

REGOLAMENTO PER IL CORRETTO UTILIZZO DEI SISTEMI INFORMATICI AZIENDALI

Premessa

Le realtà aziendali sono andate caratterizzandosi per l'elevato ricorso all'utilizzo di tecnologie informatiche che hanno consentito l'introduzione di innovative tecniche di gestione dell'impresa, ma che, d'altro canto, hanno anche dato origine a numerose problematiche relative all'utilizzo degli strumenti informatici forniti dall'azienda ai propri dipendenti per lo svolgimento delle mansioni e compiti affidati.

I controlli sull'uso degli strumenti informatici tuttavia, devono garantire tanto il diritto del datore di lavoro di proteggere la propria organizzazione, essendo i computer aziendali strumenti di lavoro la cui utilizzazione personale è preclusa, quanto il diritto del lavoratore a non vedere invasa la propria sfera personale, e quindi il diritto alla riservatezza ed alla dignità come sanciti dallo Statuto dei lavoratori.

Alla luce delle considerazioni sopra espresse e tenuto opportunamente conto delle Linee guida emanate dall'Autorità Garante per la protezione dei dati personali, con propria deliberazione n. 13 del 1 marzo 2007, sulla disciplina della navigazione in Internet e sulla gestione della posta elettronica nei luoghi di lavoro, la Casa di Cura Le Terrazze ha predisposto il regolamento per disciplinare le condizioni per il corretto utilizzo degli strumenti informatici da parte dei suoi dipendenti e/o collaboratori.

Tale regolamento, oltre a dettare una disciplina per l'utilizzo degli strumenti informatici aziendali, vuole costituire un utile strumento per sensibilizzare il personale su altri aspetti altrettanto importanti nella gestione dei sistemi informatici aziendali, quali il rispetto della normativa sulla tutela legale del software (e quindi il controllo sulla regolarità del software presente nello stesso sistema informatico), e quella sulla tutela del know-how aziendale, quando queste importanti informazioni di proprietà dell'Azienda sono custodite nel sistema informatico.

Anche l'entrata in vigore della normativa NIS2 (Network Information Security), con la conseguente necessità di adottare adeguate misure di sicurezza, costituisce un fondamentale riferimento rispetto alle possibilità di utilizzo degli strumenti informatici aziendali.

Il regolamento, redatto in modo trasparente e senza formule generiche, sarà pubblicizzato adeguatamente (con pubblicazione sulla rete interna e mediante affissioni sui luoghi di lavoro con modalità analoghe a quelle previste dall'art. 7 dello Statuto dei lavoratori) e verrà sottoposto ad aggiornamento periodico.

Sono tenuti all'osservanza delle presenti disposizioni, oltre ai Dipendenti della Casa di Cura, anche soggetti "esterni" all'Azienda nei casi relativi a collaborazioni di persone fisiche o giuridiche (convenzioni, consulenze, tirocini, ecc.).

Introduzione

La progressiva diffusione delle nuove tecnologie informatiche e, in particolare, il libero accesso alla rete Internet dai Personal Computer, espone l'azienda e gli utenti (dipendenti e collaboratori della stessa) a rischi di natura patrimoniale, oltre alle responsabilità penali conseguenti alla violazione di specifiche disposizioni di legge (legge sul diritto d'autore e legge sulla privacy, fra tutte), creando evidenti problemi alla sicurezza ed all'immagine dell'Azienda stessa.

Premesso quindi che l'utilizzo delle risorse informatiche e telematiche deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito dei rapporti di lavoro, la Casa di Cura adotta un Regolamento interno diretto ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla Sicurezza informatica e al trattamento dei dati.

Le prescrizioni di seguito previste si aggiungono ed integrano le specifiche istruzioni eventualmente già fornite agli incaricati ed ai responsabili del trattamento dei dati in attuazione del Regolamento UE 679/2016 (GDPR) e della normativa nazionale applicabile, nonché integrano le informazioni già fornite agli interessati in ordine alle ragioni e alle modalità dei possibili controlli o alle conseguenze di tipo disciplinare in caso di violazione delle stesse.

Campo di applicazione

Il regolamento si applica a tutti i dipendenti, senza distinzione di ruolo e/o livello, nonché a tutti i collaboratori dell'azienda a prescindere dal rapporto contrattuale con la stessa intrattenuto (collaboratore a progetto, in stage, consulenti, professionisti, tirocinanti ecc.).

Copia del regolamento, oltre ad essere affisso nella bacheca aziendale, è messo a disposizione in rete in "collegamento a qualità" nella sottocartella "privacy".

La consegna di una copia è una scelta facoltativa: si ricorda, infatti, che, ai sensi dell'art. 7 Legge n. 300/1970, l'unico obbligo a carico del datore di lavoro, ai fini dell'esercizio del potere disciplinare, è quello di dare adeguata pubblicità delle norme mediante l'affissione in luogo accessibile a tutti.

Per poter agire disciplinarmente nei confronti del dipendente, il regolamento dovrà pertanto essere affisso in luogo accessibile a tutti (bacheca).

I SISTEMI INFORMATICI AZIENDALI

Il personal computer (fisso o mobile, comprese le periferiche ad esso connesse) ed i relativi programmi e/o applicazioni affidati al dipendente sono, come è noto, strumenti di lavoro; tali strumenti pertanto:

- vanno custoditi in modo appropriato;
- possono essere utilizzati solo per fini professionali (in relazione, ovviamente, alle mansioni assegnate) e non a fini personali, tanto meno per scopi illeciti;
- debbono esserne prontamente segnalati all'azienda il furto, il danneggiamento o lo smarrimento.

La Casa di Cura rende noto che il personale incaricato che opera presso il CED è autorizzato a compiere interventi nel sistema informatico aziendale volti a garantire la sicurezza e la salvaguardia del sistema stesso, nonché per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware etc.).

Il personale del CED ha la facoltà di potersi collegare 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, spyware, malware, etc. L'intervento viene effettuato, anche con l'eventuale ricorso a consulenti esterni, in seguito alla chiamata dell'utente (l'attività di assistenza e manutenzione in remoto avviene previo avvertimento dell'utente interessato) o, in caso di oggettiva necessità, a seguito della rilevazione tecnica di problemi nel sistema informatico e telematico. In quest'ultimo caso, sempre che non si pregiudichi la necessaria tempestività ed efficacia dell'intervento, verrà data comunicazione della necessità dell'intervento stesso.

Ai fini sopra esposti, quindi, si riportano qui di seguito le più significative indicazioni comportamentali:

1. Norme relative all'utilizzo di personal computer

- a) Onde evitare il grave pericolo di introdurre virus informatici, nonché di alterare la stabilità delle applicazioni dell'elaboratore, non è consentito installare programmi (anche gratuiti) se non espressamente autorizzati dalla Direzione o dal Responsabile CED. Non è consentito inoltre l'uso di programmi non distribuiti ufficialmente;
- b) Non è consentito utilizzare strumenti software e/o hardware atti ad intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici;
- c) Non è consentito modificare le configurazioni impostate sul proprio PC, reinstallare o alterare il sistema operativo o qualsiasi altro software fornito in dotazione;
- d) Non è consentito smontare, modificare o manomettere in alcun modo l'hardware del PC o delle periferiche ad esso connesse o direttamente collegate alla rete dati aziendale, se non limitatamente alle operazioni strettamente legate al normale uso dell'apparecchiatura stessa, come ad esempio rimuovere parti della stampante per eliminare inceppamenti della carta o sostituire cartucce di stampa o toner;
- e) Non è permesso spostare apparecchiature informatiche "fisse" o scambiare periferiche tra diversi PC senza autorizzazione da parte del CED.;
- f) Nel caso di utilizzo di PC o altri device portatili, l'utente è tenuto a custodirli con diligenza sia durante l'utilizzo, sia durante gli eventuali spostamenti. A tali device si applicano le stesse regole previste dal presente regolamento per gli elaboratori "fissi". Qualora il device portatile sia utilizzato al di fuori della Casa di Cura, lo stesso deve essere custodito con diligenza, adottando tutti i provvedimenti che le circostanze rendono necessari per evitare danni o sottrazioni. Di norma i device portatili non vengono utilizzati per memorizzare dati o informazioni relativi ai principali trattamenti svolti dalla Casa di Cura. Qualora tale indicazione venga disattesa, per motivate ragioni operative e/o organizzative, sarà necessario, nel rispetto di quanto previsto dalla normativa NIS2, adottare un opportuno protocollo di cifratura;
- g) Non è consentita l'installazione sul PC utilizzato di mezzi di comunicazione propri (come ad esempio modem, cellulari, internet-key ecc.) se non autorizzati dal CED.;
- h) Particolare attenzione va prestata nell'utilizzo delle password di accesso alla rete o di utilizzo dei software, che non devono mai essere scritte su carta;
- i) Durante una sessione di lavoro, che comporta il trattamento di dati personali e/o sensibili, il personal computer non deve essere accessibile da parte di personale non autorizzato;
- j) Qualora, durante una sessione di trattamento di dati sensibili, si debba abbandonare, per un tempo più o meno prolungato, la postazione di lavoro, è opportuno sia impostato uno screen saver dotato di password (con tempi di avvio brevi) che blocchi l'accesso all'elaboratore;

- k) Qualora l'elaboratore sia utilizzato da più incaricati, ricordarsi, ogni volta che si è terminato di utilizzare il PC, di disconnettersi dal sistema. Prima di effettuare la disconnessione chiudere i programmi rimasti eventualmente aperti. In questo modo la persona che utilizzerà il PC in seguito dovrà comunque effettuare la procedura di autenticazione (che non sarà impedita da software rimasti aperti). Al termine della giornata lavorativa, in caso di assenze prolungate o in caso di suo inutilizzo, il PC e le relative periferiche (monitor, stampanti ecc.) **devono essere spenti**. 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;
- l) Nell'utilizzo del personal computer si raccomanda di prestare la massima attenzione nella creazione e conservazione (valutandone attentamente la possibilità di cancellazione esaurito lo scopo per il quale sono stati creati) di documenti e files contenenti dati personali e/o particolari, limitando tale eventualità ai soli casi strettamente necessari e per i quali non sia possibile ricorrere alle funzioni fornite dai software gestionali in uso. In tali casi, informare il DPO che valuterà la specifica necessità, dando indicazioni in merito alle misure tecniche e organizzative adeguate.

2. Utilizzo di supporti di memorizzazione rimovibili

- a) Al fine di rispettare quanto previsto dal requisito PR.DS-01 punto 2 delle misure di sicurezza di base per i soggetti NIS importanti (disattivazione dell'auto esecuzione dei supporti rimovibili), l'utilizzo di supporti archiviazione di massa rimovibili USB è inibito su tutte le postazioni di lavoro tramite apposita policy configurata sulla console centralizzata del software antivirus in uso;
- b) L'auto esecuzione è abilitata unicamente per i supporti CD/DVD, al fine di consentire, al personale dipendente e professionista medico, di poter agevolmente visualizzare e consultare esami radiologici e di diagnostica per immagini memorizzati su tali supporti. Sarà cura di tali figure verificare, preliminarmente all'utilizzo, la provenienza dei supporti, controllando che sia indicata la struttura che li ha prodotti. I supporti di dubbia provenienza andranno segnalati al CED, che provvederà a valutarne l'autenticità e, se del caso, ad autorizzarne l'utilizzo;
- c) I supporti rimovibili contenenti dati personali e/o sensibili (CD/DVD di esami radiologici e di diagnostica per immagini prodotti dalla Casa di Cura o provenienti da altre strutture sanitarie) devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto. I supporti contenenti dati personali e/o sensibili, se non più utilizzati, vanno distrutti. La distruzione è disciplinata nel Sistema qualità aziendale dalla procedura 07 19, cui si rimanda.

3. Utilizzo della rete aziendale

- a) Le unità di rete sono aree di condivisione di informazioni strettamente professionali e non possono, in alcun modo, essere utilizzate per scopi diversi. Pertanto, qualunque file non inerente l'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità;
- b) La Casa di Cura si riserva la facoltà di procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza del sistema, ovvero acquisiti o installati in violazione del presente Regolamento.

4. Utilizzo della rete Internet e dei relativi servizi (per gli utenti abilitati al loro utilizzo)

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

L'uso di Internet, nelle sue numerose funzionalità, è consentito esclusivamente per gli scopi attinenti al proprio lavoro e le attività svolte mediante la navigazione in Internet, o il sistema di posta elettronica, sono destinati al conseguimento dei fini istituzionali della Casa di Cura. I dati che vengono inviati mediante il sistema aziendale di posta elettronica sono di proprietà della Casa di Cura. Si riepilogano, di seguito, le disposizioni cui attenersi nell'utilizzo di tali risorse.

Navigazione in Internet:

- a) Non è consentito navigare in siti non attinenti allo svolgimento delle mansioni assegnate, soprattutto qualora il contenuto di tali siti sia di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica (il sistema Nethsecurity, interposto tra la rete aziendale e la rete Internet, impedisce l'accesso a siti web indesiderati, attraverso la valutazione del contenuto o per l'appartenenza a "black list");
- b) La navigazione è consentita dalle ore 7.00 alle ore 19.30; in orari diversi da quelli indicati il firewall della Casa di Cura blocca ed impedisce la navigazione;
- c) Non è consentita l'effettuazione di ogni genere di transazione finanziaria a titolo personale, ivi comprese le operazioni di remote banking, acquisti on-line e simili, salvo casi direttamente autorizzati dalla Direzione e con il rispetto delle normali procedure di acquisto;
- d) Non è consentito scaricare software, anche se gratuito, prelevato da siti Internet, se non espressamente autorizzato dalla Direzione o dal Responsabile CED (il download di file considerati, per la loro tipologia, potenzialmente "pericolosi" o inutili viene già bloccato dal sistema Nethsecurity);
- e) E' vietata ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa;
- f) Non è permessa la partecipazione, per motivi non professionali, a Forum, l'utilizzo di chat line, di bacheche elettroniche e le registrazioni in guest book anche utilizzando pseudonimi (o nicknames);
- g) Non è consentita la memorizzazione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.

Posta elettronica:

Nel precisare che anche la posta elettronica è uno strumento di lavoro, che le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse, si segnala che:

- a) Non è consentito utilizzare la posta elettronica (interna ed esterna) per motivi non attinenti allo svolgimento delle mansioni assegnate;
- b) La "personalizzazione" dell'indirizzo di posta elettronica, ovvero la possibilità che esso contenga riferimenti al nome e/o al cognome dell'utente, non comporta il fatto che la stessa venga considerata "privata", in quanto si tratta comunque di uno strumento di esclusiva proprietà della Casa di Cura, messo a disposizione di dipendenti e/o collaboratori a vario titolo al solo fine dello svolgimento delle proprie mansioni lavorative;
- c) Al fine di evitare inutile traffico di rete e spreco di spazio e risorse sul sistema di posta, non è consentito inviare messaggi a tutti i destinatari della rubrica indirizzi interna, salvo non si tratti di comunicazioni importanti e necessarie;
- d) La casella di posta deve essere mantenuta in ordine cancellando messaggi inutili, soprattutto qualora contengano allegati ingombranti;
- e) Non è consentito inviare o memorizzare messaggi (interni ed esterni) di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;
- f) La posta elettronica diretta all'esterno della rete informatica aziendale può essere intercettata da estranei e, dunque, non deve essere usata per inviare documenti di lavoro "Strettamente Riservati" (se non autorizzati dalla Direzione) o addirittura per trasmettere dati sensibili (ad eccezione delle comunicazioni ufficiali con Regione Lombardia e ATS Insubria);
- g) Non è consentito l'utilizzo dell'indirizzo di posta elettronica aziendale per la partecipazione a dibattiti, forum o mailing-list, salvo diversa ed esplicita autorizzazione;
- h) Non è consentito simulare l'identità di un altro utente, ovvero utilizzare credenziali di posta non proprie per l'invio di messaggi;
- i) Non è consentito l'utilizzo di critto sistemi o di qualsiasi programma di sicurezza e/o crittografia non previsto esplicitamente dal servizio informatico della Casa di Cura;
- j) E' di fondamentale importanza evitare di aprire file allegati, o cliccare su link, di messaggi di posta elettronica provenienti da mittenti o siti sconosciuti, anche qualora il mittente possa in qualche modo rimandare ad un indirizzo noto (gli allegati contenenti virus potrebbero comunque essere rimossi dal software Nethsecurity, che blocca anche il download di file pericolosi), o di rispondere a messaggi di spam (che potrebbero comunque esser segnalati come tali dal sistema Nethsecurity);
- k) In relazione all'aumento dei fenomeni di phishing, è necessario porre particolare attenzione all'utilizzo della posta elettronica, rispettando le seguenti regole comportamentali:
 - **Attenzione al mittente.** Il mittente può essere noto o sconosciuto. Se è sconosciuto occorre prestare attenzione ed interrogarsi sulla ragione del contatto, evitando di aprire le e-mail anomale inviate da indirizzi non noti, anche qualora si tratti di un'istituzione pubblica o di un ente bancario.

- **Attenzione alla grammatica del testo.** Analizzare il testo dell'e-mail, prestando attenzione particolare a:
 - messaggi inattesi,
 - testo generico,
 - testo con errori di battitura o sintassi,
 - testo tradotto da un'altra lingua,
 - messaggio ricevuto da altri mittenti,
 - contenuto istituzionale proveniente da banche, Poste Italiane, società di carte di credito, Google, Paypal, etc.,
 - contenuto riguardante sanzioni, multe, richieste di denaro, richieste di riscatti,
 - testo troncato, senza frasi di chiusura,
 - testo minaccioso, che mette ansia al lettore,
 - contenuto che promette vincite, premi, etc.

È importante non fornire mai le informazioni richieste tramite la compilazione di form, scaricando allegati o cliccando sul contenuto della mail.

Se il mittente è noto è necessario prestare attenzione alle modalità di dialogo e allertarsi se le stesse sono diverse da quelle normalmente utilizzate dall'interlocutore.

In caso di dubbi, contattare il mittente via telefono per accertarsi della veridicità del messaggio.

- **Non fornire mai informazioni riguardanti codici e password via mail.** Qualora ciò risulti essenziale, la comunicazione dovrà avvenire secondo le indicazioni fornite dalla Direzione.
- **Fare attenzione agli allegati**, in particolare qualora presentino estensioni pericolose o sospette (.exe, .bat, etc.). In tal caso procedere immediatamente all'eliminazione dei messaggi, senza aprire o salvare i file sospetti.
- **Fare attenzione ai link presenti nel testo della e-mail.** Passare il mouse e leggere bene il link sottostante per verificare se vi sono elementi di allerta.
- **In caso di dubbi, contattare il CED.**

Nell'eventualità di assenza prolungata ma programmata (o comunque prevedibile), si invita tutto il personale ad attivare la funzionalità di sistema che permette di inviare una risposta automatica ai messaggi ricevuti: nel messaggio di risposta è possibile indicare il nominativo di uno o più soggetti all'interno della struttura organizzativa, cui è possibile rivolgersi in assenza del diretto interessato.

In caso di assenza prolungata e improvvisa, l'attivazione della funzione di cui al paragrafo precedente potrà essere richiesta al CED.

In caso di violazione o inadempimento di quanto riportato al punto 4 in merito all'utilizzo della rete Internet, il CED, sentita la Direzione, procederà ad impedire all'utente la possibilità di collegamento ad Internet e ne darà comunicazione alla Direzione del Personale per l'eventuale accertamento di responsabilità disciplinari, in caso di personale dipendente, o contrattuali in caso di professionisti e/o collaboratori.

5. Assegnazione e gestione delle credenziali di autenticazione

Le credenziali di autenticazione per l'accesso al PC, la connessione alla rete e/o per l'accesso ai diversi applicativi, vengono assegnate al dipendente o al collaboratore dal CED, in seguito a specifica richiesta proveniente dalla Direzione, dal Responsabile Risorse Umane o su proposta del RdF, approvata dalla

Direzione, nell'ambito della quale il nuovo utente verrà inserito ed andrà ad operare (istruzione operativa 07 20 e relativa modulistica).

Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (user id), associato ad una parola chiave (password) riservata che dovrà essere gestita dall'incaricato con la massima diligenza e non divulgata. Le caratteristiche principali di tale sistema sono riepilogate di seguito.

1. Consiste in un codice per l'identificazione (ID) e una parola chiave (password);
2. La password è conosciuta solo dall'incaricato;
3. E' composta, preferibilmente e comunque in relazione alle possibilità offerte dai singoli sistemi, da almeno 8 caratteri, comprende lettere maiuscole e minuscole e da almeno un numero ed un carattere speciale e non contiene riferimenti facilmente riconducibili all'incaricato (nome, cognome, data di nascita ecc.);
4. Viene modificata al primo utilizzo (vedi punto 2);
5. Viene modificata almeno ogni sei mesi (nel caso di dati sensibili almeno ogni tre mesi);
6. Il codice di autenticazione (ID) non può essere assegnato ad altri incaricati, neppure in tempi diversi;
7. Le credenziali di autenticazione (ID e password) non utilizzate da almeno 6 mesi vanno disattivate;
8. Le credenziali vanno disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali;
9. Agli incaricati sono impartite istruzioni per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.

Per garantire la segretezza delle credenziali e la sicurezza durante le sessioni di trattamento dei dati, per ogni utente è opportuno:

- Evitare di scrivere qualunque password su carta
- Non lasciare accessibile l'elaboratore durante una sessione di trattamento dei dati (vedi punto successivo);
- Impostare uno screen saver dotato di password (con tempi di avvio brevi) che blocchi l'accesso all'elaboratore in caso sia necessario allontanarsi per un tempo prolungato;
- Qualora l'elaboratore sia utilizzato da più incaricati, ricordarsi, sempre al termine del lavoro effettuato, di disconnettersi dal sistema. In questo modo la persona che utilizzerà il PC in seguito dovrà comunque effettuare la procedura di autenticazione.

6. Accesso Remoto tramite Dispositivi Personali (BYOD)

La Casa di Cura mette a disposizione di dipendenti, professionisti e collaboratori, la possibilità, per comprovate motivazioni legate allo svolgimento delle proprie mansioni, di collegarsi ai sistemi informativi aziendali da remoto tramite l'utilizzo di dispositivi personali.

Si riepilogano di seguito le regole che disciplinano tali accessi, volte a garantire la sicurezza dei dati e la continuità operativa.

1. Autorizzazione

L'attivazione dell'accesso da remoto (basata sull'utilizzo di OpenVPN) è soggetta all'autorizzazione da parte della Direzione, sentito il parere del Responsabile di Funzione coinvolto e del CED. L'autorizzazione è documentata da apposito documento scritto, che viene firmato, da parte dell'utente autorizzato, anche ai fini dell'accettazione del contenuto della presente policy

2. Ambito di Applicazione

La presente policy si applica a:

- Tutti i dipendenti, consulenti e collaboratori esterni
- Smartphone, tablet, PC fissi, notebook personali ed altre tipologie di device che possono consentire il collegamento ai sistemi informativi aziendali
- Qualsiasi connessione remota indipendentemente dal luogo dalla quale viene attivata.

3. Requisiti Obbligatori del Dispositivo

Prima di effettuare l'accesso, l'utente deve verificare che il proprio dispositivo sia conforme ai seguenti standard:

- Sistema Operativo: Utilizzare versioni aggiornate e supportate dal produttore.
- Antivirus: Installare un software antivirus attivo con aggiornamenti automatici abilitati.
- Blocco Schermo: Attivare il blocco automatico dopo massimo 5 minuti di inattività.
- Autenticazione: Impostare un PIN sicuro, password complessa o riconoscimento biometrico.

4. Modalità di Connessione Sicura

L'accesso ai dati aziendali deve avvenire esclusivamente tramite i canali ufficiali predisposti:

- Utilizzo della VPN: Obbligatorio attivare la VPN aziendale prima di accedere a qualsiasi servizio interno.
- Multi-Factor Authentication (MFA): Obbligatorio configurare e utilizzare l'autenticazione a due fattori. La soluzione in uso presso la Casa di Cura prevede l'utilizzo di un certificato di sicurezza da installare in locale, abbinato ad una password che il singolo utente deve utilizzare per potersi collegare.
- Reti Sicure: Vietato l'accesso da reti Wi-Fi pubbliche o aperte senza l'uso della VPN aziendale.

5. Regole di Comportamento e Divieti

Per prevenire la perdita o il furto di informazioni sensibili, è severamente vietato:

- Salvataggio Locale: Non scaricare o memorizzare dati aziendali sulla memoria locale del dispositivo personale.
- Condivisione: Impedire a familiari o terzi l'utilizzo del dispositivo mentre si è connessi ai sistemi aziendali.
- Uso di Cloud Terzi: Vietato trasferire documenti di lavoro su account cloud personali (es. Google Drive o Dropbox privati).

- Credenziali: Non salvare le password aziendali nei browser personali.

Al fine di consentire il corretto svolgimento dei processi di backup, gli accessi da remoto sono consentiti dal lunedì al sabato nella fascia dalle ore 7.30 alle ore 22.00

6. Gestione degli Incidenti

In caso di smarrimento, furto del dispositivo o sospetto di compromissione informatica:

- L'utente deve informare il CED entro un massimo di 2 ore dall'evento.
- L'azienda si riserva il diritto di revocare immediatamente le credenziali di accesso.

7. Protezione Antivirus

Il sistema informatico dell'azienda è protetto da software antivirus aggiornato. Ogni utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale mediante virus o mediante ogni altro software aggressivo.

Nel caso il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente sospendere ogni elaborazione in corso senza spegnere il computer nonché segnalare prontamente l'accaduto al personale del CED.

8. Istruzioni sull'utilizzo di strumenti per la comunicazione di dati ed informazioni personali e/o sullo stato di salute dei pazienti

Sempre con maggior frequenza, nella normale routine lavorativa, i singoli operatori possono trovarsi nella condizione di trasmettere o condividere, anche grazie all'utilizzo di device tecnologici (spesso di proprietà personali quali gli smartphone) dati o informazioni personali e/o sullo stato di salute.

Le istruzioni sotto riportate, trovano quindi applicazione nei casi in cui la trasmissione avvenga attraverso l'utilizzo di fax, telefono, e-mail, piattaforme di comunicazione o scambio di dati fruibili via internet, applicazioni da smartphone o altro device (anche di personale proprietà dell'utilizzatore), o, in ogni caso, con strumenti e modalità per i quali non sia stata emanata apposita regolamentazione nazionale, regionale o da parte degli enti preposti.

Linee-guida

- L'utilizzo di strumenti quali fax, telefono, e-mail, applicazioni smartphone ecc. per la comunicazione di informazioni personali e/o sullo stato di salute, andrebbe limitato ai soli casi in cui tale comunicazione è **strettamente indispensabile**, per finalità diagnostiche o per consentire, o facilitare, l'erogazione di prestazioni sanitarie;
- Nell'utilizzare tali strumenti è necessario **verificare con particolare attenzione** i dati che identificano il **destinatario** (numero di telefono o fax, indirizzo e-mail ecc.), evitando che la trasmissione, anche solo per errore, possa avvenire ad un soggetto diverso da quello cui la stessa è rivolta;
- Nel caso di trasmissioni via fax è necessario utilizzare l'apposita **cover** predisposta dalla Casa di Cura che riporta espressamente le relative note di riservatezza
Nel caso di trasmissione via fax è buona norma **accertarsi della corretta ricezione** dello stesso da parte del destinatario;
- Ove possibile (in particolar modo per quanto concerne fotografie, immagini iconografiche ecc.), se non significativo, è sempre opportuno **rendere anonima la trasmissione**, tralasciando od oscurando gli eventuali dati anagrafici del paziente;

- Una volta **trasmesso il messaggio** (in particolar modo nel caso di utilizzo di applicazione da smartphone) è opportuno **procedere alla sua cancellazione**;
- In caso di utilizzo di smartphone personali per l'invio di tali comunicazioni, si raccomanda di attivare procedure che consentano la cancellazione da remoto del contenuto del device in caso di smarrimento o furto.

9. Compiti e responsabilità

Responsabilità degli utenti:

Ogni utente è responsabile della propria postazione informatica, della propria casella di Posta Elettronica e del contenuto dei messaggi da essa inviati.

E' inoltre responsabile della segretezza delle credenziali di accesso alla rete ed ai software al cui utilizzo è stato autorizzato. L'utente si impegna a comunicare alla Direzione ed al CED, non appena ne venisse a conoscenza, qualsiasi uso non autorizzato da parte di terze persone delle risorse informatiche della Casa di Cura, così come ogni sospetto di effrazione, incidente, abuso o violazione della sicurezza di tali strumenti.

Gli utenti sono responsabili per la protezione dei dati utilizzati e/o memorizzati nei sistemi in cui hanno accesso; è fatto loro divieto di accedere direttamente o indirettamente a directory, files e servizi non espressamente e preventivamente autorizzati dalla Casa di Cura.

Gli utenti sono tenuti a mantenersi aggiornati, prendendo visione delle eventuali direttive emanate dalla Direzione o dal CED e divulgate tramite e-mail o circolare.

I responsabili delle Unità Operative e/o Servizi Aziendali dovranno adottare misure idonee per un corretto utilizzo delle risorse informatiche messe a disposizione della loro struttura, esercitando una funzione di istruzione, indirizzo e controllo sugli utenti incaricati ed individuando con precisione le responsabilità per la gestione dei dati, dei salvataggi e delle risorse stesse.

Responsabilità e compiti del CED:

Della gestione delle risorse informatiche è responsabile il CED, il quale è tenuto a:

- Adottare le misure più idonee a garantire continuità, disponibilità e sicurezza del servizio
- Gestire i dati degli utenti nel rispetto della vigente normativa sulla tutela dei dati personali
- Informare tempestivamente gli utenti con anticipo di eventuali fermi o interruzioni di servizio che si rendessero necessari per manutenzione o per cause di forza maggiore
- Monitorare i canali di comunicazione del CSIRT Italia al fine di acquisire, analizzare e rispondere alle informazioni sulle vulnerabilità.
- Monitorare i livelli di servizio al fine di garantire la massima efficienza
- Garantire la funzionalità tecnica

In particolare cura:

1. l'attribuzione e la revoca di account e di password e la gestione dei livelli di accesso.
2. l'individuazione delle risorse informatiche e software relativamente agli acquisti ed il collaudo di tutte le attrezzature informatiche, telematiche e software.

3. l'assegnazione – sulla base di quanto stabilito dalla Direzione - degli accessi ad internet sulla base delle effettive necessità e compatibilmente con la banda minima da garantire per le normali attività dell'azienda.
4. la configurazione e l'amministrazione delle risorse informatiche e reti. Per risorse informatiche si intendono:
 - workstation, personal computer, notebook, stampanti utilizzati da dipendenti, personale con incarichi professionali, stagisti, tirocinanti ed eventuali ospiti;
 - tutte le macchine facenti comunque parte della rete;
 - apparati di rete;
 - tutto il software e i dati acquistati o prodotti per l'amministrazione dei sistemi, per l'utilizzo da parte degli utenti o di terzi autorizzati.
5. la revoca dell'accesso temporaneo alla risorsa Informatica e di rete, sentita la Direzione, qualora questo sia utilizzato impropriamente o in violazione delle leggi vigenti; potrà altresì interrompere temporaneamente la prestazione del servizio in presenza di motivati problemi di sicurezza, riservatezza o guasto tecnico, dandone tempestiva comunicazione all'utente.
6. l'Attivazione/disattivazione, sentita la Direzione o su indicazione di questa, delle caselle di Posta Elettronica.

Al fine di agevolare e tracciare le attività sopra elencate, la Casa di Cura, nell'ambito dell'istruzione operativa 07 20, ha adottato apposita modulistica con la quale il Responsabile Risorse Umane (su eventuale sollecitazione del Responsabile di Funzione coinvolto ed eventuale coinvolgimento del CED) comunica le assunzioni/cessazioni o le collaborazioni attivate/cesstate, da cui dipendano attività di attribuzione/revoca di account di rete, credenziali di accesso a software o caselle di posta elettronica.

Il CED può accedere in qualsiasi momento, anche senza preavviso, ai locali e alle risorse informatiche della Casa di Cura, sia in caso di emergenza, sia per effettuare gli interventi di assistenza, verifica e supporto.

Il CED non effettua alcuna misura, controllo, censura, modifica, cancellazione di messaggi sul server di posta elettronica tranne quando ciò è legato a:

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

Vige l'assoluto divieto di effettuare controlli con le seguenti modalità:

- la lettura e la registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio e-mail;
- la lettura e la registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo;
- l'analisi occulta di computer portatili affidati in uso.

10. Controlli

I controlli inerenti il rispetto delle norme sopra indicate saranno svolti in conformità alla legge, anche saltuari o occasionali, sia per eseguire verifiche sulla funzionalità e sicurezza del sistema, sia per verificare il

corretto utilizzo da parte degli utenti (dipendenti, collaboratori ecc.) tanto della rete internet che della posta elettronica.

Nell'esercizio del potere di controllo la Casa di Cura si atterrà al principio generale di proporzionalità e non eccedenza delle attività di controllo, rispettando le procedure di informazione/consultazione delle rappresentanze dei lavoratori previste dai contratti collettivi e informerà preventivamente i lavoratori dell'esistenza di dispositivi di controllo atti a raccogliere i dati personali.

In ogni caso, nell'espletare le attività di controllo, sarà tenuto in debita considerazione che le informazioni trattate ed oggetto di verifica possono riguardare, oltre all'attività lavorativa, anche la sfera personale e la vita privata di lavoratori e di terzi.

I controlli si svolgeranno in forma graduale:

1. In via preliminare l'azienda provvederà ad eseguire dei controlli su dati aggregati, riferiti all'intera struttura lavorativa ovvero a sue aree e dunque ad un controllo anonimo, che può concludersi con un avviso generalizzato relativo ad un rilevato utilizzo anomalo degli strumenti aziendali e con l'invito ad attenersi scrupolosamente a compiti assegnati e istruzioni impartite. L'avviso può essere circoscritto a dipendenti afferenti all'area o settore in cui è stata rilevata l'anomalia.
2. In assenza di successive anomalie non si effettueranno controlli su base individuale;
3. Nel perdurare delle anomalie si procederà a controlli su base individuale, o per postazioni di lavoro, e in caso di abusi singoli e reiterati si eseguiranno controlli nominativi o su singoli dispositivi e/o postazioni di lavoro (inoltrando preventivi avvisi collettivi o individuali ed indicando le ragioni legittime, specifiche e non generiche, per cui i controlli verrebbero effettuati e le relative modalità operative);
4. Nel caso in cui la posta elettronica e la rete Internet siano utilizzate indebitamente, o di riscontrato e reiterato uso non conforme delle risorse informatiche, il CED, che effettua i controlli, segnalerà il comportamento alla Direzione, che valuterà se attivare eventuali procedimenti disciplinari nelle forme e con le modalità previste dal C.C.N.L. e dallo specifico regolamento aziendale ed in conformità dell'art. 7 della Legge 300/1970;
5. Per il personale non dipendente cui non è ovviamente applicabile il C.C.N.L. il comportamento andrà sempre segnalato alla Direzione per l'adozione degli atti di specifica competenza.

11. Interruzione e cessazione d'ufficio del servizio

Ai sensi del presente regolamento, le credenziali di accesso alla rete, a specifici software, così come l'utilizzo del servizio di accesso ad Internet e di utilizzo della posta elettronica, cessano d'ufficio nei seguenti casi:

- se non sussiste più la condizione di dipendente o collaboratore autorizzato o non è confermata l'autorizzazione all'uso;
- se è accertato un uso non corretto delle risorse informatiche da parte dell'utente o comunque un uso estraneo ai suoi compiti professionali;
- se vengono sospettate manomissioni e/o interventi sul hardware e/o sul software da parte dell'utente, eventualmente per il tramite di personale non autorizzato;

- in caso di diffusione o comunicazione, imputabili direttamente o indirettamente all'utente, di password e/o altre informazioni tecniche riservate;
- in caso di accesso doloso dell'utente a directory, a siti e/o file e/o servizi da chiunque resi disponibili non rientranti fra quelli per lui autorizzati e in ogni caso qualora l'attività dell'utente comporti danno, anche solo potenziale;
- in ogni altro caso in cui sussistono ragionevoli evidenze di una violazione degli obblighi dell'utente.

12. Disposizioni finali

1. Il presente Regolamento è sottoposto a revisione annuale ovvero ogni qual volta il mutamento delle condizioni operative e/o organizzative lo rendesse necessario;
2. La sua pubblicazione avviene sulla rete aziendale in "collegamento a qualità" nella sottocartella privacy, nonché mediante affissione nei luoghi di lavoro con modalità analoghe a quelle previste dall'art. 7 dello Statuto dei lavoratori;
3. E' fatto obbligo a tutto il personale dipendente ed a tutti i collaboratori della Casa di Cura, l'osservanza delle norme di cui si compone;
4. Poiché in caso di violazioni contrattuali e giuridiche, sia l'azienda, sia il singolo lavoratore sono potenzialmente perseguibili con sanzioni disciplinari, civili e penali, l'azienda verificherà, nei limiti consentiti dalle norme legali e contrattuali, secondo quanto previsto dal presente Regolamento, il rispetto delle regole e l'integrità del proprio sistema informatico.