REGOLAMENTO
PER L'USO DEGLI STRUMENTI INFORMATICI

1.0 Premessa e finalità

L'osservanza dei principi di correttezza e diligenza nel contesto lavorativo è un presupposto fondamentale per il valido utilizzo delle risorse informatiche e telematiche del Policlinico.
L'Ospedale Policlinico San Martino, titolare esclusivo dei diritti connessi ai propri sistemi informativi (dati compresi), fornisce ai dipendenti (o altri collaboratori autorizzati), le strumentazioni ritenute necessarie per l'espletamento del lavoro.

Pertanto l'Ospedale Policlinico San Martino provvede:

- All'adozione delle regole interne di comportamento preordinate ad evitare condotte inconsapevoli o scorrette durante l'attività lavorativa in merito agli strumenti informatici (questo documento in particolare)
- Alla predisposizione di un'informativa sul trattamento dei dati da fornire agli interessati secondo gli obblighi di trasparenza previsti dal Regolamento UE 2016/679.
- Alla predisposizione delle misure minime di sicurezza idonee per garantire l'integrità e la sicurezza dei dati e dei sistemi.

Questo documento contiene un insieme di regole di comportamento per il corretto utilizzo degli strumenti informatici messi a disposizione dall' Ospedale Policlinico San Martino per i propri operatori.
Le regole contenute in questo documento sono riferite prevalentemente al trattamento dei dati con sistemi informatici, ma si possono ritenere adeguate anche per il trattamento dei dati mediante supporti tradizionali (carta, …).
Con questo documento vengono fornite le indicazioni a cui attenersi per non venire meno agli obblighi imposti dal codice sulla privacy e dalle altre normative a tutela dell'integrità dei sistemi e dei dati del Policlinico e per garantire le misure minime di sicurezza sugli stessi.

Si tratta per la maggior parte di norme comportamentali a cui deve attenersi tutto il personale che, a qualsiasi titolo, intrattenga rapporti con il Policlinico (dipendenti, collaboratori esterni, specializzandi, borsisti, convenzionati, ecc.).
Seguendo queste indicazioni, oltre a impedire che il Policlinico incorra in uno dei divieti sanciti dalla norma, gli incaricati del trattamento di dati personali eviteranno anche un loro coinvolgimento diretto, con possibili **conseguenze disciplinari, amministrative e penali,** così come previsto dalla norma e/o da altri regolamenti e atti del Policlinico, contribuendo a ridurre la possibilità di subire attacchi di natura informatica.

2.0 Sigle

ICT**:** U.O. Information & Communication Technologies

3.0 Modifiche alla revisione precedente

Capitolo/Paragrafo modificato	Descrizione della modifica
1.0 e segg.	Revisione complessiva sia per cambio ragione sociale dell'Ospedale e nome dell'UO HSI sia per contenuti.
4.0	Revisione dei contenuti
5.0	Revisione dei contenuti
6.0	Revisione dei contenuti alla luce del DPR 81/2023

4.0 Descrizione attività

4.1 Le principali linee guida di comportamento

Le risorse informatiche (che comprendono i computer desktop, i pc portatili, i telefoni, i cellulari, le attrezzature periferiche e di rete, i programmi o software, i dati e i supporti):

- sono parte integrante del patrimonio dell'Ospedale Policlinico San Martino.
- devono essere utilizzate esclusivamente per scopi legati al Policlinico e di servizio, secondo le finalità per cui sono rese disponibili agli operatori (fatte salve le eventuali autorizzazioni specifiche).
- devono essere rese disponibili solo alle persone autorizzate, esplicitamente (in seguito ad un atto di nomina a "incaricato del trattamento"), o implicitamente, (poiché appartenenti a un determinato profilo di autorizzazione).
- devono essere protette da danneggiamenti, furti e altre cause che possano comprometterne l'utilizzo e interrompere l'operatività delle attività cui sono destinate
- non devono essere usate per compromettere la sicurezza e la riservatezza del Sistema Informativo, per pregiudicare ed ostacolare le attività del Policlinico e non possono essere destinate al perseguimento di interessi privati in contrasto con quelli del Policlinico.

4.2 I principali divieti

- Introdursi abusivamente nei sistemi informatici del Policlinico o di soggetti esterni.
- Fornire ad altri le proprie credenziali di identificazione ed autenticazione (user e password, PIN smart card). La password, così come le smart card ed i PIN per la firma digitale sono strettamente personali.
- Procurare a sé o ad altri profitto, o arrecare danni al Policlinico, procurandosi, riproducendo, diffondendo o consegnando credenziali di autenticazione ovvero codici, parole chiave/passwords o altri mezzi idonei all'accesso ai sistemi informatici del Policlinico o di soggetti esterni.
- Intercettare, modificare, impedire, interrompere le comunicazioni inerenti ai sistemi informatici del Policlinico o di soggetti esterni.
- Riprodurre e/o asportare documentazione di qualsiasi tipo anche se non classificata come riservata (compresi progetti, schede, prospetti, documentazione clinica, ecc.), se non dietro esplicita autorizzazione del titolare dei relativi diritti (o di persona da esso delegata).
- Distruggere, deteriorare, rendere inservibili, del tutto o in parte, i sistemi informatici ovvero i programmi e le informazioni, le procedure, i dati, i supporti ecc.
- Riprodurre, duplicare e asportare programmi di cui il Policlinico è licenziatario o proprietario.
- Scaricare (cosiddetto download), installare, utilizzare programmi software che non siano stati regolarmente acquistati, distribuiti e installati dagli uffici competenti.
- Utilizzare in modo improprio i servizi informatici del Policlinico, quali ad es. l'accesso a Internet e la posta elettronica, per attività non correlate alla propria

attività lavorativa.

- In generale, utilizzare gli strumenti informatici del Policlinico per fini personali (ad es. per la conservazione di documenti personali di qualsiasi natura, per la stampa o la copia di documenti/fotografie personali, l'invio di fax personali, ecc.).
- Diffondere dati personali o del Policlinico attraverso internet, ad es. attraverso i siti di social network quali Facebook, Twitter, ecc… Si ricorda infatti che tali siti non hanno carattere "privato" e che tutto quello che è "postato" diviene, di fatto, pubblico.

- **Movimentare e riparare autonomamente le attrezzature informatiche (pc, stampanti, telefoni)**

4.3 Regole Operative

- Dati personali che siano trattati per svolgere attività relative alla propria mansione non devono essere copiati, estratti, trasmessi, divulgati tramite supporti informatici. In particolare, è vietato utilizzare condivisioni su rete pubblica o senza restrizione all'accesso per scambiare file riservati. Nel caso ciò fosse inevitabile, i file devono essere crittografati (almeno mediante protezione con password). In ogni caso, i file che transitano in cartelle condivise devono essere immediatamente rimossi dopo il ricevimento: l'obbligo del controllo della rimozione vale sia per chi li riceve sia per chi li deposita.
- È deprecato, ai fini della sicurezza, l'uso di supporti di memorizzazione removibili (CD/DVD, chiavi USB, HD esterni ecc.) per la memorizzazione di dati personali o sensibili. Deroghe a tali divieti sono possibili solo nei casi in cui sia possibile dimostrare il corretto uso dei supporti di memorizzazione necessari al recupero di dati non più disponibili.

  In generale i supporti di memorizzazione – anche non removibili - che contengono dati personali o sensibili, nel caso non possano essere cancellati in maniera da renderne irrecuperabile il contenuto, una volta dismessi – per es. per obsolescenza o per guasto -, dovranno essere distrutti o smaltiti in maniera tale che il contenuto non sia più recuperabile.
- **Le Password:** La configurazione di accesso ai dati ed alle applicazioni, ovvero **le cosiddette credenziali di autenticazione** (costituite normalmente da un "nome utente/user" e una "password"), è personale, riservata, univoca e deve essere adeguatamente custodita.
- In particolare la password:
  - Non deve essere comunicata o distribuita a terzi, anche se colleghi.
  - Non deve essere scritta o apposta (ad es. con post-it,..) né riportata in maniera leggibile in luoghi pubblici, quali ad esempio monitor, calendari, lavagne o pareti, sotto il telefono. Non deve essere salvata su file non crittografati: non deve essere individuabile con facilità, in particolare in prossimità del posto di lavoro (es. nell'agenda, nella cassettiera, sulla scrivania).
  - La componente riservata della credenziale (cioè la password) deve essere aggiornata periodicamente (al massimo ogni 3 mesi): ogni utente è in grado di modificarla autonomamente (in caso contrario rivolgersi alla UO ICT). Per semplificare queste operazioni tutte le procedure informatiche saranno

progressivamente adeguate in maniera opportuna, in modo tale da ricordare all'utente le scadenze e da semplificare le operazioni di modifica della propria password.

- La componente riservata della credenziale deve essere scelta in modo non banale; sono da evitare ad es. i nomi propri (dei propri congiunti, del proprio animale domestico…), le date di nascita o di matrimonio, le città, ecc., al fine di evitare la sua facile identificazione da parte di eventuali attaccanti (guessing attack)
- Per renderla efficace, ma al tempo stesso facile da ricordare, si possono utilizzare giochi mnemonici personalizzati (un esempio: l'incrocio di due nomi comuni con la seconda e la quarta lettera in maiuscolo: tavolo+sedia = tAvOledia; acronimi di frasi, poesie, testi conosciuti a memoria "Mi illumino di immenso = MIlmnDImns8)
- La password deve essere obbligatoriamente di lunghezza non inferiore a 12 (dodici!) caratteri, avere almeno un carattere maiuscolo, un carattere minuscolo, un numero e un carattere speciale.

- **Antivirus/antispyware/malware**: i computer utilizzati presso l'Ospedale Policlinico San Martino sono dotati di un prodotto antivirus ed antispyware periodicamente aggiornato secondo le policy di sicurezza del Policlinico che consente il monitoraggio ed il blocco delle infezioni da virus informatici, dell'introduzione di software di tipo spyware o di malware. Non è ammesso l'utilizzo di un prodotto diverso da quello fornito. In casi particolari (postazioni universitarie, collegate a medicali, ...), nel caso in cui si accerti che un computer sia sprovvisto di questi sistemi, è obbligatorio darne immediata comunicazione all' UO ICT affinché provveda alla messa in sicurezza dell'attrezzatura. Si consideri che in una rete aziendale un singolo PC compromesso espone a rischio di attacco o contagio tutti i pc collegati alla rete.
- Il Policlinico persegue una politica di centralizzazione nella gestione dei dati, per cui progressivamente le gestioni locali di dati scompariranno sostituite da gestioni centralizzate su server. Fino a quando questo processo non sarà portato a compimento potranno esistere gestioni locali di dati su stazioni di lavoro personali - personal computer non connessi in rete o connessi in rete, ma con la possibilità di gestire localmente documenti e/o dati – la cui tutela è demandata all'utente finale.
- Al fine di evitare perdite accidentati causate da guasti è buona norma non conservare dati riservati o comunque importanti solo sul proprio pc, ma farne una copia sulle cartelle server che l'UO ICT mette a disposizione sia a livello di UO che singolo utente. In tal modo i dati saranno sottoposti alle procedure di backup gestite sui sistemi centrali.

- **La rete di trasmissione dati e fonia** è un prezioso e complesso bene del Policlinico che permette le comunicazioni di vario tipo all'interno e all'esterno del Policlinico e, come tale, va monitorata e gestita nel rispetto delle esigenze complessive del Policlinico stesso. Per questo motivo è necessario seguire alcune misure precauzionali volte ad evitare che un uso scorretto o per fini non istituzionali della rete generi rallentamenti o addirittura blocchi nei servizi forniti dal Policlinico.

In particolare è vietato:

- connettere in rete stazioni di lavoro se non dietro esplicita e formale

autorizzazione della UO ICT;

- modificare in qualsiasi modo la configurazione software o hardware della stazione di lavoro o di altri dispositivi direttamente connessi alla rete (stampanti condivise, ecc…);
- modificare le partizioni del disco fisso e installare altri sistemi operativi
- monitorare ciò che transita in rete;
- installare e/o utilizzare hardware o software di qualsiasi tipo (ad es.: è vietato installare sistemi wireless, modem, hard disk esterni, ecc.).
- per ragioni di sicurezza è severamente vietata la connessione ad Internet tramite modem nelle postazioni di lavoro connesse (o facilmente collegabili) alla rete del Policlinico. Le stazioni di lavoro scollegate dalla rete del Policlinico devono essere espressamente autorizzate dal Responsabile ICT.

4.4 Ulteriori regole per i dispositivi portatili

- Le regole di comportamento ed i divieti descritti valgono anche per le attrezzature di tipo mobile quali computer portatili, notebook, netbook, tablet, ecc.
- A differenza della maggior parte dei computer fissi (computer desktop), che solitamente vengono assegnati ad uno specifico servizio/UO per essere utilizzati in maniera condivisa da più utenti, l'assegnatario di un dispositivo portatile è personalmente responsabile del corretto uso del bene che gli è stato consegnato (nel caso in cui sia assegnato ad una UO il responsabile è il direttore della stessa).
- **I dispositivi portatili (pc, cellulari, tablet) concessi ai dipendenti per motivazioni di servizio, al venir meno delle condizioni che ne hanno consentito l'assegnazione (es. fine del rapporto di lavoro, trasferimento presso altra sede, decadenza dell'incarico, ecc.), devono essere restituiti completi (compresi di carica batterie, mouse, alimentatore)**
- Salvo casi eccezionali, che devono essere in ogni caso esplicitamente autorizzati dal Responsabile dell'UO ICT, non è consentito il collegamento alla rete del Policlinico di PC o altri dispositivi mobili (notebook, tablet, …) di proprietà dell'utente. Nei rarissimi casi ammessi e comunque per esigenze di servizio motivate, valgono le stesse regole qui indicate per i PC portatili del Policlinico.
- È vietato conservare dati tutelati dalla legge sul disco fisso del PC portatile, salvo casi eccezionali autorizzati. In questi ultimi casi, i dati devono essere crittografati e protetti da password (in aggiunta alla protezione standard dell'elaboratore portatile, ovvero password di avvio, autenticazione del Sistema Operativo ecc.).
- Anche per l'elaboratore portatile si devono utilizzare soltanto programmi autorizzati, di proprietà del Policlinico o dotati di regolare licenza (sempre intestata al Policlinico).
- È obbligatorio segnalare tempestivamente i casi di furto, o qualsiasi altro incidente: in modo particolare, se ciò ha implicazioni inerenti alla sicurezza dei dati personali conservati nell'elaboratore, deve esserne data immediata comunicazione al corrispondente responsabile del trattamento (cioè al Direttore di UO in cui è avvenuto il fatto) che dovrà renderne edotto il Responsabile Protezione Dati aziendale.
- Non è ammesso l'uso di programmi con connessione automatica ai sistemi centrali

per mezzo di linee telefoniche o con altri sistemi telematici salva autorizzazione scritta della UO ICT.

- In luoghi pubblici o in ambienti non riservati non devono essere inseriti o declamati a voce dati personali o informazioni di carattere riservato.
- Nel caso di utilizzo dei pc aziendali fuori dal Policlinico (es. per attività di smart working, per attività di coordinamento, ecc.) si invita il personale a recarsi con cadenza mensile presso la UO ICT per effettuare gli aggiornamenti di sicurezza

4.5 Utilizzo del software assegnato

- Sui computer del Policlinico sono installate solo procedure e programmi software ritenuti necessari dal Policlinico per l'espletamento del proprio lavoro e devono essere utilizzati solo per le attività legate al Policlinico.
- È vietata qualsiasi riproduzione (permanente, temporanea, parziale o totale), installazione, download o distribuzione di software di soggetti terzi, che non sia autorizzata dalla struttura competente (UO ICT).
- È vietato l'uso nel Policlinico di software acquisito privatamente o procurato per vie non ufficiali e, analogamente, è vietato l'uso all'esterno del software del Policlinico.

4.6 Regole d'utilizzo della rete internet, della posta elettronica e dei social

Con il presente disciplinare l'Ospedale Policlinico San Martino definisce i criteri e le modalità operative di accesso e utilizzo del servizio internet da parte dei dipendenti e di tutti gli altri soggetti che a vario titolo prestano servizio o attività per conto e nelle strutture del Policlinico (collaboratori, tirocinanti, studenti, stagisti, consulenti).
Il Policlinico si riserva di adeguare in qualsiasi momento le proprie policies di sicurezza in funzione di eventuali mutamenti legislativi o in ragione di particolari necessità tecniche.

Ogni dipendente e chiunque a vario titolo presta servizio o attività per conto e nelle strutture del Policlinico deve attenersi alle disposizioni del presente regolamento, ai sensi dell'attuale normativa in tema di tutela della riservatezza, in tema di tutela del diritto d'autore ed in tema di criminalità informatica.

Il computer (sia esso un portatile, una postazione statica, un palmare o altro strumento di telecomunicazione) è di proprietà del Policlinico e deve essere utilizzato unicamente per fini lavorativi. A ciascun dipendente ed a chiunque, a vario titolo, presta servizio o attività per conto e nelle strutture del Policlinico viene attribuita la responsabilità di utilizzare il computer e gli accessori ad esso collegati in maniera professionale, a norma di legge e rispettando i comuni principi morali ed etici, nonché la privacy e la segretezza dei dati trattati.
Ciascun dipendente e chiunque a vario titolo presta servizio o attività per conto e nelle strutture del Policlinico, è responsabile, qualora il computer del Policlinico e gli strumenti (computer portatili, palmari, telefoni cellulari ed ogni altro dispositivo mobile) a lui affidati vengano utilizzati da parte di terzi.

Sono considerati "Utenti" della Rete, tutti i soggetti che, con qualsiasi dispositivo e a qualunque titolo, accedono, anche temporaneamente, alle risorse informatiche della Rete del Policlinico.

Di regola, l'utilizzo della rete internet e della posta elettronica del Policlinico è consentito

solo per motivi attinenti allo svolgimento dell'attività lavorativa.

Utilizzo di internet

Per ragioni di sicurezza e per garantire l'integrità dei sistemi informatici, l'accesso ad Internet effettuato tramite elaboratori connessi alla Rete del Policlinico, è scrupolosamente protetto da appositi dispositivi di sicurezza informatica (firewall, antivirus, ecc.). Non è consentito l'accesso diretto ad Internet (tramite modem esterni o altri dispositivi) che si perfezioni bypassando il sistema di sicurezza predisposto all'interno del Policlinico.
La banda impiegata per la connessione Internet è una risorsa limitata.
Ogni utente ha la responsabilità di non compiere operazioni che monopolizzino le risorse informatiche del Policlinico (eccessivo traffico in download/upload) a discapito degli altri legittimi utenti e sistemi.

Trattamento e conservazione dei dati conseguenti all'utilizzo di internet

Le credenziali di autenticazione in rete, l'host-name ed il percorso di accesso alle risorse disponibili su internet vengono raccolti e trattati in modo del tutto automatico mediante files di log, ovvero archivi temporanei idonei a monitorare il traffico di rete ed elaborare le statistiche di traffico.
Dette informazioni, accessibili al solo amministratore di sistema, non sono raccolte per essere associate ad utenti identificati ma potrebbero per loro stessa natura attraverso elaborazioni ed associazioni con dati detenuti da questo Policlinico, consentire l'identificazione dell'utente.
I dati riferibili ad utenti individuabili vengono cancellati automaticamente, salvo se ne renda necessaria la conservazione per il tempo strettamente necessario a perseguire finalità organizzative, produttive e di sicurezza, nonché per garantire la continuità d'accesso al servizio, e comunque per un periodo congruo alla criticità dell'evento e conformemente ai principi di pertinenza e non eccedenza, nei casi eccezionali di:

- esigenze tecniche o di sicurezza segnalate dal Responsabile UO ICT;
- 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.

Internet: attività non consentite

Costituiscono abusi ovvero attività non consentite:

- qualsiasi atto che possa compromettere la sicurezza e la riservatezza delle risorse informatiche del Policlinico.
- il download (c.d. scarico) di software, anche se gratuito, da siti Internet. Al fine di prevenire la manomissione della configurazione hardware e software delle postazioni di lavoro, salvo i casi necessari per il funzionamento di specifici applicativi, gli utenti sono configurati con diritti limitati. La configurazione e l'amministrazione delle postazioni di lavoro è riservata al personale della UO ICT.
- E' in assoluto vietato l'accesso a internet tramite strumentazioni (es. modem) e/o browser non autorizzati dalla direzione dell'UO ICT dell'Ospedale Policlinico San Martino.
- E' in assoluto vietato l'accesso ai siti internet aventi contenuto pornografico e/o pedopornografico, ingiurioso, diffamatorio, oltraggioso e/o discriminatorio per sesso, lingua, religione, razza, origine etnica, condizione di salute, opinione e appartenenza sindacale e/o politica. Qualora erroneamente si abbia accesso ad un sito internet avente il contenuto suddetto, ne dovrà essere data informazione immediata al responsabile dell'UO ICT per consentire ogni più opportuno controllo di sicurezza. In

tal caso, fino al momento del controllo, non devono cancellarsi dati inerenti la navigazione effettuata (cache, cronologia, coookies).

- È vietato compiere attività di trading on line tramite internet.
- È vietato inviare tramite internet o posta elettronica software di qualunque genere e natura, salvo preventiva approvazione della direzione dell'UO ICT.
- È in assoluto vietato scaricare e/o inviare tramite internet o posta elettronica materiale protetto dalla legge sul diritto d'autore (immagini, musica, film, etc…) salvo che non se ne abbiano i diritti.
- È in particolare vietato partecipare, per motivi non lavorativi, a social network (Facebook, Twitter, …), forum, blog, chat line, bacheche elettroniche o altri servizi similari. Si ricorda infatti che tali siti non hanno carattere "privato" e che tutto quello che viene "postato" diviene, di fatto, pubblico.
- E' assolutamente vietata l'installazione o comunque l'utilizzo di software "peer to peer", di file sharing e di controllo remoto delle postazioni (es. Teamviewer o simili).
- È in assoluto vietato usare internet in modo da comunicare e/o diffondere dati personali e/o informazioni riservate di proprietà dell'Ospedale Policlinico San Martino.

Utilizzo dei social

- nell'utilizzo dei propri account di social media, il dipendente utilizza ogni cautela affinché le proprie opinioni o i propri giudizi su eventi, cose o persone, non siano in alcun modo attribuibili direttamente alla pubblica amministrazione di appartenenza
- in ogni caso il dipendente è tenuto ad astenersi da qualsiasi intervento o commento che possa nuocere al prestigio, al decoro o all'immagine dell'amministrazione di appartenenza o della pubblica amministrazione in generale

Utilizzo della posta elettronica

La posta elettronica è uno strumento di lavoro e, come tale, deve essere impiegato esclusivamente per fini professionali in relazione alle specifiche mansioni assegnate al dipendente all'interno del Policlinico.
Chiunque utilizzi la posta elettronica è tenuto ad adottare tutte le misure idonee per non interferire nel corretto funzionamento della stessa e per assicurare agli altri utenti il godimento del medesimo servizio.
Al fine di evitare inutile traffico di rete e dispendio di risorse sul sistema posta, gli allegati ai messaggi di posta elettronica non devono, laddove possibile, consistere in file di ingenti dimensioni.
E' buona regola la periodica pulizia della casella di posta, con la cancellazione di e-mail obsolete ed inutili. L'autorità Garante Privacy con Provvedimento n. 255 del 25/07/2022, in merito alla problematica della conservazione delle mail, premesso l'esplicito divieto di equiparare i sistemi di posta elettronica ad archivi aziendali, indica di individuare e conservare i soli dati e documenti specifici necessari alla continuità operativa dell'Azienda. Allo stesso modo, l'archiviazione completa delle comunicazioni presenti nei servizi di e-mail per ipotesi di futura difesa in giudizio è da ritenersi, secondo il Garante, non conforme ai principi di necessità, pertinenza e non eccedenza di cui all'articolo 5, paragrafo 1, lettere c) ed e), del GDPR.
I file ottenuti da fonti esterne alla Rete del Policlinico, inclusi gli allegati ai messaggi di posta elettronica, sono spesso veicolo di virus, trojan horses o altre porzioni di codice maligno. Il server di posta elettronica interno al Policlinico è dotato di strumenti di protezione logica costantemente aggiornati ed atti a contenere i rischi derivanti da possibili incidenti informatici. Resta evidentemente in capo ad ogni singolo utente la responsabilità di un

atteggiamento consapevole nei confronti di tali insidie. **Gli utilizzatori del servizio di posta elettronica non devono pertanto aprire, per nessuna ragione, file allegati a messaggi e-mail di provenienza incerta e qualora sospettino che porzioni di codice maligno siano state introdotte all'interno della Rete del Policlinico sono tenuti a darne pronta comunicazione all' UO ICT.**
I protocolli di trasmissione della posta elettronica inviano i dati relativi ai messaggi email in "chiaro" con la conseguenza diretta che la posta elettronica inviata all'esterno della rete informatica del Policlinico è soggetta al rischio di intercettazione. Documenti di lavoro strettamente riservati o contenenti dati sensibili possono essere trasmessi via e-mail solo se contenuti nell'allegato ed in forma cifrata. Il Policlinico utilizza opportuni sistemi antispam ed antivirus, ossia dei sistemi che consentono di bloccare la propagazione di codice infetto o comunque dannoso, ed eventuali azioni illecite, per quanto possibile.

Posta elettronica: attività non consentite

- non è consentito utilizzare la posta elettronica per motivi personali o per ragioni che esulino dallo svolgimento delle mansioni assegnate;
- è espressamente vietato qualsiasi utilizzo della posta elettronica che possa tradursi in un danno o semplicemente in un disturbo a terzi, ad esempio l'invio indiscriminato di messaggi di posta elettronica indirizzati ad un medesimo soggetto (mail bombing), la diffusione via e-mail di materiale pubblicitario e/o commerciale non richiesto (spamming), etc.;
- non è consentito trasmettere via e-mail virus, worms, trojan – horses o altro codice maligno, noto per arrecare danni e malfunzionamenti ai sistemi informatici;
- non è consentito inviare o archiviare messaggi e/o allegati informatici (testo, audio, immagini, filmati, etc.) di natura oltraggiosa, discriminatoria per sesso, religione, origine etnica, appartenenza sindacale o politica o che comunque possano risultare offensivi della dignità umana;
- non è consentito fornire a soggetti terzi non autorizzati l'accesso al servizio di posta elettronica del Policlinico;
- è fatto divieto agli utenti di utilizzare lo strumento della posta elettronica per inviare, trasmettere o comunque divulgare a terzi non autorizzati informazioni riservate del Policlinico
- è fatto divieto a qualunque utilizzatore del servizio di posta elettronica di "effettuare spoofing" (falsificazione) dell'indirizzo e-mail assegnatogli;
- non è consentito all'amministratore leggere e registrare sistematicamente i messaggi di posta elettronica ovvero i relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio e-mail;
- non è consentito utilizzare la posta elettronica per fini non ammessi dalle norme vigenti;
- l'utilizzo di caselle di posta elettroniche personali è di norma evitato per attività o comunicazioni afferenti il servizio

Posta elettronica: chiusura degli account

L'Autorità Garante, con Provvedimento n. 255 del 25/07/2022, specifica che alla conclusione del rapporto lavorativo del dipendente con il datore, è necessario procedere all'immediata cancellazione dei dati e alla disattivazione dell'account.
È vietato

- impostare sistemi automatici (es. risposte automatiche) di mancato recapito alle eventuali nuove comunicazioni in arrivo e indicando degli indirizzi aziendali alternativi di contatto

- impostare l'inoltro diretto ad altra casella di posta aziendale delle eventuali ulteriori nuove mail in arrivo

Regole di comportamento generali

- È necessario che le impostazioni del browser, utilizzato per la navigazione in internet, non siano mai modificate.
- È necessario che le informazioni inerenti alla navigazione in rete: quali la cache, la cronologia, i cookies, non siano mai cancellate, se non nel rispetto delle procedure adottate dalla direzione dell' UO ICT.
- Il sistema di posta elettronica del Policlinico non può essere utilizzato per finalità di "spamming" o simili, che possano pregiudicare il corretto funzionamento dell'infrastruttura (come ad es. l'invio, ad un numero elevato di destinatari, di messaggi di posta elettronica con allegati).
- L'utente è direttamente e totalmente responsabile del contenuto dei messaggi inviati e dell'uso che egli fa del servizio di posta elettronica e di accesso a Internet, dei contenuti che ricerca, dei siti che contatta, delle informazioni che vi immette, delle modalità con cui opera e dell'eventuale materiale scaricato sulla rete del Policlinico.
- In ottemperanza alla disciplina emanata dal Garante della Privacy e dalla raccomandazione del Dipartimento della Funzione Pubblica n. 2/2009 (della Presidenza del Consiglio) il Policlinico ha attivato dei sistemi per assicurare il corretto utilizzo della risorsa internet rispondente ai requisiti della tutela della privacy dell'utente della rete.

4.7 Le buone abitudini nel luogo di lavoro

- Il PC, il terminale e le periferiche, a fine lavoro, devono essere spenti, salvo indicazioni diverse dell' UO ICT.
- Quando ci si allontana dalla propria postazione di lavoro (per pausa mensa, riunione,…) ci si deve sempre accertare che la postazione sia protetta da accesso non autorizzato. Di norma è bene scollegarsi dal sistema.
- Ciò vale anche per i supporti (CD/DVD, chiavi USB, HD esterni ecc.) che sono asportabili con facilità ancora maggiore. I supporti magnetici, inoltre, se contengono dati sensibili, dopo il loro utilizzo devono essere distrutti o resi inutilizzabili. Possono essere riutilizzati esclusivamente nel caso in cui il contenuto precedente sia stato reso permanentemente inintelligibile (attenzione: non è sufficiente la semplice cancellazione del contenuto).
- Al fine di prevenire il diffondersi di virus informatici è bene conoscere sempre con precisione quale sia la fonte dei dati, ed essere certi che tale fonte sia affidabile e sicura; è preferibile non utilizzare un supporto di memorizzazione removibile di cui non si conosca la fonte.
- Allo stesso modo è sempre bene evitare di leggere o utilizzare allegati di messaggi di posta elettronica che non provengano da fonti certe, riconosciute e sicure; nel caso pervenga un messaggio di fonte incerta procedere immediatamente alla eliminazione. Nel caso si abbia il sospetto che il proprio sistema di elaborazione sia stato infettato avvertire il personale tecnico competente e non operare per alcun motivo scambio di supporti di memorizzazione o posta elettronica con altri.

- Nelle presentazioni (slide) devono sempre essere utilizzati dati privi di qualsiasi riferimento (inclusi codici di collegamento) a persone fisiche o giuridiche.

5.0 Informativa su responsabilità e sanzioni

- E' pubblicato sulla intranet, a disposizione di tutti gli utenti del Policlinico, il testo commentato della legge n. 547 del 23/12/93 relativa al crimine informatico.
- E' vietata (legge n. 248 del 18/08/2000 relativa alla tutela del diritto d'autore) la riproduzione o la duplicazione con qualsiasi mezzo e a qualsiasi titolo dei programmi informatici e dei manuali a corredo dei programmi; si ricorda infatti che anche i manuali sono coperti dalla legge sul diritto di autore e possono essere riprodotti solo dietro autorizzazione del titolare dei diritti esclusivi. L'UO ICT, qualora tecnicamente possibile può predisporre copie di riserva dei programmi dotati di regolare licenza allo scopo di prevenire accidentali perdite dell'originale e quindi danni patrimoniali al Policlinico. Tale copia di riserva potrà essere usata soltanto per ripristinare le funzionalità del programma, quando non sia possibile utilizzare il programma originale.
- L'utente è civilmente responsabile di qualsiasi danno arrecato al Policlinico, all'Internet Provider e/o a terzi in dipendenza della mancata osservanza di quanto sopra.
- L'utente è informato del fatto che la conoscenza della password da parte di terzi consente a questi ultimi l'accesso alla rete del Policlinico e l'utilizzo dei relativi servizi in nome dell'utente e l'accesso ai dati cui il medesimo è abilitato, con le conseguenze che la cosa può comportare, quali ad esempio la visualizzazione di informazioni riservate, la distruzione o la modifica dei dati, la lettura della propria posta elettronica, l'uso indebito di servizi, ecc..
- L'utente prende atto che è vietato servirsi o dar modo ad altri di servirsi della rete del Policlinico e dei servizi da essa messi a disposizione per utilizzi illeciti che violino o trasgrediscano diritti d'autore, marchi, brevetti, comunicazioni private o altri diritti tutelati dalla normativa corrente, per utilizzi contro la morale e l'ordine pubblico, per recare molestia alla quiete pubblica o privata, per recare offesa o danno diretto o indiretto al Policlinico e comunque a chicchessia.
- L'utente si assume la responsabilità civile per i propri fatti illeciti e per quelli commessi da chiunque utilizzi il suo codice identificativo, con particolare riferimento all'immissione in rete di contenuti critici o idonei ad offendere l'ordine pubblico o il buon costume.
- Nei casi di utilizzo indebito e/o non in linea con le indicazioni del presente regolamento per l'uso dei sistemi informatici si rimanda, ai fini interni, al Codice disciplinare del personale del Policlinico.