Istruzioni per la compilazione:__
Il fornitore, dopo avere compilato completamente la Sezione1, sottoscritto il documento, potrà inviarlo alla P.O. SIA via fax al n. 0881/732296 oppure via pec all'indirizzo protocollo.ospriunitifg@pec.rupar.puglia.it e all'indirizzo e-mail g.piccolo@ospedaliriunitifoggia.it. Alla richiesta dovrà essere allegata copia di un documento d'identità in corso di validità del richiedente.

Sezione 1: da compilare a carico della ditta richiedente

1. **Tipologia della VPN:**
   a. Site to site
   b. VPN Client

2. **Obiettivi della VPN:**
   a. Manutenzione applicativa Applicazione: _____
   b. Manutenzione sistemistica Sistema: _____
   c. Telelavoro

3. **Parametri della VPN da attivare / disattivare:**
   a. Indirizzo IP, porte (e protocollo) delle postazioni da raggiungere tramite VPN:
      1. IP: . . . PORTA:_____
      2. IP: . . . PORTA: _____
      3. IP: . . . PORTA: _____
      4. IP: . . . PORTA: _____
      5. IP: . . . PORTA: _____
      6. IP: . . . PORTA: _____
   b. Indirizzo IP del remote peer (nel caso di attivazione / disattivazione di VPN site to site):
      1. IP: . . .
   c. Indirizzo IP delle reti remote a cui appartengono le postazioni da cui sarà avviata / rimossa la VPN (nel caso in cui l'accesso debba essere aperto da qualsiasi postazione indicare Network 0.0.0.0 Subnet 0.0.0.0):
      1. Network:. . . Subnet: . . . .
      2. Network:. . . Subnet: . . . .
      3. Network:. . . Subnet: . . . .
      4. Network:. . . Subnet: . . . .

4. **Riferimento fornitore per la gestione delle password della VPN**

Nome_____

Cognome_____

Telefono_____

e-mail_____

5. **Periodo attivazione VPN:** dal_____ al _____

Il Richiedente, identificato con i dati di cui sopra, avendo fatto richiesta di connessione VPN, dichiara sotto la propria responsabilità:

- di essere a conoscenza della natura della connessione;
- di essere a conoscenza di essere connesso alla rete dati dell'Azienda Ospedali Riuniti di Foggia e quindi di operare secondo le sue Policy e Regolamenti;
- di assumersi le responsabilità che derivano dalla connessione in oggetto;
- di comunicare eventuali variazioni alle informazioni di cui sopra all'indirizzo e.mail_____.

Foggia, lì_____ Il Richiedente_____

Sezione 2: Autorizzazione, da compilare a cura della P.O. SIA

Il Funzionario Responsabile della P.O. SIA in relazione alla richiesta di cui innanzi, esprime il seguente parere:

□ FAVOREVOLE
□ NON FAVOREVOLE, per i seguenti motivi: _____
_____.

Foggia, lì_____

Il Responsabile P.O. S.I.A.

_____