CENTRO NEUROLESI BONINO PULEJO

REGOLAMENTO INTERNO SULL' UTILIZZO DEGLI STRUMENTI AZIENDALI

INDICE

PREMESSA

Le disposizioni del presente Regolamento disciplinano l'utilizzo delle risorse aziendali (informatiche, telematiche ecc...) dell'IRCCS Centro Neurolesi Bonino Pulejo di Messina, da parte del personale dipendente e degli altri operatori abilitati, tenuto conto delle seguenti finalità e principi:

- l'uso delle tecnologie informatiche, telefoniche e telematiche, che ha consentito l'introduzione di innovative tecniche di gestione delle attività, ha dato origine a numerose problematiche relative all'utilizzo di questi strumenti forniti dall'Istituto ai propri collaboratori per lo svolgimento delle mansioni e dei compiti loro affidati;
- le implicazioni in termini di sicurezza, disponibilità ed integrità dei sistemi informatici dell'IRCCS;
- prevenire comportamenti inconsapevoli che possano innescare problemi o minacce alla sicurezza dei sistemi aziendali e nel trattamento dei dati.
- 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;
- è fortemente sentita la necessità di porre in essere adeguati sistemi di controllo sull'utilizzo di tali strumenti da parte degli operatori nel rispetto dei criteri e dei principi stabiliti dal Garante per la protezione dei dati personali e di valutare conseguentemente gli usi scorretti che, oltre ad esporre l'Istituto stesso a rischi, tanto patrimoniali quanto penali, possono di per sé considerarsi contrari ai doveri di diligenza e fedeltà previsti dagli artt. 2104 e 2105 del Codice Civile;
- i controlli sull'uso di questi strumenti deve garantire sia il diritto della P.A. di proteggere la propria organizzazione, essendo i computer, gli applicativi per la gestione delle diverse attività, i telefoni aziendali e gli altri mezzi strumenti di lavoro, la cui utilizzazione personale è preclusa, sia il diritto del lavoratore a non vedere invasa la propria sfera personale, il diritto alla riservatezza ed alla dignità come sanciti dallo Statuto dei lavoratori (legge n. 300/1970) e dal Codice sul trattamento dei dati personali (D.Lgs. n. 196/2003) nonché dal Regolamento europeo in materia (Reg. (CE) 27.4.2016, n. 2016/679/UE);
- informare gli interessati sulle finalità dell'utilizzo degli strumenti informatici, del controllo e sulle specifiche metodologie adottate per effettuarlo;
- sensibilizzare gli interessati al rispetto della normativa sulla tutela legale del software;
- l'utilizzo delle risorse e dei servizi informatici e di rete è subordinato al rispetto da parte degli operatori delle norme civili, penali e amministrative applicabili.

L'IRCCS attraverso questo regolamento adotta una procedura interna diretta ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla sicurezza nel trattamento dei dati.

1. UTILIZZO DEL PERSONAL COMPUTER

Il Personal Computer affidato al dipendente è uno **strumento di lavoro**. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.
L'accesso all'elaboratore è protetto da password che deve essere custodita dall'incaricato con la massima diligenza e non divulgata.
Non è consentito installare autonomamente programmi provenienti dall'esterno senza l'autorizzazione esplicita del *Responsabile dei sistemi informatici aziendali*, in quanto sussiste il grave pericolo di portare Virus informatici e di alterare la stabilità delle applicazioni dell'elaboratore.
L'inosservanza della precedente disposizione espone sia l'Istituto sia l'utente a gravi responsabilità civili; inoltre 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 non protetto dal diritto d'autore, sono sanzionate penalmente.
Non è consentito l'uso di programmi diversi da quelli distribuiti ed installati ufficialmente dal *Responsabile dei sistemi informatici*. L'inosservanza di questa disposizione, infatti, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre l'azienda a gravi responsabilità civili ed anche penali in caso di violazione 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.
Non è consentito all'utente modificare le caratteristiche impostate sul proprio PC, salvo autorizzazione esplicita del *Responsabile dei sistemi informatici aziendali*.
Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio. 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. In ogni caso deve essere attivato lo screen saver e la relativa password.
Non è consentita l'installazione sul proprio PC di alcun dispositivo di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, ecc.), se non con l'autorizzazione espressa del *Responsabile dei sistemi informatici aziendali*.
Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il *Responsabile dei sistemi informatici aziendali* nel caso in cui vengano rilevati virus.
Nel personal computer **non devono essere presenti file personali**, quali ad esempio fotografie, file musicali, file video, file di attività extra lavorative. L'Azienda può monitorare la tipologia di file presenti e procede, senza nessun preavviso, alla rimozione degli stessi. Durante le operazioni di cambio / sostituzione del personal computer (ammodernamento del parco macchine), il tecnico addetto alla sostituzione rimuoverà, se presenti, tutti i file non inerenti all'attività lavorativa.
Il personale incaricato, anche dei servizi esternalizzati, che opera presso i Sistemi Informativi **è autorizzato a compiere interventi nel sistema informatico aziendale** diretti a garantire la sicurezza e la salvaguardia del sistema stesso, nonché per ulteriori motivi tecnici e/o manutentivi (quali aggiornamento, sostituzione, implementazione di programmi, manutenzione hardware, alto). Detti interventi potranno comportare l'accesso in qualunque momento ai dati trattati da ciascun utente, ivi compresi gli archivi di posta elettronica, nonché alla verifica sui siti internet acceduti dagli utenti abilitati alla navigazione esterna. Analogamente, sempre ai fini di sicurezza del sistema e per garantire la corretta operatività delle attività istituzionali, si procede in caso di assenza prolungata od impedimento dell'utente.
Il personale incaricato del servizio di assistenza ai Sistemi Informativi e dei **servizi affidati in outsourcing è autorizzato a collegarsi e visualizzare in remoto** -previa autorizzazione da parte del personale che opera presso i sistemi informativi, e previa comunicazione all'utente - il desktop delle singole postazioni di personal computer al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza contro virus, spyware, malware, e simili. 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, fatta salva l'urgenza di procedere per non pregiudicare l'efficacia dell'intervento, verrà data comunicazione della necessità dell'intervento stesso.

2. UTILIZZO DELLA RETE

Le unità di rete sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità, vengono svolte regolari attività di controllo, amministrazione e backup.
Le password d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite. **È assolutamente proibito entrare nella rete e nei programmi con altri nomi utente.**
Il *Responsabile dei sistemi informatici aziendali* può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la Sicurezza sia sui PC degli incaricati sia sulle unità di rete.
Costituisce buona regola la periodica (almeno ogni sei mesi) **pulizia degli archivi**, ovviamente nel rispetto del regolamento di conservazione e scarto adottato dall'IRCCS, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. È infatti assolutamente da evitare un'archiviazione ridondante.
È cura dell'utente effettuare la stampa dei dati solo se strettamente necessaria e di ritirarla prontamente dai vassoi delle stampanti comuni.
È compito di ciascun utente, per quanto di propria competenza e secondo i canoni della diligenza, **preservare i dati, le notizie e le informazioni aziendali** che circolano nella rete informatica dalla conoscibilità di terzi soggetti non espressamente autorizzati ad averne notizia.
I sistemi di teleassistenza remota sono permessi solo tramite VPN, preventivamente autorizzata dai Sistemi Informativi. Altre modalità potranno essere valutate per i singoli casi

3. GESTIONE DELLE PASSWORD

Le password di ingresso alla rete, di accesso ai programmi e dello screen saver, sono previste ed attribuite dal *Responsabile dei sistemi informatici aziendali*.
È necessario procedere alla **modifica della password almeno ogni sei mesi**; nel caso di trattamento di dati particolari (ex dati sensibili) e di dati giudiziari la periodicità della variazione deve essere ridotta a tre mesi.
Le password possono essere formate da lettere (maiuscole o minuscole) e numeri ricordando che lettere maiuscole e minuscole hanno significati diversi per il sistema; devono essere composte da almeno otto caratteri e non deve contenere riferimenti agevolmente riconducibili all'autorizzato al trattamento.
La password deve essere immediatamente sostituita, dandone comunicazione al *Responsabile dei sistemi informatici aziendali*, nel caso si sospetti che la stessa abbia perso la segretezza.
Qualora l'utente venisse a conoscenza delle password di altro utente, è tenuto a darne immediata notizia alla Direzione o al *Responsabile dei sistemi informatici aziendali*.

4. UTILIZZO DEI SUPPORTI MAGNETICI

Tutti i supporti magnetici riutilizzabili (dischetti, cassette, pen drive) contenenti dati particolari (ex dati sensibili) e giudiziari devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato. Una persona esperta potrebbe infatti recuperare i dati memorizzati anche dopo la loro cancellazione. E' **necessario crittografare i dati** in essi contenuti. I supporti magnetici contenenti dati particolari (ex dati sensibili) e giudiziari devono essere custoditi in archivi chiusi a chiave.
Al fine di assicurare **la distruzione e/o inutilizzabilità di supporti magnetici** e digitali rimovibili contenenti dati sensibili, ciascun utente dovrà contattare il personale del servizio di assistenza ai Sistemi Informativi e seguire le istruzioni da questo impartite.

5. UTILIZZO DI PC PORTATILI

L'utente è responsabile del PC portatile assegnatogli dal *Responsabile dei sistemi informatici aziendali* e **deve custodirlo con diligenza** sia durante gli spostamenti sia durante l'utilizzo nel

luogo di lavoro.
Ai PC portatili si applicano le regole di utilizzo previste per i Pc connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna.
I PC portatili utilizzati all'esterno (convegni, visite in azienda, ecc...), in caso di allontanamento, devono essere custoditi in un luogo protetto.
Le disposizioni del presente articolo si applicano anche nei confronti di incaricati esterni quali consulenti, collaboratori, altro.

6. USO DELLA POSTA ELETTRONICA

La casella di posta, assegnata dall'Azienda all'utente, è uno **strumento di lavoro.** Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.
È fatto divieto di utilizzare le caselle di posta elettronica aziendale (_____@irccsme.it) per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail-list salvo diversa ed esplicita autorizzazione.
È buona norma evitare messaggi completamente estranei al rapporto di lavoro o alle relazioni tra colleghi. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.
La documentazione elettronica che costituisce per l'azienda "know how" aziendale tecnico o commerciale protetto, e che, quindi, viene contraddistinta da diciture od avvertenze dirette ad evidenziarne il carattere riservato o segreto, non può essere comunicata all'esterno senza preventiva autorizzazione della Direzione.
Per la trasmissione di file all'interno dell'IRCCS è possibile utilizzare la posta elettronica, prestando attenzione alla dimensione degli allegati.
È obbligatorio controllare i file attachements di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).
È vietato inviare catene telematiche (o di Sant'Antonio). Se si dovessero ricevere messaggi di tale tipo, si deve comunicarlo immediatamente al *Responsabile dei sistemi informatici aziendali*. Non si devono in alcun caso attivare gli allegati di tali messaggi.
È obbligatorio mantenere il **seguente schema tipo** per la firma in calce, inclusa la clausola di riservatezza delle informazioni:
Cognome Nome
Ruolo (opzionale)
IRCCS Messina
tel._____
CLAUSOLA DI RISERVATEZZA: "*Il contenuto della presente comunicazione è strettamente riservato, essendo indirizzato esclusivamente al destinatario sopra individuato e potendo contenere informazioni strettamente personali e/o confidenziali. Qualora fosse pervenuto a soggetto diverso dal destinatario questi deve intendersi sin d'ora avvisato che qualsiasi forma di diffusione dei dati, dei fatti e delle notizie apprese è assolutamente vietata. Si chiede cortesemente di cancellare il messaggio erroneamente ricevuto dal proprio sistema, dopo aver notificato al mittente l'errore commesso*".

7. USO DELLA RETE INTERNET E DEI RELATIVI SERVIZI

Il PC abilitato alla navigazione in Internet costituisce uno strumento aziendale necessario allo svolgimento della propria attività lavorativa. **È assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa** stessa.
È fatto divieto all'utente di scaricare (downlod) software gratuito (freeware) e shareware prelevato da siti Internet, se non espressamente autorizzato dal *Responsabile dei sistemi informatici aziendali*.
Al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa, l'Istituto può adottare uno specifico sistema di blocco o filtro automatico per prevenire determinate operazioni quali l'upload o l'accesso a determinati siti inseriti in una **black list.**
È tassativamente vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili salvo i casi direttamente autorizzati dalla

Direzione e con il rispetto delle normali procedure di acquisto.
È da evitare ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa. È vietata la partecipazione a Forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames).

8. UTILIZZO DI TELEFONO, FAX, SCANNER E FOTOCOPIATRICI AZIENDALI

Il telefono aziendale affidato all'utente è uno strumento di lavoro.
Ne viene concesso l'uso esclusivamente per lo svolgimento dell'attività lavorativa, non essendo quindi consentite comunicazioni a carattere personale o comunque non strettamente inerenti l'attività lavorativa stessa. La ricezione o l'effettuazione di telefonate personali è consentita solo nel caso di comprovata necessità ed urgenza, mediante il telefono aziendale a disposizione.
Al cellulare aziendale si applicano le medesime regole sopra previste per l'utilizzo del telefono fisso aziendale. In particolare è vietato l'utilizzo del telefono cellulare messo a disposizione per inviare o ricevere SMS o MMS di natura personale o comunque non pertinenti allo svolgimento dell'attività lavorativa. L'eventuale uso promiscuo (anche per fini personali) del telefono cellulare aziendale è possibile soltanto in presenza di preventiva autorizzazione scritta e in conformità delle istruzioni al riguardo impartite digitando il prefisso per l'addebito delle chiamate personali.
È vietato l'utilizzo dei fax aziendali per fini personali sia per spedire sia per ricevere documentazione, salva diversa esplicita autorizzazione da parte del responsabile della funzione/unità organizzativa.
È vietato l'utilizzo di scanner aziendali per fini personali, salvo preventiva ed esplicita autorizzazione da parte del responsabile della funzione/unità organizzativa.
È vietato l'utilizzo delle fotocopiatrici aziendali per fini personali, salvo preventiva ed esplicita autorizzazione da parte del responsabile della funzione/unità organizzativa. Nel caso di utilizzo per fini lavorativi dovranno essere osservate le seguenti regole:

A) Effettuare copie solo dei documenti per i quali è richiesto. Evitare di fare duplicati inutili;
B) Ritirare i documenti stampati o fotocopiati in un tempo ragionevole per permettere anche agli altri operatori di fruire degli strumenti senza inutili ritardi;
C) Non lasciare incustoditi i documenti all'interno delle fotocopiatrici perché potrebbe configurarsi una diffusione illecita dei dati.

9. OSSERVANZA DELLE DISPOSIZIONI IN MATERIA DI PROTEZIONE DATI PERSONALI

È obbligatorio attenersi alle disposizioni in materia di protezione dati personali ai sensi del GDPR 2016/679, del Codice della Privacy 196/2003, dei provvedimenti del Garante della Privacy e di altre disposizioni ad essi collegati.

10. NON OSSERVANZA DELLA NORMATIVA AZIENDALE

Il mancato rispetto o la violazione delle regole contenute nel presente regolamento è perseguibile con provvedimenti disciplinari nonché con le azioni civili e penali consentite.

11. AGGIORNAMENTO E REVISIONE

Il presente Regolamento entra in vigore a decorrere dalla data di approvazione del relativo provvedimento di adozione ed è soggetto a revisione.

Il Direttore Amministrativo
Avv. Maria Felicita Crupi

Il Direttore Generale
Dott. Vincenzo Barone