REGOLAMENTO
PER L'USO DEGLI STRUMENTI INFORMATICI

1 Sommario

2 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.

Regolamento per l'uso degli strumenti informatici

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.

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 autorizzati al 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.

3 Sigle

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

4 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
7.0	Revisione dei contenuti inerenti alla password policy
8.0	Inserimento paragrafo relativo ai metadati della posta elettronica, in ottemperanza al Provvedimento dell'Autorità Garante n. 642 del 21 dicembre 2023 ed al suo successivo aggiornamento con Provvedimento n. 364 del 06 giugno 2024
9.0	Revisione dei contenuti inerenti alle attività non consentite via internet, a seguito di una segnalazione di Data Breach
10.0	Revisione completa dei contenuti Inserimento paragrafo relativo alla rete della ricerca

5 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 IRCCS;
- devono essere utilizzate esclusivamente per finalità aziendali (fatte salve le eventuali autorizzazioni specifiche);
- devono essere rese disponibili solo alle persone autorizzate, esplicitamente (in seguito ad un atto di nomina dell'autorizzato/incaricato al trattamento dei dati);
- 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 dei dati trattati, per pregiudicare ed ostacolare le attività del Policlinico e non possono essere destinate al perseguimento di interessi privati in contrasto con quelli del Policlinico.

Valgono le seguenti **buone abitudini di lavoro**:

- Il PC, il terminale e le periferiche, a fine lavoro, devono essere spenti, salvo indicazioni diverse dell'UO ICT o specifiche necessità del contesto in cui si opera;
- 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 disconnettersi dal sistema;
- I supporti esterni (CD/DVD, chiavette USB, HD esterni, ecc.) devono essere utilizzati solo in via eccezionale e, se contengono dati personali, devono essere custoditi in luoghi sicuri e non lasciati collegati al pc o in luoghi facilmente accessibili. In caso di dismissione dei supporti esterni, questi devono essere distrutti o resi inutilizzabili attraverso sistemi di punzonatura o deformazione meccanica, distruzione fisica o disintegrazione, prendendo contatti con l'U.O. ICT.
- 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 supporti di memorizzazione esterni e removibili.
- E' necessario 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 da fonte incerta si raccomanda di procedere immediatamente alla sua eliminazione e segnalarlo alla U.O. ICT tramite Help Desk;
- Nei documenti e nei testi delle varie comunicazioni in qualsiasi forma devono sempre essere utilizzati dati privi di qualsiasi riferimento a persone fisiche o giuridiche;
- In luoghi pubblici o in ambienti non riservati non devono essere comunicati a voce dati personali o informazioni di carattere riservato.

6 I principali divieti

È vietato:

- Introdursi abusivamente nella rete del Policlinico;
- Fornire ad altri le proprie credenziali di identificazione ed autenticazione (user e password, PIN), in quanto sono strettamente personali;
- 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, installare, utilizzare programmi software che non siano stati regolarmente autorizzati 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;
- 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, ecc.);
- Diffondere dati personali o del Policlinico attraverso internet, ad es. attraverso i siti di social network quali Facebook, Twitter, Instagram, ecc.;
- Movimentare e riparare autonomamente le attrezzature informatiche (pc, stampanti, telefoni);
- Utilizzare supporti informatici esterni quali chiavette usb e hard disk, se non preventivamente autorizzato o per esigenze motivate.

7 Regole Operative

7.1 Credenziali di accesso

Le credenziali di autenticazione (costituite normalmente da un "nome utente/user" e una "password") sono personali, riservate, univoche e devono essere adeguatamente custodite.

Valgono le seguenti prescrizioni:

- Non devono essere comunicate o distribuite a terzi, anche se colleghi;
- Non devono essere scritte o apposte (ad es. con post-it...) né riportata in maniera leggibile in luoghi pubblici, quali ad esempio monitor, calendari, lavagne o pareti, sotto il telefono. nell'agenda, nella cassettiera, sulla scrivania);
- La componente riservata della credenziale (cioè la password) deve essere aggiornata ogni 3 mesi: ogni utente è in grado di modificarla autonomamente o dal pc ospedaliero o collegandosi al link https://idem.hsanmartino.it;
- 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.

7.2 Postazioni di lavoro (pc fissi, pc portatili, tablet)

Nell'utilizzo delle postazioni di lavoro si raccomanda:

- Di non connettere in rete dispositivi se non dietro esplicita e formale autorizzazione dell'UO ICT;
- Di non modificare in qualsiasi modo la configurazione software o hardware della postazione di lavoro o di altri dispositivi direttamente connessi alla rete (stampanti condivise, stampanti etichette);
- Di non modificare le partizioni del disco fisso e installare altri sistemi operativi;
- Di salvare i dati sulle cartelle condivise messe a disposizione dall'UO ICT e sottoposte a backup periodico, e non sul disco fisso del pc.

Dispositivi portatili

Relativamente ai dispositivi portatili:

- L'assegnatario 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 motivi 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, fine dell'attività di smart working), devono essere restituiti completi (compresi di carica batterie, mouse, alimentatore, eventuale borsa);
- 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, ad eccezione dell'accesso alla rete wifi free messa a disposizione dal Policlinico stesso;
- 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, deve esserne data immediata comunicazione al Referente Privacy della propria UO, che informerà gli uffici competenti;
- 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.

7.3 Software aziendali

- Sui computer del Policlinico sono installate solo procedure e programmi software autorizzati per l'espletamento del proprio lavoro;
- È vietata qualsiasi riproduzione (permanente, temporanea, parziale o totale), installazione, download o distribuzione di software di soggetti terzi;
- 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;
- Per l'acquisto di qualsiasi software è necessario richiedere preventivamente parere tecnico all'UO ICT.

7.4 Infrastruttura di rete

L'infrastruttura della rete dati del Policlinico che consente la condivisione di dati e delle informazioni del Policlinico è gestita e manutenuta dall'UO ICT mediante la definizione di architetture ad hoc con lo scopo di proteggere i dati aziendali.

In particolare è vietato:

- monitorare ciò che transita in rete;
- installare e/o utilizzare hardware o software di rete di qualsiasi tipo, quali sistemi wireless, modem, router, hub;
- l'accesso a sottoreti specifiche deve essere espressamente richiesto ed autorizzato dall'UO ICT.

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

Di regola, l'utilizzo della rete 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 è protetto da appositi dispositivi di sicurezza informatica (firewall, antivirus, proxy, ecc.).

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 utenti e sistemi.

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.

Regolamento per l'uso degli strumenti informatici

Costituiscono attività non consentite:

- E' 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 utilizzare l'indirizzo mail aziendale per accessi o iscrizioni a siti o piattaforme web non prettamente collegate con la propria attività lavorativa. Qualora ciò sia avvenuto, si raccomanda di procedere immediatamente alla cancellazione dei profili, nel rispetto delle regole sul codice di comportamento dei dipendenti pubblici;
- 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 vietato scaricare e/o inviare tramite internet o posta elettronica materiale protetto dalla legge sul diritto d'autore (immagini, musica, film, etc…) e dal Regolamento UE 2016/679;
- È in particolare vietato partecipare, per motivi non lavorativi, a social network (Facebook, twitter, instagram…), 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;
- 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;
- E' vietata l'installazione e l'utilizzo di software "peer to peer", di file sharing e di controllo remoto delle postazioni (es. Teamviewer, Anydesk o simili);
- È vietato modificare le impostazioni del browser, utilizzato per la navigazione in internet;
- È vietato cancellare le informazioni inerenti alla navigazione in rete (es. la cache, la cronologia, i cookies).

7.5 Antivirus/antispyware/malware:

- I computer aziendali sono dotati di un antivirus 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;
- Per le postazioni universitarie, collegate a dispositivi medicali, pc della ricerca che risultano sprovviste di questi sistemi, è obbligatorio darne immediata comunicazione all' UO ICT affinché provveda alla messa in sicurezza del dispositivo. Si consideri che in una rete aziendale un singolo PC compromesso espone a rischio di attacco o contagio tutti i pc collegati alla rete.

7.6 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.

È 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. Il Policlinico utilizza opportuni sistemi antispam ed antivirus costantemente aggiornati, che consentono di bloccare la propagazione di codice infetto o comunque dannoso, ed eventuali azioni illecite, per quanto possibile.

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 personali possono essere trasmessi via e-mail solo se contenuti nell'allegato ed in forma cifrata

Costituiscono 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;
- 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);
- 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 vietato per attività o comunicazioni afferenti il servizio.

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.

Metadati

In ottemperanza al Provvedimento dell'Autorità Garante n. 642 del 21 dicembre 2023 che ha adottato il Documento di indirizzo "Programmi e servizi informatici di gestione della posta elettronica nel contesto lavorativo e trattamento dei metadati", ed al suo successivo aggiornamento con Provvedimento n. 364 del 06 giugno 2024, con il termine metadati, il Garante fa riferimento alle informazioni registrate nei log generati dai sistemi server di gestione e smistamento della posta elettronica e dalle postazioni tra i diversi server interagenti o tra questi e i client. Tra questi sono escluse le informazioni che contribuiscono a formare il corpo del messaggio, che rimane sotto l'esclusivo controllo dell'utente (sia esso il mittente o il destinatario dei messaggi).
Il Policlinico, nel rispetto di quanto indicato nel Documento di indirizzo, effettua la raccolta e conservazione dei metadati per finalità organizzative, produttive, di sicurezza e di tutela del patrimonio aziendale escludendo finalità di controllo dell'attività del lavoratore.
Al fine di assicurare le finalità di cui sopra, in particolare le finalità della sicurezza aziendale, e considerata la criticità del contesto di riferimento, tali metadati sono conservati dal Policlinico per un periodo di tempo superiore ai 21 giorni. Il titolare adotta, a tal fine, tutte le misure tecniche ed organizzative per assicurare l'accessibilità selettiva da parte dei soli soggetti autorizzati e adeguatamente istruiti, nonché la tracciatura degli accessi effettuati.
Le nomine di autorizzazione sono conservate agli atti della UO ICT.

7.7 Rete ricerca

È stata istituita una rete dedicata all'attività di ricerca, separata dalla rete delle attività cliniche, al fine di aumentare il livello di sicurezza dei dati aziendali e al contempo di consentire ai ricercatori lo svolgimento delle loro attività in maniera più agevole.

I pc collegati su rete della ricerca sono riconoscibili dallo sfondo del desktop di colore verde, anziché blu, che riporta la dicitura "*La ricerca che cura*".

È stato altresì messa a disposizione uno spazio dedicato all'archiviazione dei dati accessibile dalla rete della ricerca.

Ogni U.O. afferente alla Direzione Scientifica può prendere contatti con l'U.O. ICT per:

- concordare il trasferimento su rete della ricerca dei pc in dotazione, al fine di usufruire di tutti i servizi aziendali (ad es. installazione antivirus, aggiornamenti di sicurezza, utilizzo delle cartelle condivise, ecc…);
- concordare la messa a disposizione di cartelle di rete per la migliore gestione dei dati di cui si rende necessaria l'archiviazione.

Raccomandazioni

Per quanto attiene i software utilizzati per lo svolgimento delle attività, si raccomanda di:

- Verificare, prima dell'acquisto o dell'installazione, mediante apposita richiesta di parere all'U.O. ICT, le specifiche tecniche del software, l'architettura e la compatibilità con il sistema operativo installato sulle postazioni, anche nel rispetto della normativa vigente in materia di cybersecurity;
- Adottare, nel caso di trattamento di dati relativi alla salute, le misure di sicurezza previste in accordo con il Regolamento UE 2016/679;
- Non importare dati relativi all'attività di ricerca su postazioni personali.

8 Normativa di riferimento

- Regolamento (UE) 2016/679 (General Data Protection Regulation)
- Direttiva UE 2022/2555 (NIS2)
- Provvedimenti dell'Autorità Garante per la Protezione dei Dati Personali (GPDP)
- Misure minime di sicurezza ICT per le pubbliche amministrazioni (Linee Guida AgID)