AZIENDA OSPEDALIERA "SAN PIO" – BENEVENTO
OSPEDALE RILIEVO NAZIONALE (DPCM 23.4.93)
D.E.A. DI II LIVELLO (L.R. 11.1.94 n°2)
Via dell'Angelo, 1 – Tel. 0824 57111

Regolamento per l'utilizzo degli strumenti elettronici, della posta elettronica e della rete Internet in ambito lavorativo

INDICE

1 PREMESSA 4

2 PRINCIPI GENERALI 4

3 ENTRATA IN VIGORE E PUBBLICITÀ 4

4 AMBITO DI APPLICAZIONE 4

4.1. Ambito Soggettivo: Destinatari del Regolamento 4

4.2. Ambito Oggettivo 5

5 UTILIZZO E PROTEZIONE DEGLI STRUMENTI INFORMATICI DI LAVORO 5

5.1 DISTRUZIONE DEI SUPPORTI 6

5.2 PERSONAL COMPUTER 6

5.3 *DISPOSITIVI MOBILI* *7*

5.4 DISPOSITIVI DI MEMORIZZAZIONE RIMOVIBILI 8

6 GESTIONE ED ASSEGNAZIONE DELLE CREDENZIALI DI AUTENTICAZIONE 9

7 BACKUP 10

8 UTILIZZO DELLA RETE DELL' AO SAN PIO 10

9 UTILIZZO DELLA POSTA ELETTRONICA 10

9.1 E-MAIL DI MASSA/E-MAIL BATCH 11

9.2 SICUREZZA DELLE E-MAIL 11

9.3 ASSENZE PROGRAMMATE E IMPROVVISE 11

9.4 UTILIZZO DELLA POSTA ELETTRONICA PER USO PERSONALE 12

10 NAVIGAZIONE IN INTERNET 12

11 ACCESSO REMOTO / SMART WORKING 13

12 RIEPILOGO DELLE DISPOSIZIONI SUL CORRETTO UTILIZZO DEGLI STRUMENTI 13

13 PROTEZIONE DA VIRUS E MALWARE 15
14 ACCESSO AI DATI TRATTATI DALL'UTENTE 15
14.1 REGISTRAZIONE DI ATTIVITÀ SU INTERNET 16
15 CONTROLLI GRADUALI 17
16 SANZIONI 17
17 AGGIORNAMENTO E REVISIONE 17

1 PREMESSA

Consapevole dell'importanza che ha un corretto trattamento dei dati personali di tutti i soggetti che, per qualsiasi ragione, entrano in contatto con la propria struttura, la AO SAN PIO di Benevento (di seguito "**AO SAN PIO**") dedica particolare attenzione al rispetto dei principi contenuti nel Regolamento Europeo 2016/679 in materia di protezione dei dati ("**GDPR"**) nonché nei provvedimenti emanati dall'Autorità Garante per la Protezione dei Dati Personali, applicabili alla propria attività.

In tale ottica, questa AO SAN PIO ritiene opportuno adottare il presente "*Regolamento per l'utilizzo dei dispositivi elettronici, della posta elettronica e della rete Internet in ambito lavorativo*" (di seguito il "**Regolamento**"), che integra le istruzioni tempo per tempo fornite a tutte le persone autorizzate al trattamento dati personali ai sensi degli art. 29 GDPR e 2-*quaterdecies* D.Lgs. 196/2003 come modificato dal D.Lgs. 101/2018 ("**Codice**").

2 PRINCIPI GENERALI

La diffusione delle tecnologie informatiche e, in particolare, della posta elettronica e degli accessi alla rete Internet tramite strumenti elettronici (personal computer, *device* mobili) richiede di armonizzarne l'utilizzo con il rispetto delle regole in tema di protezione dei dati personali, nonché in tema di riservatezza, di sicurezza e di tutela del patrimonio e dell'immagine aziendale. Il tutto bilanciando adeguatamente i diritti e gli interessi dell'Azienda e quelli dei lavoratori (dipendenti e/o altri collaboratori).

Si evidenzia peraltro, a tale riguardo, che **l'utilizzo delle risorse informatiche messe a disposizione dall'Azienda deve sempre ispirarsi ai principi di diligenza, correttezza e buona fede** che normalmente caratterizzano i rapporti di lavoro, tenendo in debito conto che i mezzi informatici sono strumenti di lavoro e vengono posti nella disponibilità del personale esclusivamente per finalità connesse allo svolgimento della prestazione lavorativa.

Pertanto, l'AO SAN PIO ha adottato il presente Regolamento interno per disciplinare, con criteri di trasparenza, l'utilizzo degli strumenti elettronici, della posta elettronica e della rete Internet, in conformità anche alle Linee Guida adottate dall'Autorità Garante per la protezione dei dati personali ("**Garante**") con delibera n. 13 del 1° marzo 2007.

L'omessa osservanza delle misure previste dal presente Regolamento può esporre i destinatari – ove ne ricorrano i presupposti contrattuali e di legge – a provvedimenti disciplinari ai sensi dell'art. 7 della L. n. 300/1970.

3 ENTRATA IN VIGORE E PUBBLICITÀ

Il Regolamento entra in vigore all'atto della sua diffusione al personale.

4 AMBITO DI APPLICAZIONE

4.1. Ambito Soggettivo: Destinatari del Regolamento

Il presente Regolamento si applica agli "**Utenti**", per i quali devono intendersi tutti i lavoratori dipendenti – senza distinzione di funzione, inquadramento e/o livello – nonché tutti i collaboratori dell'Azienda, sia che lavorino *in loco* sia tramite accesso remoto (anche nel caso di *smart working* / lavoro agile) e a prescindere dal rapporto contrattuale con la stessa intrattenuto (lavoratori somministrati, collaboratori a progetto, consulenti, *stagiaire*, tirocinanti, volontari, ecc.), che siano in possesso di specifiche credenziali di autenticazione personalizzate (di seguito "**Credenziali**") per l'accesso alla rete informatica dell'AO SAN PIO e/o di strumenti informatici aziendali per l'esercizio della loro prestazione lavorativa.

Trattandosi di mere istruzioni comportamentali/*best practices* di ordine generale, l'applicazione delle seguenti disposizioni non fonda alcun rapporto di subordinazione con i soggetti non dipendenti dall'Azienda che devono osservarle.

L'accesso alla rete aziendale e, più in genere, al trattamento informatizzato di dati di cui sia titolare la AO SAN PIO di Benevento non è consentito se non tramite l'utilizzo delle Credenziali o di altre modalità tempo per tempo adottate dall'Azienda.

4.2. Ambito Oggettivo

Il presente Regolamento si applica all'accesso e all'utilizzo di tutti i dati e Sistemi Informativi di AO SAN PIO, indipendentemente dal fatto che siano ospitati internamente o esternamente (es. "*Cloud*" o "*Software as a Service*") e/o accessibili tramite dispositivi aziendali oppure dispositivi personali dell'Utente (di seguito "**Dispositivi**"), quali a titolo esemplificativo:

- telefoni cellulari / smartphone, tablet, laptop, PC, server;
- sistemi di telefonia fissa, fax, stampa, scansione, fotocopiatura;
- siti web, intranet aziendale, archiviazione di file, applicazioni, servizi di posta elettronica, servizi esterni basati sul Web;
- altri Sistemi Informativi, servizi Wi-Fi e Internet (es. Social Media, Sito);
- database, documenti, materiali stampati, supporti rimovibili.

5 UTILIZZO E PROTEZIONE DEGLI STRUMENTI INFORMATICI DI LAVORO

I Dispositivi assegnati all'Utente sono strumenti di lavoro e devono essere utilizzati per scopi legittimi legati allo svolgimento dell'attività lavorativa.

L'utilizzo personale dei Dispositivi aziendali è consentito solo se strettamente marginale e in conformità con questo Regolamento e con le eventuali altre *policy* e istruzioni fornite dalla Azienda, a condizione che questo non comporti la violazione della riservatezza, della sicurezza e della privacy dei dati trattati.

L'AO SAN PIO si riserva il diritto di limitare o impedire, anche temporaneamente, l'uso dei Dispositivi aziendali, in qualsiasi momento e senza alcun preavviso, laddove ritenga che il loro utilizzo da parte dell'Utente risulti eccessivo o inappropriato o contrario a legge.

I Dispositivi aziendali devono essere custoditi con cura dall'Utente evitando ogni possibile forma di danneggiamento, accesso non autorizzato, utilizzo difforme dalle regole aziendali e dalla normativa vigente.

L'AO SAN PIO detiene la sola ed esclusiva titolarità di tutti i Sistemi Informativi, delle caselle di posta elettronica aziendale, dei Dispositivi aziendali e delle apparecchiature aziendali concessi in uso agli Utenti. Se richiesto - anche per aggiornamenti di routine, sicurezza ed altre relative verifiche - gli Utenti devono tempestivamente mettere a disposizione delle competenti strutture aziendali i Dispositivi in loro possesso o sotto il loro controllo.

Del pari, gli Utenti sono tenuti a restituire all'U.O.C. TECNICA E PROGRAMMAZIONE - CED tutti i Dispositivi aziendali in loro possesso prima di lasciare l'impiego presso l'Azienda, anche per scadenza del contratto; in tale circostanza, è proibito agli Utenti effettuare, senza l'autorizzazione scritta della AO SAN PIO, copie dei dati e/o della documentazione, che non potrà conseguentemente essere trattenuta e fatta oggetto di trattamento oltre il termine del rapporto di lavoro/collaborazione.

Nelle ipotesi di riutilizzo o dismissione dei Dispositivi aziendali e altre apparecchiature aziendali, la U.O.C. TECNICA E PROGRAMMAZIONE - CED procede nel rispetto dei seguenti principi:

1) in caso di reimpiego, riciclo o invio in manutenzione dei dischi magnetici o di parte di essi, del sistema centrale e degli hard disk dei server che contengano dati personali, cancellando preventivamente i dati in essi contenuti, mediante l'adozione delle seguenti tecniche:

- cancellazione sicura delle informazioni, ottenibile con programmi informatici (quali *wiping program* o *file shredder o altri*);
- formattazione a basso livello o altre tecniche (in caso di dischi rigidi, chiavette USB, *floppy disk*, nastri magnetici su bobine aperte o in cassette);

- qualora valutato necessario dalla U.O.C. TECNICA E PROGRAMMAZIONE - CED , demagnetizzazione dei dispositivi di memoria basati su supporti magnetici o magneto-ottici, da eseguire tramite apposite Azienda terze, sotto la supervisione della stessa U.O.C. TECNICA E PROGRAMMAZIONE – CED oppure attraverso l'utilizzo di altre tecniche ;

2) in caso di smaltimento di rifiuti elettrici ed elettronici, cancellando i dati personali dai supporti contenuti nelle apparecchiature mediante procedure che comportano la distruzione dei supporti di memorizzazione di tipo ottico o magneto-ottico, in modo da garantirne l'effettività e da impedire l'acquisizione indebita di dati personali.

5.1 Distruzione dei Supporti

La distruzione dei supporti deve essere effettuata, anche in ossequio a quanto prescritto nel provvedimento "*Rifiuti di apparecchiature elettriche ed elettroniche (Raae) e misure di sicurezza dei dati personali*" del 13 ottobre 2008 del Garante, e comunque con procedure o strumenti differenziati a seconda del loro tipo, quali:

- sistemi di punzonatura o deformazione meccanica;
- distruzione fisica o disintegrazione (per i supporti ottici come cd rom e dvd);
- demagnetizzazione ad alta intensità.

Per lo svolgimento di tali attività, l'AO SAN PIO, per mezzo della U.O.C. TECNICA E PROGRAMMAZIONE - CED, potrà coinvolgere società terze che, tramite la dovuta strumentazione, avranno il compito di eseguire la distruzione dei supporti; in tal caso la U.O.C. TECNICA E PROGRAMMAZIONE - CED provvederà a supervisionare l'intero processo, avendo cura di accertarsi che sia stato eseguito nel pieno rispetto delle normative vigenti.
La U.O.C. TECNICA E PROGRAMMAZIONE – CED potrà inoltre avvalersi delle professionalità interne qualora opportunamente formate.

5.2 Personal Computer

Nel presente paragrafo si dettagliano le istruzioni operative relative all'utilizzo dei personal computer, intendendosi per tali sia i Dispositivi fissi che mobili (es. laptop, notebook).

Il personal computer assegnato in uso al singolo Utente permette l'accesso alla rete di AO SAN PIO solo attraverso specifiche credenziali di autenticazione. Agli Utenti assegnatari di personal computer è consentito esclusivamente l'utilizzo dei programmi ufficialmente installati dalla U.O.C. TECNICA E PROGRAMMAZIONE - CED .

È conseguentemente vietato agli Utenti installare o eseguire autonomamente altri programmi, sussistendo – tra l'altro – il grave pericolo di introdurre virus informatici nel sistema IT aziendale e/o di alterare la funzionalità delle applicazioni software esistenti. L'inosservanza di tale divieto espone la stessa AO SAN PIO a gravi danni e responsabilità civili; si evidenzia inoltre che le eventuali violazioni della normativa a tutela dei diritti d'autore sul software – la quale impone la presenza nel sistema di software regolarmente licenziato, o comunque libero ("*open source*") e quindi non protetto dal diritto d'autore – sono sanzionate anche penalmente.

Salva la preventiva autorizzazione espressa di questa AO SAN PIO, è vietato all'Utente modificare le caratteristiche impostate sul personal computer ricevuto in uso nonché installare dispositivi di memorizzazione, comunicazione o altro (a titolo esemplificativo e non esaustivo, masterizzatori, modem, sistemi wi-fi o *connect card*). Allo stesso modo è fatto divieto di collegare alla rete aziendale qualsiasi ulteriore apparecchiatura non aziendale come, a titolo esemplificativo e non esaustivo, Pc switch, *hub*, apparati di memorizzazione di rete. È assolutamente proibito, in particolare, effettuare collegamenti verso l'esterno di qualsiasi tipo (tramite modem, c*onnect card* ecc.) utilizzando un personal computer che sia contemporaneamente collegato alla rete aziendale.

Ogni Utente deve prestare la massima attenzione ai supporti di origine esterna (per es. chiavi USB, dischi esterni ecc.), il cui utilizzo dovrà essere espressamente autorizzato dalla U.O.C. TECNICA E PROGRAMMAZIONE – CED. Nel caso in cui siano rilevati virus occorre adottare quanto previsto dal presente Regolamento in ordine alle procedure di protezione antivirus e darne comunicazione ad horas alla U.O.C. TECNICA E PROGRAMMAZIONE – CED.

È fatto obbligo agli Utenti di non lasciare incustodito ed accessibile il personal computer assegnato in uso. Quest'ultimo deve essere spento o bloccato con password, a cura dell'Utente, al termine dell'orario di lavoro o della prestazione giornaliera, ovvero in caso di assenza prolungata dalla postazione, e comunque

prima di lasciare la sede di lavoro. In ogni caso, 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. Al fine di evitare tali evenienze occorre procedere come segue:

- al termine dell'attività o in caso di temporaneo abbandono della postazione l'Utente deve effettuare il "*log-off*" della stazione di lavoro o dalla specifica applicazione utilizzata, impedendone così l'utilizzo improprio;
- in caso di abbandono temporaneo della postazione di lavoro, l'Utente ha l'obbligo di bloccare l'utilizzo del PC prima di allontanarsi dallo stesso, anche digitando contemporaneamente i tasti CTRL+ALT+CANC e in seguito il tasto "invio", oppure premendo (il tasto Windows) ⊞+L.

In generale, si rammenta che gli Utenti sono responsabili di ogni attività svolta tramite le proprie Credenziali (es. navigazione sul web, accesso a file, e-mail inviate e altre attività pertinenti i Sistemi Informativi aziendali) il cui utilizzo non deve essere concesso ad altri.

In aggiunta a quanto sopra, la U.O.C. TECNICA E PROGRAMMAZIONE - CED adotta adeguati strumenti per la protezione della rete aziendale dagli accessi abusivi e ne cura l'aggiornamento periodico. In particolare, a fini di protezione dai programmi informatici diretti a danneggiare o interrompere il sistema informatico o telematico (art. 615- *quinquies* del codice penale), sui computer collegati alla rete è installato un programma antivirus. Il programma antivirus è sempre attivo e viene costantemente e automaticamente aggiornato, all'atto del collegamento alla rete aziendale, direttamente dal server della LAN. La U.O.C. TECNICA E PROGRAMMAZIONE - CED provvede agli aggiornamenti periodici sulla base delle indicazioni fornite dal produttore.

Le opzioni stabilite dalla U.O.C. TECNICA E PROGRAMMAZIONE - CED non possono essere autonomamente modificate dagli Utenti.

Per i personal computer portatili tutti gli aggiornamenti dovranno essere effettuati collegandosi periodicamente tramite la LAN aziendale.

La U.O.C. TECNICA E PROGRAMMAZIONE - CED cura, sulla base dei rilasci effettuati dai fornitori, l'aggiornamento periodico dei programmi e dei sistemi finalizzato alla prevenzione delle vulnerabilità e alla correzione dei difetti.

5.3 Dispositivi mobili

Di seguito si dettagliano le istruzioni operative relative all'utilizzo di telefoni cellulari, smartphone, iPhone, iPad, tablet e altri Dispositivi aziendali simili per caratteristiche e funzionalità. Si evidenza che in via residuale è consentito l'utilizzo di Dispositivi personali per lo svolgimento delle attività lavorative, ferme restando le disposizioni del presente Regolamento.

Gli Utenti devono assicurarsi che i Dispositivi mobili utilizzati per accedere ai Sistemi Informativi, indipendentemente dal fatto che il Dispositivo sia di proprietà personale o di proprietà dell'Azienda, siano sempre custoditi in un luogo sicuro, specialmente durante gli eventuali spostamenti fuori dai locali della AO SAN PIO e non siano lasciati in luoghi non protetti o a vista.

Quando gli Utenti lavorano in un luogo pubblico, devono assicurarsi che le informazioni confidenziali visualizzate sul display, non possano essere lette da altre persone esterne all'Azienda.

Gli Utenti devono avvisare tempestivamente la U.O.C. TECNICA E PROGRAMMAZIONE - CED in caso di furto o smarrimento del Dispositivo mobile. In tale circostanza, gli Utenti sono tenuti a consegnare all'U.O.C. TECNICA E PROGRAMMAZIONE - CED copia della denuncia presentata alla Pubblica Autorità.

Con riferimento ai Dispositivi mobili forniti in dotazione dalla AO SAN PIO, le applicazioni la cui installazione è consentita sono esclusivamente quelle provviste di un'adeguata licenza e fornite da canali di distribuzione riconosciuti dal mercato (ad esempio Google Play, App Store Apple, Microsoft Store, Amazon Apps, Samsung Apps).

Con riferimento ai Dispositivi mobili personali utilizzati per le attività lavorative, gli Utenti devono adottare misure adeguate al fine di preservare la sicurezza delle informazioni aziendali eventualmente memorizzate o accessibili dagli stessi. In particolare, devono:

- provvedere alla tempestiva cancellazione dei dati e delle informazioni aziendali al termine del loro utilizzo;

- astenersi da ogni tipologia di back up dei dati e delle informazioni aziendali.

5.4 Dispositivi di memorizzazione rimovibili

Di seguito si dettagliano le istruzioni operative relative all'utilizzo di Dispositivi di memorizzazione rimovibili. Si evidenza che non è consentito l'utilizzo di Dispositivi personali per lo svolgimento delle attività lavorative, ferme restando le disposizioni del presente Regolamento.

I Dispositivi interessati sono tutti quelli rimuovibili e/o mobili utilizzati come strumento per l'archiviazione dei dati ed appartenenti alle seguenti categorie:

- Memory card;
- Drive USB;
- Hard Disk;
- DVD riscrivibili e simili.

Gli Utenti devono custodire e controllare i supporti informatici sui quali sono registrati dati personali (soprattutto se appartenenti a categorie particolari e/o giudiziari) in maniera tale che soggetti non autorizzati non possano venire a conoscenza nemmeno accidentalmente dei contenuti di tali supporti. Al termine di ogni lavorazione i supporti informatici dovranno essere custoditi in armadi o cassetti muniti di serratura e chiusi a chiave.

In caso di cattivo funzionamento che determini l'impossibilità della lettura dei dati in essi registrati, i supporti devono essere fisicamente distrutti prima di essere dismessi.

Con riferimento ai Dispositivi di memorizzazione personali utilizzati per le attività lavorative, gli Utenti devono adottare misure adeguate al fine di preservare la sicurezza delle informazioni aziendali eventualmente memorizzate o accessibili dagli stessi. In particolare, devono:

- provvedere alla tempestiva cancellazione dei dati e delle informazioni aziendali al termine del loro utilizzo;
- astenersi da ogni tipologia di back up dei dati e delle informazioni aziendali.

6 GESTIONE ED ASSEGNAZIONE DELLE CREDENZIALI DI AUTENTICAZIONE

Ad ogni Utente possono essere assegnate una o più credenziali di autenticazione per l'accesso a sistemi diversi.

Le credenziali degli Utenti sono assegnate e disattivate dagli uffici preposti in caso di non utilizzo nonché in caso di perdita della qualità atta a garantire all'Utente l'accesso ai dati personali (ad es. di soggetto autorizzato al trattamento), secondo le modalità e le procedure definite tempo per tempo dall'AO SAN PIO.

Fanno eccezione le credenziali di sistema assegnate e preventivamente autorizzate per finalità di gestione tecnica e di emergenza dei sistemi.

Il codice identificativo per l'accesso alla rete aziendale è personale ed univoco. Lo stesso codice non potrà essere attribuito a più di un Utente. In caso di cessazione del rapporto per qualsiasi ragione, il codice identificativo del personale interessato viene cancellato.

Per l'uso dei personal computer, nonché per l'accesso ai dati ed alla rete è, tra l'altro, obbligatorio:

- l'uso di un codice identificativo personale e di una parola chiave per l'accesso ai dati, nonché di un programma antivirus, per i PC connessi in rete;

Al momento della creazione dell'utenza, gli uffici preposti assegnano una parola chiave provvisoria che dovrà essere cambiata dall'Utente al primo accesso. La parola chiave non può essere condivisa, trascritta o annotata in maniera da essere accessibile ad altri.

Ogni personal computer e il sistema informatico aziendale, ferma la predilezione della AO SAN PIO per gli accessi c.d. "single sign-on", possono prevedere la possibilità di utilizzare diverse parole chiave:

1. di dominio, che viene digitata sulla stessa maschera di ingresso insieme al codice identificativo personale;

2. di dominio per la protezione dello schermo video (screen saver);
3. di accesso diretto ai singoli applicativi;
4. di accesso alla casella di posta elettronica (e-mail).

Le parole chiave hanno natura personale e, come tali, non possono essere comunicate a nessun altro soggetto.

Agli Utenti si raccomanda di utilizzare, per gli accessi di propria competenza, parole chiave diverse tra loro laddove non sia disponibile il single sign-on.

La parola chiave non deve contenere riferimenti agevolmente riconducibili all'Utente ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni 90 giorni.

L'AO SAN PIO può stabilire, comunicandoli ai singoli Utenti, ulteriori e più restrittivi criteri di composizione e lunghezza della parola chiave – e/o ulteriori e più restrittivi criteri di sicurezza – per particolari funzioni aziendali e nel caso di trattamenti di dati di particolare rilevanza.

In caso di smarrimento della password, il reset avviene ad opera degli Amministratori di Sistema nominati nell'ambito delle singole UO che rilasciano le password.

L'AO SAN PIO si riserva di accedere ai pc in uso all'Utente tramite gli Amministratori di Sistema esclusivamente per motivi di sicurezza e protezione del sistema informatico (a titolo esemplificativo seppur non esaustivo, per finalità di contrasto di virus, *malware*, intrusioni telematiche) ovvero per motivi tecnici e/o manutentivi e/o comunque finalizzati al di regolare svolgimento dell'attività lavorativa (ad esempio aggiornamento, sostituzione implementazione di programmi, manutenzione hardware) con il consenso espresso dell'Utente.

7 BACKUP

I backup aziendali vengono eseguiti esclusivamente sui server di AO SAN PIO e non sulle singole postazioni. Conseguentemente, i file salvati dagli Utenti esclusivamente sulle proprie postazioni (hard disk locali) possono andare irreversibilmente perduti in caso di incidente informatico.

8 UTILIZZO DELLA RETE AZIENDALE

Per l'accesso alla rete aziendale ciascun Utente deve essere in possesso delle specifiche Credenziali di autenticazione.

È vietato accedere alla rete e ai programmi con un codice d'identificazione Utente diverso da quello ricevuto come abilitazione personale. Le parole chiave d'ingresso alla rete ed (eventualmente) ai programmi sono segrete e vanno gestite secondo le procedure impartite.

Le cartelle presenti nei server aziendali sono aree di condivisione di informazioni strettamente connesse all'attività lavorativa e non possono essere utilizzate per scopi diversi.

Risulta opportuno che, con regolare periodicità, ciascun Utente provveda alla pulizia delle cartelle di rete di cui è responsabile, con la cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati, al fine di evitare un'archiviazione ridondante.

Si sottolinea, inoltre, che le informazioni aziendali e i dati personali non possono essere salvati in backup o memorizzati su alcun servizio di archiviazione disponibile in Internet o su "Cloud" (es. "iCloud", "Google Drive", "DropBox", ecc.) non autorizzato dalla Azienda.

9 UTILIZZO DELLA POSTA ELETTRONICA

L'utilizzo della posta elettronica è riconosciuto a tutti i dipendenti di AO SAN PIO, nonché, previa richiesta del Responsabile dell'unità operativa in cui operano, ai collaboratori (lavoratori somministrati, collaboratori a progetto, consulenti, *stagiaire*, tirocinanti, ecc.).

La casella di posta elettronica assegnata agli Utenti è uno strumento di lavoro e deve essere utilizzata esclusivamente per finalità connesse in via diretta allo svolgimento dell'attività lavorativa.

Ogni e qualsiasi utilizzo diverso, e comunque non inerente all'attività lavorativa, salvo espressa autorizzazione dell'AO SAN PIO, è conseguentemente vietato, ad eccezione di quanto previsto al paragrafo 9.4 del presente Regolamento.

L'Utente può fornire a terzi il proprio indirizzo di posta elettronica aziendale solo per ragioni di lavoro; nella formulazione dei messaggi di posta deve inoltre far uso di un linguaggio appropriato, corretto e rispettoso, a tutela della dignità delle persone e dell'immagine e reputazione della AO SAN PIO.

Le e-mail trasmesse sono sotto la responsabilità degli Utenti assegnatari dell'indirizzo, che devono essere consapevoli del fatto che tali messaggi possono essere considerati alla stregua di un documento firmato e possono generare obblighi vincolanti per l'azienda.

Gli Utenti assegnatari delle caselle di posta elettronica sono responsabili del loro corretto utilizzo; in particolare:

- non devono inviare informazioni aziendali e dati personali più di quanto sia necessario in ragione della finalità lavorativa perseguita, sia internamente sia esternamente;
- hanno l'obbligo di controllare gli allegati prima del loro utilizzo, non eseguire il download di file eseguibili (.exe) o scaricare documenti da siti Web non attendibili o da altre fonti non riconducibili ad attività lavorative in essere.
- non possono creare o inoltrare "lettere a catena o catene di Sant'Antonio" ("*chain letters*"), ovvero e-mail che esortino i destinatari a inoltrare il contenuto ad altri destinatari. Bisogna pertanto eliminare qualsiasi messaggio ricevuto di questo tipo.

La casella di posta, inoltre, deve essere fatta oggetto di manutenzione, cancellando periodicamente documenti inutili e allegati ingombranti all'interno della casella stessa. In ogni caso il sistema non consente di ricevere o spedire messaggi che globalmente - compresi cioè eventuali allegati - superino i 70 MB. Nel caso che i limiti di spazio della casella vengano superati, l'utente viene avvertito con messaggi automatici. Nel caso ulteriore che l'Utente non provveda a rientrare al di sotto dei limiti fissati, non gli sarà possibile inviare la posta. Se ancora l'utente non provvederà a liberare la casella, sarà interdetta anche la ricezione della posta.

9.1 E-mail di Massa/E-mail Batch

Al fine di proteggere i destinatari da e-mail di massa non autorizzate e proteggere i Sistemi Informativi aziendali da un volume eccessivo di e-mail, gli Utenti devono utilizzare il campo "Bcc/Ccn" (copia "blind") o la funzionalità di "Mail Merge" quando inviano messaggi di posta elettronica di massa/batch: questo è necessario per evitare di divulgare i Dati Personali (nomi e/o indirizzi di posta elettronica) ad altri destinatari del messaggio in violazione degli obblighi di riservatezza, privacy e protezione dei dati della Azienda.

9.2 Sicurezza delle E-mail

In caso di messaggi anomali o sospetti (es., ma non solo, mail in un italiano con errori evidenti di ortografia) vanno rispettate le seguenti regole:

- il messaggio non va aperto;
- nel caso in cui il sospetto di anomalia sorga solo dopo l'apertura del messaggio, occorre astenersi assolutamente dall'aprire gli eventuali allegati (immagini, documenti, presentazioni, filmati), qualunque formato ed estensione essi abbiano per evitare la diffusione del virus;
- il messaggio va immediatamente segnalato alla U.O.C. TECNICA E PROGRAMMAZIONE - CED per le indagini del caso; successivamente, salve diverse indicazioni della stessa U.O.C. TECNICA E PROGRAMMAZIONE - CED , esso deve essere cancellato nel più breve tempo possibile;
- qualsiasi Utente che sia a conoscenza di una potenziale minaccia di "*phishing" o virus/malware* tramite posta elettronica deve segnalarlo alla U.O.C. TECNICA E PROGRAMMAZIONE - CED , la quale è l'unica autorizzata ad inviare messaggi riguardanti potenziali minacce di sicurezza.

Si rende noto, in proposito, che l'AO SAN PIO adotta sistemi automatici non presidiati anti-spam e anti-*malwar*e. I messaggi più sospetti sono cancellati immediatamente, mentre i meno sospetti sono posti in quarantena e vengono cancellati periodicamente in maniera automatica.

9.3 Assenze Programmate e Improvvise

L'Utente, in caso di assenza programmata di almeno una giornata lavorativa (ad esempio per ferie o attività di lavoro fuori sede), ha facoltà di attivare l'apposita funzionalità di sistema che consente di inviare

automaticamente a terzi un messaggio di risposta contenente le “coordinate” (anche elettroniche o telefoniche) di un altro Utente o altre modalità utili di contatto della struttura.

9.4 Utilizzo della Posta Elettronica per Uso Personale

L’utilizzo della posta elettronica aziendale per uso personale non è consentito in conformità con questo regolamento ed altre policy in materia di violazione della riservatezza, della sicurezza e della privacy dei dati trattati.

A tal fine gli Utenti:

- **non devono mai, in nessuna occasione, utilizzare una firma personale che contenga un riferimento all’AO SAN PIO o qualsiasi riferimento che possa implicare l'invio dell’e-mail per conto dell’Azienda;**
- **devono aver cura di eliminare l’avvertimento standardizzato nel quale viene dichiarata la natura non personale dei messaggi;**
- **devono indicare nell’oggetto del messaggio la dicitura “Personale” o “Privato”.**

L'utilizzo personale di posta elettronica, inoltre, non deve:

- prevedere contenuti che l'Utente non desidera vengano letti da una terza parte (es. U.O.C. TECNICA E PROGRAMMAZIONE - CED durante le attività di cui al §14 e §15 di questo regolamento);
- avere priorità rispetto alle attività di carattere aziendale o alle responsabilità lavorative dell'Utente;
- interrompere il normale flusso di attività (es. lettere a catena, allegati di grandi dimensioni non necessari);
- interferire con le attività di altri Utenti;
- costituire reato;
- provocare costi, obblighi o passività aggiuntivi per l’Azienda, di qualsiasi tipo.

10 NAVIGAZIONE IN INTERNET

L’accesso ad Internet è consentito ai dipendenti ed ai consulenti.

L’abilitazione alla navigazione in Internet è riconosciuta all’Utente per finalità connesse allo svolgimento della propria attività lavorativa.

In questo senso, a titolo puramente esemplificativo, l’Utente non può utilizzare Internet per ragioni personali. È in ogni caso vietato l’uso per:

- l’upload o il download di software gratuiti (per es. freeware e shareware), nonché l’utilizzo di documenti provenienti da siti web o http, se non strettamente attinenti all’attività lavorativa (per es. filmati) e previa verifica dell’attendibilità dei siti in questione (nel caso di dubbio, dovrà venir a tal fine contattato il personale della U.O.C. TECNICA E PROGRAMMAZIONE - CED);
- l’uso di servizi di rete con finalità ludiche;
- la partecipazione a forum non professionali, l'utilizzo di chat line, di bacheche elettroniche (esclusi gli strumenti autorizzati);
- navigazione sui social network per finalità estranee a quelle lavorative.

Al fine di evitare la navigazione in siti non pertinenti all’attività lavorativa, l’AO SAN PIO adotta uno specifico sistema di blocco o filtro automatico, idoneo a prevenire determinate operazioni reputate inconferenti con l’attività lavorativa, quali l’upload o l’accesso a determinati siti inseriti in una black list, ovvero il download di file o software aventi particolari caratteristiche dimensionali o di tipologia di dati.

Per esigenze aziendali, alcune utenze hanno delle deroghe su determinati siti Web in black list.

11 ACCESSO REMOTO / SMART WORKING

L'AO SAN PIO, anche in ragione della necessità di favorire forme di lavoro agile / *smart working*, ha implementato tecnologie che consentono di accedere "da remoto" (ovvero al di fuori degli uffici della Azienda) ad alcuni Sistemi Informativi aziendali.

Nello svolgimento della prestazione lavorativa da remoto, ogni Utente avrà cura di continuare a garantire:

- il rispetto delle politiche di sicurezza informatica e di corretto trattamento dati personali vigenti nella AO SAN PIO.
- L'utilizzo, per lo svolgimento delle prestazioni lavorative affidate, di soli strumenti informatici – personali o di AO SAN PIO – corredati da software originale e aggiornato, protetti da adeguato antivirus originale e
  aggiornato e il cui accesso sia protetto da password.
- La piena riservatezza e confidenzialità delle credenziali informatiche di accesso agli strumenti lavorativi, ai programmi e alle informazioni aziendali.
- Il trattamento dei dati personali di titolarità della AO SAN PIO nei limiti di stretta necessità collegati alla corretta esecuzione della prestazione lavorativa.
- La segregazione fisica e logica delle informazioni trattate per conto della AO SAN PIO da qualsiasi altra di natura personale o, comunque, estranea alla prestazione lavorativa.
- Il blocco delle postazioni informatiche in tutte le occasioni in cui la persona autorizzata al trattamento se ne allontani per qualsiasi ragione.

In tale contesto, in particolare, gli Utenti avranno cura di far sì che le Credenziali loro assegnate rimangano assolutamente riservate e confidenziali e in nessun caso possono essere comunicate a soggetti terzi ivi inclusi i familiari e i conviventi.

Allo stesso modo, le informazioni trattate per conto della AO SAN PIO dovranno essere custodite con estrema attenzione rendendole non accessibili a terzi (ad es. chiuse a chiave in un cassetto laddove si tratti di documentazione cartacea ovvero in una cartella protetta da password per i file informatici) e, in ogni caso, sempre separate da qualsiasi altra di natura personale o, comunque, estranea alla prestazione lavorativa.

12 RIEPILOGO DELLE DISPOSIZIONI SUL CORRETTO UTILIZZO DEGLI STRUMENTI

Nell'utilizzo degli strumenti aziendali, gli Utenti sono tenuti al rispetto delle disposizioni in precedenza riportate, talune delle quali di seguito brevemente richiamate congiuntamente ad ulteriori specifiche disposizioni.

In termini generali:

- attenersi alla stretta osservanza delle istruzioni ricevute dalla Azienda contenute nel presente Regolamento e nelle ulteriori indicazioni ricevute con riferimento a specifici contesti di operatività;
- conservare la documentazione cartacea ed elettronica per il periodo di tempo massimo indicato dal proprio Responsabile e comunque in conformità al Registro dei Trattamenti adottato tempo per tempo dall'Azienda;
- astenersi dall'utilizzare i Sistemi Informativi aziendali per scopi professionali diversi da quelli dell'Azienda.

Con riferimento agli accessi fisici ed ai documenti cartacei:

- non cedere mai ad altri il proprio *badge* ovvero le chiavi degli armadietti/cassetti assegnati;
- denunciare immediatamente il furto o lo smarrimento del proprio *badge* o delle proprie chiavi;

- conservare tutti i documenti cartacei relativi o contenenti dati personali in cassetti, armadi o spazi accessibili tramite chiavi e in modo tale da consentire l'accesso selezionato dei dati stessi (a titolo di esempio, facendo uso di cartelle, classificatori e schedari);
- distruggere tutto il materiale di lavoro da cestinare, contenente informazioni aziendali o dati personali, utilizzando le apposite apparecchiature distruggi documenti o comunque facendo in modo che i dati non siano visibili;
- in caso di consultazione, accedere per quanto possibile ai soli documenti di interesse e riporre questi ultimi nel luogo di conservazione al termine di ogni giornata lavorativa anche qualora il giorno successivo sia necessario effettuare una nuova consultazione;
- non portare al di fuori dei locali aziendali, se non strettamente necessario per ragioni lavorative e/o previa autorizzazione del proprio Responsabile, documenti cartacei o supporti contenenti informazioni aziendali o dati personali.

Con riferimento agli accessi logici e ai documenti elettronici:

- non cedere mai ad altri le proprie password;
- è vietato tentare o ottenere l'accesso non autorizzato a Sistemi Informativi aziendali o informazioni aziendali (inclusi file protetti da password) senza autorizzazione;
- occorre modificare le password al primo accesso e periodicamente, in conformità alle indicazioni fornite dalla U.O.C. TECNICA E PROGRAMMAZIONE - CED ;
- non scrivere le password in uso su supporti accessibili a terzi;
- attenersi alle ulteriori disposizioni emanate tempo per tempo dall'AO SAN PIO;
- bloccare il proprio personal computer in caso di allontanamento anche momentaneo dalla propria postazione e, in particolare, non lasciare la postazione di lavoro con sessioni applicative aperte tramite password;
- non copiare o salvare informazioni aziendali e/o dati personali su dispositivi, sistemi o servizi non approvati (ad esempio supporti rimovibili come unità USB non cifrati o applicazioni di memorizzazione su Cloud);
- non scaricare da Internet o da altra fonte programmi che non siano di origine ufficiale e certa e che non siano strettamente funzionali alle mansioni di competenza;
- non inviare o scaricare materiale in violazione del copyright;
- in generale, utilizzare gli strumenti aziendali in conformità al presente Regolamento, alle policy e alle regole anche tecniche tempo per tempo emanate;
- provvedere al trasporto dei documenti su altri supporti elettronici solo ove ciò sia strettamente necessario e in tal caso provvedere alla loro cancellazione al termine del loro utilizzo;
- non collegare apparecchiature non aziendali (ad esempio computer o dispositivi mobili) alle reti della Azienda se non autorizzati dalla U.O.C. TECNICA E PROGRAMMAZIONE - CED .

Con riferimento all'utilizzo degli applicativi:

- non condividere con terzi le credenziali di accesso al personal computer (nome utente e password) in quanto strettamente personali;
- rispettare le politiche di back-up e disaster recovery stabilite dall'AO SAN PIO;
- non condividere le utenze applicative nominative con consulenti e fornitori;
- non creare, distribuire, pubblicare, inviare o condividere materiale offensivo, abusivo, osceno, discriminatorio, razzista o criminale che possa mettere in pericolo o causare imbarazzo all'Azienda, ai Pazienti, al Personale o ad altri;
- non inviare posta indesiderata, "Spam", lettere a catena, virus, truffe o qualsiasi rete o trasmissione di dati intenzionale che interferisca con il normale funzionamento dei Sistemi Informativi aziendali;
- utilizzare in modo conforme al presente Regolamento la copia nascosta (Bcc) per le email di massa/in batch.

Con riferimento ai supporti rimovibili:

- custodire i supporti contenenti dati personali per il tempo strettamente necessario al loro utilizzo in armadi o cassetti con serratura e chiusi a chiave;
- provvedere alla preventiva cancellazione sicura, secondo le istruzioni in tal senso ricevute dagli Amministratori di Sistema, delle informazioni presenti nei supporti e contenenti dati personali prima del loro riutilizzo successivo o smaltimento;
- procedere alla cancellazione sicura dei dati ovvero alla distruzione fisica dei supporti contenenti informazioni aziendali o dati personali nel caso di dismissione per guasto e/o obsolescenza.

13 PROTEZIONE DA VIRUS E MALWARE

I software maligni per il computer (malware) quali ad esempio "Virus", "Worms", "Trojans" costituiscono una seria minaccia alla sicurezza e alla stabilità dei Sistemi Informativi e dei dati aziendali. L'AO SAN PIO utilizza diversi strumenti di protezione dai malware sui propri Sistemi Informativi. Essi includono i servizi per la sicurezza delle e-mail (es. anti-spam) e la sicurezza su Internet tramite i fornitori del servizio mail e connettività, disegnati appositamente per contrastare e-mail e siti web maligni, come ad esempio software anti-virus installati su personal computer, dispositivi mobili e server.

I creatori di malware continuano ad aggiornare i loro software nel tentativo di evitarne il rilevamento da parte dei suddetti strumenti. Come descritto all'interno del presente Regolamento, gli Utenti non devono mai aprire e-mail, allegati o visitare siti web dei quali non sono sicuri o che non hanno specificamente richiesto. Se un Utente ha il sospetto relativo a determinate e-mail, allegati o siti web, dovrà rivolgersi alla U.O.C. TECNICA E PROGRAMMAZIONE - CED , che valuterà se sono necessarie ulteriori azioni e gestirà le comunicazioni necessarie all'azienda.

I virus possono anche provenire da programmi contenuti nei dispositivi di archiviazione rimovibili, ad esempio unità USB, schede SD, CD e DVD. I dispositivi non espressamente autorizzati non devono essere collegati ai Sistemi Informativi aziendali.

L'installazione o l'esecuzione di software e programmi eseguibili (compresi giochi, screen saver, wallpaper e altre applicazioni) non forniti dall'Azienda possono causare infezioni da malware nel dispositivo dell'Utente e quindi nella rete aziendale ed è pertanto vietata. In caso di dubbi o particolari esigenze, si prega di contattare la U.O.C. TECNICA E PROGRAMMAZIONE - CED .

14 ACCESSO AI DATI TRATTATI DALL'UTENTE

La U.O.C. TECNICA E PROGRAMMAZIONE - CED , in alcuni casi, può accedere ai dati trattati dall'Utente tramite posta elettronica o navigazione in rete al fine di:

- garantire la sicurezza e la protezione del sistema informatico (a titolo esemplificativo seppur non esaustivo, contrasto di virus, malware, intrusioni telematiche, spamming, phishing, spyware);
- svolgere attività tecniche e/o di manutenzione (ad esempio, aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware);
- garantire mediante l'applicazione di misure di sicurezza informatiche preventive, che l'utilizzo a scopo lavorativo dei Sistemi Informativi aziendali, tra cui posta elettronica, internet, scansione, stampa, social media e altre comunicazioni sia conforme alle politiche e alle norme dell'Azienda;
- proteggere le informazioni aziendali e i dati personali;
- adempiere agli obblighi giuridici dell'Azienda, anche in qualità di datore di lavoro;
- garantire che l'Azienda rispetti gli obblighi di legge e contrattuali.

Ove sia necessario per garantire la sicurezza e l'operatività del sistema, il personale della U.O.C. TECNICA E PROGRAMMAZIONE - CED incaricato avrà anche la facoltà di collegarsi e visualizzare in remoto il desktop delle singole postazioni, avendo cura di avvertire con la massima tempestività l'Utente che dovrà fornire il proprio consenso e sovraintenderà alle operazioni compiute.

Il personale incaricato della U.O.C. TECNICA E PROGRAMMAZIONE - CED può, nei casi suindicati, procedere a tutte le operazioni di configurazione e gestione necessarie a garantire la corretta funzionalità del sistema informatico aziendale (a titolo esemplificativo, rimozione di file o applicazioni pericolosi).

L'AO SAN PIO di Benevento, inoltre, fatto salvo quanto previsto dalla Legge 300/1970 e nel rispetto

dei principi di pertinenza e non eccedenza, laddove se ne ravvisi la stretta necessità, si riserva il diritto di:

- recuperare materiale scansionato, stampato e copiato;
- proteggere le informazioni aziendali e i dati personali;
- indagare sull'uso improprio dei Sistemi Informativi e su altri atti non idonei;
- intraprendere altre azioni ragionevolmente necessarie per conformarsi a qualsiasi obbligo legale o contrattuale.

In ogni caso, l'AO SAN PIO garantisce la non effettuazione di trattamenti mediante sistemi *hardware* e *software*
specificatamente preordinati al controllo a distanza dell'attività lavorativa, quali, a titolo esemplificativo:

- lettura e registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori (*log*) al di là di quanto tecnicamente necessario per svolgere il servizio *e-mail*;
- riproduzione ed eventuale memorizzazione sistematica delle pagine *web* visualizzate dal lavoratore;
- lettura e registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo.

Il personale incaricato della U.O.C. TECNICA E PROGRAMMAZIONE - CED è autorizzato ad accedere ai dati contenuti negli strumenti informatici restituiti dall'Utente all'AO SAN PIO, a titolo di esempio, per cessazione del rapporto o per sostituzione delle apparecchiature. Sarà cura dell'Utente provvedere alla cancellazione preventiva di tutti gli eventuali dati personali ivi contenuti. Nel caso di cessazione del rapporto, ed in mancanza della cancellazione dei dati da parte dell'interessato, detta cancellazione sarà operata dalla U.O.C. TECNICA E PROGRAMMAZIONE - CED .

14.1 Registrazione di Attività su Internet

Il personale incaricato della U.O.C. TECNICA E PROGRAMMAZIONE - CED può procedere a controlli sulla navigazione finalizzati a garantire l'operatività e la sicurezza del sistema.

Di seguito si riportano le informazioni che vengono registrate per ragioni tecniche di funzionamento dei sistemi in relazione all'utilizzo di Internet da parte di un Utente:

- Indirizzo IP;
- Data e ora;
- URL richiesti dal browser;
- Durata / Tempo trascorso;
- Caricamenti e download di file.

15 CONTROLLI GRADUALI

Nel rispetto dei principi di pertinenza e non eccedenza, le verifiche sul corretto utilizzo degli strumenti informatici saranno realizzate dall'AO SAN PIO nel pieno rispetto dei diritti e delle libertà fondamentali degli Utenti e del presente Regolamento.

In caso di anomalie, l'AO SAN PIO privilegerà, per quanto possibile, controlli preliminari anonimi riferiti alla zona in cui si è verificata l'anomalia.

16 SANZIONI

Tutti gli Utenti sono tenuti ad osservare le disposizioni contenute nel presente Regolamento. Il mancato rispetto o la violazione delle regole sopra richiamate può determinare l'applicazione dei provvedimenti disciplinari previsti dal CCNL /dal contratto di lavoro applicabile.

17 AGGIORNAMENTO E REVISIONE

Il presente Regolamento è soggetto ad aggiornamento e revisione periodica, anche in base all'evoluzione tecnologica e normativa, nonché in linea con l'aggiornamento delle attrezzature hardware e software messe a disposizione degli Utenti.