DELIBERAZIONE DEL DIRETTORE GENERALE

Deliberazione n.ro	Data di Adozione
0002242	06/11/2025

OGGETTO: Nuovo Regolamento aziendale per l'utilizzo delle Postazioni di lavoro (PdL). Approvazione.

PROPOSTA DI DELIBERAZIONE DEL DIRETTORE GENERALE N.RO 20250002567 DEL 04/11/2025
COMPOSTA COMPLESSIVAMENTE DA 5 (cinque) PAGINE
DI 1 (uno) ALLEGATI SOGGETTI A PUBBLICAZIONE PER UN TOTALE DI 28 (ventiotto) PAGINE
DI 0 (zero) ALLEGATI NON SOGGETTI A PUBBLICAZIONE PER UN TOTALE DI 0 (zero) PAGINE
DI 1 (uno) DOCUMENTI ISTRUTTORI NON ALLEGATI PER UN TOTALE DI 8 (otto) PAGINE

Con la sottoscrizione in calce, i Direttori dichiarano di non versare in alcuna situazione di conflitto di interesse, anche potenziale, ex art. 6-bis, l. 241/90, artt. 6, 7 e 13, c. 3, D.P.R. 62/2013, vigente codice di comportamento aziendale e art. 1, c. 9, lett. e), l. 190/2012 – quest'ultimo come recepito, a livello aziendale, della vigente sezione Anticorruzione e Trasparenza del PIAO – tale da pregiudicare l'esercizio imparziale di funzioni e compiti attribuiti, in relazione al procedimento indicato in oggetto, così come di non trovarsi in alcuna delle condizioni di incompatibilità di cui all'art. 35-bis, D.L.gs. 165/2001.

Parere della Direttrice Amministrativa	Parere della Direttrice Sanitaria
Firmato Digitalmente il 05/11/2025 14:09 Rachele POPOLIZIO	*Firmato Digitalmente il 06/11/2025 08:28* Rosella SQUICCIARINI

Il Segretario	Il Direttore Generale
Firmato Digitalmente il 06/11/2025 10:24 Raffaele IORIO	*Firmato Digitalmente il 06/11/2025 09:37* Luigi FRUSCIO

ATTESTAZIONE DI AVVENUTA PUBBLICAZIONE

Si attesta che il presente provvedimento viene pubblicato all'Albo pretorio *on-line* della ASL BA, ai sensi dell'art. 32, c. 1, l. 69/2009, per la durata di 30 giorni naturali, decorrenti dal **06/11/2025**

Unità Operativa Affari Generali
L'Addetto alla Pubblicazione
Firmato Digitalmente il 06/11/2025 10:24
Domenico ROVETO

OGGETTO:	**Nuovo Regolamento aziendale per l'utilizzo delle Postazioni di lavoro (PdL). Approvazione.**

IL DIRETTORE GENERALE

Vista la Deliberazione n. 329 del 17/02/2025, con l'assistenza del Segretario, sulla base dell'istruttoria e della proposta formulata dal Direttore f.f. U.O.C. Sistemi Informativi, Ing. Dario Ricci e dal Dirigente Responsabile U.O.S. Affari Generali, Avv. Raffaele Iorio, che ne attestano la regolarità formale del procedimento ed il rispetto della legalità, si considera e determina quanto segue.

PREMESSO:

- che, il Garante per la protezione dei dati personali, con Provvedimento del 1°/03/2007 n. 58 avente ad oggetto *"Trattamento di dati personali relativo all'utilizzo di strumenti elettronici da parte dei lavoratori"*, raccomanda l'adozione da parte dei datori di lavoro pubblici e privati, di un disciplinare interno, definito con il coinvolgimento delle rappresentanze sindacali, in cui siano indicate le regole per l'uso di Internet, della posta elettronica e della tenuta di file della rete interna nel rispetto della Legge 20/05/1970, n. 300 (Statuto dei lavoratori) e del Decreto Legislativo 30/06/2003 n. 196 (Codice in materia di protezione dei dati personali);
- che, i processi ICT e le relative procedure aziendali dell'ASL BA rispettano i principi enunciati dall' art. 5 del Regolamento (UE) 2016/679 (GDPR);
- che, l'ASL di Bari promuove l'utilizzo della Rete Informatica e Telematica, di Internet e della Posta Elettronica quali strumenti utili a perseguire le proprie finalità istituzionali;
- che, la sicurezza deve essere considerata da tutti gli utenti una componente essenziale nell'attività quotidiana, finalizzata alla protezione dei dati, delle informazioni e delle apparecchiature, da manomissioni, uso improprio o distruzione;

DATO ATTO:

- che, con nota prot. ASL BA n. 72084 del 24/09/2025, il Direttore f.f. dell'U.O.C. Sistemi Informativi ha condiviso con la Direzione Generale e con la Direzione Amministrativa, per conoscenza con la Direzione Sanitaria, il Dipartimento Investimenti Acquisti e Tecnologie, l'U.O.C. Controllo di Gestione e l'U.O.S.V.D. Cybersecurity, la proposta di un nuovo Regolamento aziendale per l'utilizzo delle Postazioni di lavoro (PdL), precisando che, *"il documento intende definire in maniera organica le regole di utilizzo delle dotazioni informatiche aziendali, con particolare riferimento al corretto impiego delle risorse hardware e software, alle misure di sicurezza informatica e tutela dei dati, alla responsabilità degli utenti e ai principi di buona prassi a supporto della continuità operativa"*, con l'obiettivo di aggiornare e uniformare le disposizioni già in vigore, assicurandone coerenza con le normative e le policy aziendali in materia di sicurezza e protezione delle informazioni;

- in riscontro alla proposta del summenzionato Regolamento, con nota prot. ASL BA n. 78632 del 15/10/2025, il DPO aziendale ha enunciato nel dettaglio, per quanto di competenza, una serie di indicazioni normative e di provvedimenti deliberativi aziendali da inserire nel Regolamento e a rettifica dello stesso: a titolo meramente esemplificativo e non esaustivo:
  - Regolamento aziendale per la protezione dei dati personali, giusta DDG n. 1776 del 15/10/2021;
  - DDG n. 2120 del 1°/12/2021 recante "Attribuzione delle deleghe, ex art. 2-quaterdecies c. 1 del D.lgs 196/03;
  - art. 11-bis del vigente Codice di comportamento (D.P.R. 81/2023),
  - DDG n. 195 del 30/01/2024 relativa alla Social Media Policy aziendale;
  - DDG n. 162 del 9/02/2022 relativa alla gestione dei data breach prevista dalla procedura aziendale in caso di violazione dei dati;
- con comunicazioni a mezzo mail del 19/09/2025 e del 23/09/2025 (agli atti dell'U.O.C. Sistemi Informativi), il Dirigente Responsabile dell'U.O.SV.D. Cybersicurezza riscontrava per quanto di competenza, con osservazioni e moduli da inserire nel Regolamento in parola;
- con comunicazione a mezzo mail del 29/10/2025 (acquisita al prot. ASL BA n. 82519/2025), il Direttore f.f. dell'U.O.C. Sistemi Informativi ha trasmesso all'U.O.S. Affari Generali il Regolamento definitivo e relativa istruttoria, ai fini della predisposizione dell'atto deliberativo di approvazione, come disposto dal Direttore Generale con nota in calce al prot. n. 72084/2025;

RITENUTO:

pertanto, di procedere ad approvare il nuovo Regolamento aziendale per l'utilizzo delle Postazioni di lavoro (PdL), allegato sub A) alla presente deliberazione di cui costituisce parte integrante e sostanziale;

Acquisiti i pareri favorevoli del Direttore Amministrativo e del Direttore Sanitario, resi ai sensi dell'art. 3, d. lgs. 502/1990.

Per le motivazioni esposte in premessa, che qui si intendono completamente acquisite e che formano parte essenziale e fondamentale del presente atto dispositivo;

DELIBERA

1. di approvare il nuovo Regolamento aziendale per l'utilizzo delle Postazioni di lavoro (PdL), allegato sub A) alla presente deliberazione di cui costituisce parte integrante e sostanziale;
2. di dare atto che il presente provvedimento non comporta oneri a carico del bilancio aziendale;
3. di trasmettere a cura dell'U.O.S. Affari Generali il presente provvedimento, unitamente al Regolamento in parola, a tutte le macrostrutture aziendali, nonché al Collegio Sindacale;
4. di demandare all'U.R.P. la pubblicazione del presente provvedimento nella sezione Amministrazione Trasparente/Disposizioni generali/Atti generali/Regolamenti, presente sul sito web aziendale, ai sensi dell'art. 12, c. 1, D. lgs. 33/2013 e della delibera ANAC n. 1310/2016;

5. altresì, di dare ampia diffusione del nuovo Regolamento mediante la sua pubblicazione sul Portale del Dipendente;
6. di dare atto che tutti i firmatari del presente atto attestano di non versare in alcuna situazione di conflitto di interesse, anche potenziale, ex art. 6-bis, l. 241/90, artt. 6, 7 e 13, c. 3, D.P.R. 62/20213, ai sensi del vigente codice di comportamento aziendale e art. 1, c. 9, lett. e), l. 190/2012 - quest'ultimo come recepito, a livello aziendale, dalla Sezione Anticorruzione e Trasparenza del vigente PIAO - tale da pregiudicare l'esercizio imparziale di funzioni e compiti attribuiti, in relazione al procedimento indicato in oggetto, così come di non trovarsi in alcuna delle condizioni di incompatibilità di cui all'art. 35-bis, d.lgs. 165/2001.

Disciplinare della ASL Bari per l'uso di Internet, della Posta elettronica e della tenuta di file della rete interna

REGOLAMENTO PER L'UTILIZZO DEI SERVIZI ICT – Settembre 2025

ASL Bari

U.O.C. Sistemi Informativi

Sommario

INTRODUZIONE ED AMBITO DI APPLICAZIONE

Il Garante per la protezione dei dati personali, con Provvedimento del 1.03.2007 pubblicato sulla G. U. R.I. del 10.03.2007, n. 58, ad oggetto *"Trattamento di dati personali relativo all'utilizzo di strumenti elettronici da parte dei lavoratori"* raccomanda l'adozione da parte dei datori di lavoro pubblici e privati, di un disciplinare interno, definito con il coinvolgimento delle rappresentanze sindacali, in cui siano indicate le regole per l'uso di Internet, della posta elettronica e della tenuta di file della rete interna nel rispetto della Legge 20.05.1970, n. 300 (Statuto dei lavoratori) e del Decreto Legislativo 30.06.2003, n. 196 (Codice in materia di protezione dei dati personali).

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 ASL di Bari, con il presente Regolamento, intende orientare i comportamenti degli operatori, in modo da evitare che azioni inconsapevoli possano innescare problemi o minacce alla sicurezza nel trattamento dei dati e garantire la massima efficienza operativa delle macchine messe a disposizione degli operatori interni ed esterni all'Azienda. A tale riguardo, si integra quanto disposto dal Regolamento (UE) 2016/679 del parlamento europeo e del Consiglio del 27 aprile 2016 (GDPR -General Data Protection Regulation) e del D.lgs. 101/2018, della Direttiva NIS2 (D.lgs. 138/2024) e delle Misure Minime di Sicurezza ICT definite da AgID e ACN nel 2025.

Porre vincoli e limiti all'utilizzo delle risorse costituisce modalità atta a garantire la correttezza e sicurezza nella pratica, anche in relazione a quanto stabilito dal "Regolamento recante il codice di comportamento dei dipendenti pubblici, a norma dell'art. 54 del D.Lgs. 30 marzo 2001, n.165" di cui al D.P.R. 16 aprile 2013, n. 62, che, all'art. 11, comma 3, stabilisce "Il dipendente utilizza il materiale o le attrezzature di cui dispone per ragioni d'ufficio e i servizi telematici nel rispetto dei vincoli posti dall'amministrazione".

Con il presente regolamento sono quindi disciplinate le condizioni di utilizzo delle risorse informatiche e di comunicazione che la ASL mette a disposizione degli operatori per l'esecuzione delle funzioni di competenza.

Sono altresì regolate le modalità con le quali la ASL può accertare e inibire le condotte illecite degli utilizzatori di Internet, della posta elettronica e dell'accesso alle risorse di archiviazione di massa (server – hard disk).

Sono tenuti all'osservanza delle presenti disposizioni i Direttori/Responsabili di Struttura, individuati come "Delegati al trattamento dei dati – SATD", i Dipendenti designati che vengono nominati "Incaricati del trattamento" dei dati personali ai sensi del Regolamento Europeo 2016/679, nonché i Responsabili ed Incaricati del trattamento "esterni" all'ASL, nei casi relativi a collaborazione di persone fisiche o giuridiche (convenzioni, consulenze, tirocini, appalti, ecc.).

Ai fini del Regolamento si considerano le definizioni:

Account Utente: le credenziali composte dalla coppia "Username" e "Password" tramite le quali un Utente è identificato univocamente dai sistemi e per mezzo delle quali ha l'autorizzazione ad accedere ai Servizi erogati dalle Risorse Tecnologiche;

Amministratori di Sistema: l'insieme del personale incaricato di provvedere alla gestione e al regolare funzionamento delle Risorse Tecnologiche;

ASL: l'Azienda Sanitaria Locale di Bari;

Delegati al trattamento dei dati (SATD): in coerenza con le deliberazioni DG n. 1776/2021 e n. 2120/2021, sono tutti i referenti interni alla ASL Bari (Direttori e Responsabili di Struttura) preposti al trattamento dei dati;

Incaricati: insiemi degli utenti che sono autorizzati all'uso dei Servizi Informatici (dipendenti, collaboratori, personale esterno, etc.…);

Indirizzo e-mail: l'indirizzo di posta elettronica eventualmente associato all'Account Utente;

MFA: Multi Factor Authentication, autenticazione a più fattori;

OTP: One Time Password;

PdL: Postazione di Lavoro;

Responsabili al trattamento: i soggetti esterni alla ASL designati ex art. 28 GDPR;

Risorse Tecnologiche: tutti i server, le workstation, i personal computer, le periferiche (come ad esempio le stampanti, i sistemi di archiviazione, etc.) gestite sotto la responsabilità dell'Ente, unitamente ad ogni dispositivo di rete sia attivo che passivo a cui tali sistemi possono essere interconnessi, compresi i sistemi per l'accesso ad Internet. A quanto sopra indicato si aggiungano software, applicazioni, librerie di supporto, documenti o servizi informatici connessi con i sistemi o le reti sopra indicate, così come la posta elettronica ed ogni altro servizio Internet;

Servizi: l'insieme di funzionalità che il sistema informativo ICT aziendale mette a disposizione degli Incaricati;

SLA: Service Level Agreement, ovvero i livelli concordati di servizio, definiti contrattualmente, che il fornitore è tenuto a rispettare rispetto alle richieste di assistenza e manutenzione.

Spazio Disco Utente: porzione delle Risorse Tecnologiche riservata agli Utenti di specifici Servizi per l'archiviazione di materiale in formato elettronico (file);

VPN: Virtual Private Network.

SICUREZZA

La sicurezza deve essere considerata da tutti gli utenti una componente essenziale nell'attività quotidiana, finalizzata alla protezione dei dati, delle informazioni e delle apparecchiature, da manomissioni, uso improprio o distruzione. La sicurezza delle informazioni dipende principalmente dai seguenti aspetti:

- il controllo degli accessi alle informazioni;
- il mantenimento della loro integrità e riservatezza;
- la sicurezza nella trasmissione e nella comunicazione sia all'interno dell'Ente che all'esterno (ad es. Internet);
- la sicurezza delle postazioni di lavoro e dei personal computer;
- la tempestiva rivelazione e segnalazione di eventuali problemi di sicurezza.
- Tutti gli incaricati devono concorrere alla realizzazione della sicurezza, pertanto devono proteggere le informazioni loro assegnate per lo svolgimento delle proprie attività lavorative in termini di:
- utilizzo delle risorse informatiche;
- accesso ai sistemi e ai dati;
- uso delle password.

PRINCIPI GENERALI

L'ASL promuove l'utilizzo della Rete Informatica e Telematica, di Internet e della Posta Elettronica quali strumenti utili a perseguire le proprie finalità istituzionali

L'utilizzazione dei Servizi da parte dell'incaricato è condizionata all'accettazione integrale del presente Regolamento.

I servizi sono erogati nel rispetto delle finalità dell'ASL.

Ogni incaricato è responsabile civilmente e penalmente del corretto uso delle Risorse informatiche e dei servizi ai quali ha accesso, compresi i propri dati, quindi, consapevole delle potenzialità offerte dagli strumenti informatici e telematici, si impegna ad agire con responsabilità e a non commettere abusi aderendo a un principio di autodisciplina.

Gli Incaricati sono i soli responsabili dell'accuratezza dei dati ottenuti tramite l'utilizzo dei servizi. L'ASL, dunque, non è responsabile dei risultati derivanti dall'utilizzazione dei Servizi, né tanto meno del loro successivo impiego.

L'ASL non è responsabile dell'integrità delle Risorse Tecnologiche e dello Spazio Disco utilizzato dagli incaricati.

La Postazione di Lavoro (PdL), costituito da personal computer, fisso o portatile, stampante, etichettatrice e quant'altro ritenuto necessario all'espletamento dell'attività lavorativa afferente al comparto ICT, viene consegnata completa di quanto necessario per svolgere le proprie funzioni, software applicativo compreso. È pertanto vietato modificarne la configurazione.

Nell'utilizzare gli strumenti informatici messi a disposizione dall'Azienda, il dipendente è tenuto ad usare la massima diligenza, nel rispetto degli obblighi di cui agli articoli 2104 e 2105 del codice civile, utilizzandoli esclusivamente per ragioni di servizio.

Comportamenti difformi possono causare gravi rischi alla sicurezza ed all'integrità dei sistemi aziendali e possono essere oggetto di valutazione da un punto di vista disciplinare oltre che da un punto di vista penale.

In conformità a quanto previsto dall'art. 11-bis del D.P.R. 81/2023 (Codice di comportamento dei dipendenti pubblici), è ammesso un uso personale degli strumenti informatici e telematici aziendali solo in tempi ristretti e senza pregiudizio per l'attività lavorativa, fermo restando il divieto di utilizzo per finalità non conformi ai doveri d'ufficio o che possano compromettere la sicurezza e l'integrità dei sistemi aziendali.

Il personale è inoltre tenuto ad attenersi alle disposizioni contenute nella Social Media Policy aziendale, approvata con Determinazione del Direttore Generale n. 195 del 30/01/2024, che disciplina i comportamenti da adottare nell'utilizzo dei social media, sia attraverso account personali sia mediante canali istituzionali, al fine di tutelare l'immagine e l'affidabilità dell'Ente.

L'uso dei servizi deve essere effettuato in conformità alle norme vigenti e senza provocare alcun danno morale o materiale all'ASL od a terzi.

Un uso dei servizi in maniera non conforme al Regolamento può comportare la sospensione all'Incaricato dell'erogazione dei medesimi ed un'eventuale azione legale al fine di tutelare gli interessi dell'ASL.

L'accesso alla rete ed ai servizi è assicurato compatibilmente con le potenzialità delle attrezzature. Gli accessi potranno essere regolamentati, anche temporaneamente, per esigenze di servizio.

PRINCIPI DI TRATTAMENTO DEI DATI PERSONALI

Ai fini dell'organizzazione aziendale e in coerenza con quanto disposto dal "Regolamento aziendale per la protezione dei dati personali", approvato con Deliberazione del Direttore Generale n. 1776 del 15/10/2021 e successivamente integrato con Deliberazione n. 2120 del 01/12/2021, i Direttori, Dirigenti e Responsabili di Struttura sono individuati quali Delegati al trattamento dei dati (SATD).

I "Responsabili del trattamento" restano esclusivamente i soggetti esterni contrattualmente designati ai sensi dell'art. 28 del Regolamento (UE) 2016/679 (GDPR).

In conformità all'art. 5 del Regolamento (UE) 2016/679 (GDPR), l'ASL Bari adotta i seguenti principi, che non si limitano a essere enunciati ma vengono formalmente tracciati nei processi ICT e nelle procedure aziendali:

1. Liceità, correttezza e trasparenza
    - Ogni trattamento effettuato tramite sistemi ICT è registrato nei Registri dei trattamenti aziendali, con l'indicazione della base giuridica, del titolare e del responsabile.

- Gli utenti sono informati tramite informative privacy standardizzate, pubblicate sulla intranet aziendale e allegate ai moduli di richiesta accesso.
- Le attività di logging e monitoraggio vengono effettuate secondo procedure approvate, con accesso riservato agli Amministratori di sistema designati.

2. Limitazione della finalità e minimizzazione dei dati

- Le richieste di nuove utenze, cartelle condivise o accessi a database devono essere motivate e approvate dal Delegato al trattamento dei dati – SATD della struttura richiedente.
- Gli account vengono profilati secondo il principio del **"***least privilege***"**: accesso ai soli dati strettamente necessari allo svolgimento delle mansioni.
- È vietato archiviare dati personali particolari (es. sanitari) in cartelle condivise generiche o su dispositivi locali; tali dati devono transitare esclusivamente negli applicativi clinici aziendali dedicati.

3. Esattezza e aggiornamento dei dati

- Sono previste verifiche periodiche (almeno annuali) della correttezza e pertinenza degli archivi condivisi, con responsabilità in capo al referente nominato per ciascun Centro di Responsabilità.
- Gli utenti sono tenuti a segnalare tempestivamente eventuali errori o incongruenze tramite ticket al servizio ICT.

4. Limitazione della conservazione

- I file log e i dati trattati nei sistemi ICT hanno tempi di conservazione definiti da procedure aziendali e registrati in un piano di retention approvato dal DPO.
- Gli archivi condivisi devono essere periodicamente rivisti: i documenti obsoleti vengono cancellati o archiviati secondo le linee guida ICT.

5. Integrità e riservatezza

- Tutti gli accessi sono tracciati, autenticati con credenziali univoche e, per i servizi critici, protetti da MFA.
- I dati in transito e a riposo sono protetti mediante cifratura secondo le policy ICT aziendali.
- Incidenti o sospetti data breach devono essere notificati entro 24 ore al DPO tramite comunicazione formale via mail all'indirizzo dpo@asl.bari.it e nota protocollata indirizzata all'ufficio preposto.

La gestione delle violazioni dei dati personali (data breach) è disciplinata dalla Procedura aziendale per la gestione delle violazioni dei dati, approvata con deliberazione del Direttore Generale n. 162 del 09/02/2022, cui il presente Regolamento espressamente rinvia.

In merito alla tenuta e aggiornamento del Registro dei Trattamenti (art. 30 GDPR) si rimanda alle indicazioni presenti nel Registro dei trattamenti predisposto dal DPO aziendale.

RUOLI E RESPONSABILITÀ ICT

La U.O.C. “Sistemi Informativi” agisce, per conto del Titolare del trattamento, in qualità di soggetto delegato ai sensi delle deliberazioni del Direttore Generale n. 1776 del 15/10/2021 e n. 2120 del 01/12/2021, in materia di attribuzione delle deleghe ex art. 2-quaterdecies del D.Lgs. 196/03.

Essa coordina le attività tecniche e organizzative necessarie a garantire la sicurezza, la continuità operativa e la corretta gestione dei sistemi informatici aziendali, nel rispetto delle normative in materia di protezione dei dati personali e di sicurezza informatica.

Gli Amministratori di Sistema sono individuati all’interno della struttura ICT e nominati con provvedimento formale dal Titolare, in conformità a quanto previsto dal Provvedimento del Garante per la Protezione dei Dati Personali del 27 novembre 2008.

Essi operano secondo le procedure aziendali e sotto la diretta responsabilità della U.O.C. “Sistemi Informativi”, con compiti di gestione, controllo e monitoraggio delle infrastrutture tecnologiche, nonché di tracciamento delle attività svolte, nel rispetto dei principi di integrità, riservatezza e disponibilità dei dati trattati.

UTILIZZO DELLA PDL (POSTAZIONE DI LAVORO)

Per Postazioni di lavoro, di seguito PdL, si intende l’insieme dei componenti hardware e software che costituiscono la dotazione di lavoro dell’operatore aziendale. Queste riguardano:

- PC fissi e portatili con relativi accessori e periferiche di input-output;
- monitor; stampanti e multifunzioni;
- stampanti etichettatrici;
- scanner;
- telefoni analogici e digitali/VoIP/DECT;
- fax;
- tablet;
- videoproiettori.

La PdL affidata all’utente è uno strumento di lavoro. Ogni utilizzo non inerente all'attività lavorativa è vietato perché può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.

La PdL deve essere custodita con cura evitando ogni possibile forma di danneggiamento.

Al momento della consegna di un PdL sarà richiesta un'esplicita assunzione di responsabilità circa la regolare custodia e mantenimento della PdL, mediante firma di apposito modulo *(Allegato_4_Modulo_consegna_hw)*.

Eventuali, motivate, modifiche alla configurazione fisica possono essere effettuate solo dai tecnici della U.O.C. "Sistemi Informativi". Eventuale e motivato spostamento della PdL può essere effettuato solo se autorizzati dai tecnici della U.O.C. "Sistemi Informativi".

La PdL data in affidamento all'utente permette l'accesso alla rete dell'Azienda solo attraverso specifiche credenziali di autenticazione, come meglio descritto nei paragrafi successivi del presente Regolamento.

Il personale incaricato della U.O.C. "Sistemi Informativi" ha la facoltà di collegarsi e visualizzare in remoto il desktop delle singole postazioni PC, al fine di garantire l'assistenza tecnica e la normale attività operativa.

Le attività poste al controllo della massima sicurezza contro virus, spyware, malware, etc. saranno a cura di personale adeguatamente predisposto dalla U.O.S.V.D. "Cybersecurity".

L'intervento viene effettuato esclusivamente su chiamata dell'utente, attraverso la specifica apertura della procedura di ticketing. In caso di oggettiva necessità, a seguito della rilevazione tecnica di problemi nel sistema informatico e telematico, è altresì possibile l'intervento diretto. In quest'ultimo caso, e sempre che non si pregiudichi la necessaria tempestività ed efficacia dell'intervento, verrà data comunicazione della necessità dell'intervento stesso.

Non è consentito l'uso di programmi diversi da quelli ufficialmente installati dal personale della U.O.C. "Sistemi Informativi" per conto dell'ASL, né viene consentito agli utenti di installare autonomamente programmi provenienti dall'esterno, sussistendo infatti il grave pericolo di introdurre Virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti. L'inosservanza della presente disposizione espone la stessa Azienda a gravi responsabilità civili; si evidenzia inoltre che 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 quindi non protetto dal diritto d'autore, vengono sanzionate anche penalmente.

Salvo preventiva espressa autorizzazione del personale della U.O.C. "Sistemi Informativi", non è consentito all'utente modificare le caratteristiche impostate sul proprio personal computer o sulla PdL in generale, né procedere ad installare dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, modem/router USB, dispositivi di memorizzazione USB ecc…).

Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il personale della U.O.C. "Sistemi Informativi" nel caso in cui siano rilevati virus o altre anomalie concernenti la sicurezza informatica.

A tale riguardo, in caso di segnalazioni relative ad eventi tipo (si riporta un elenco non esaustivo):

- Ricezione di e-mail sospette contenenti link o allegati potenzialmente malevoli;
- Accessi non autorizzati o tentativi ripetuti di accesso con credenziali errate;

- Malfunzionamenti improvvisi di applicativi o PdL correlati a possibili infezioni da malware;
- Blocco o criptazione di file/cartelle aziendali non imputabile ad attività lecite;
- Rilevazione di dispositivi esterni collegati senza autorizzazione (USB, router, Wi-Fi, ecc.)

Dovrà essere comunicata tramite mail alla casella di posta sicurezza.informatica@asl.bari.it, all'attenzione del Direttore U.O.S.V.D. Cybersecurity.

RICHIESTA DI NUOVA PDL O SOSTITUZIONE DI PDL

Le Unità Operative potranno richiedere alla U.O.C. "Sistemi Informativi" la fornitura di una nuova PdL o la sostituzione della PdL in uso utilizzando esclusivamente gli appositi moduli (*Allegato 1 - Modulo nuovo HW* e *Allegato 2 - Modulo spostamento HW*).

All'interno del modulo dovranno essere evidenziate le tipologie di apparecchiature da installare (PC, portatili, stampanti, multifunzione ecc) e altre funzioni utili all'attività installazione e configurazioni, come specificato sul modulo stesso.

Si precisa che, come indicato nel modulo sopra richiamato, la richiesta dovrà essere corredata del visto del Direttore della Struttura di afferenza. La stessa, successivamente, sarà trasmessa via mail alla casella supporto.ict@asl.bari.it per la generazione di un ticket, che consentirà la pianificazione dell'attività, in base all'urgenza, alla complessità e alla necessità.

Laddove si renda necessario, formattare, cancellare o spostare dei dati tutti o in parte contenuti nell'hard disk della pdl l'utente dovrà compilare l'apposito modulo *(Allegato 3 Modulo manutenzione HW)* e procedere all'invio alla casella di posta di cui sopra.

RICHIESTA DI ACCOUNT DI DOMINIO

Per ottenere le credenziali di accesso al dominio aziendale, ogni incaricato deve presentare apposita richiesta utilizzando il modulo predisposto dalla U.O.C. Sistemi Informativi (*Allegato 8 – Modulo richiesta account dominio*). La richiesta deve essere autorizzata e firmata dal Responsabile della Struttura di appartenenza, il quale certifica la necessità dell'accesso per finalità istituzionali e lavorative.

Il modulo, compilato in tutte le sue parti, deve essere trasmesso al servizio di Help Desk tramite casella di posta dedicata supporto.ict@asl.bari.it. Successivamente, gli Amministratori di Sistema provvederanno alla creazione dell'account di dominio, attribuendo credenziali personali e non cedibili, che saranno collegate univocamente all'utente richiedente.

Al primo accesso l'utente è tenuto a modificare la password iniziale, conformemente alle regole di sicurezza vigenti (complessità, lunghezza, rotazione periodica). In caso di cessazione del rapporto di lavoro, trasferimento o cambio di mansioni, l'account verrà immediatamente disattivato dal personale della U.O.C. Sistemi Informativi, previa comunicazione del Responsabile di Struttura.

MODALITÀ DI ACCESSO ALLA RETE ED AGLI APPLICATIVI

Gli utenti possono accedere alla rete e agli applicativi aziendali previa autorizzazione ed esclusivamente per finalità compatibili con le attività lavorative svolte. Al fine di garantire la corretta operatività delle attività lavorative mediante l'utilizzo di tali strumenti, è vietato:

- utilizzare le risorse assegnate per scopi che esulano dalle attività lavorative;
- utilizzare le risorse assegnate in modo da compromettere la stesse dal punto di vista dell'integrità, riservatezza e disponibilità;
- utilizzare software e hardware non acquisito dalla struttura sanitaria, che potrebbe portare all'introduzione di codice malevolo sulla rete aziendale;
- scaricare, copiare, distribuire software non licenziato, documenti, musica, filmati in violazione o in presunta violazione delle leggi sul diritto d'autore;
- modificare, senza previa autorizzazione, le configurazioni o i dati sui dispostivi telematici e informatici in uso;
- eseguire attività non strettamente correlate con l'attività lavorativa che potrebbero causare un degrado delle prestazioni di sistema;
- accedere alla rete aziendale attraverso software di accesso remoto non autorizzato dalla struttura sanitaria;
- utilizzare account assegnati ad altri utenti;
- comunicare ad altri le proprie credenziali personali di autenticazione o utilizzare le credenziali di autenticazione di altri utenti, anche se solo temporaneamente.

È responsabilità di ogni utente adottare tutte le misure di sicurezza necessarie a prevenire eventuali accessi non autorizzati, furti, danneggiamenti o altre violazioni nell'utilizzo delle risorse informatiche, e a segnalare eventuali violazioni delle medesime alle Unità Operative afferenti al comparto IT.

La concessione in uso della rete e degli applicativi dell'ASL, pertanto, oltre alla responsabilità dei singoli utilizzatori, coinvolge anche specifiche responsabilità delle strutture coinvolte ed è revocabile in qualsiasi momento per la condotta e/o per attività non conformi alle regole del presente documento e più in generale a leggi o regolamenti vigenti.

PRINCIPI GENERALI

Qualsiasi accesso alla rete e agli applicativi deve essere associato alle credenziali di una persona fisica, cui saranno collegate tutte le attività svolte.

L'incaricato che ottiene l'accesso alla rete e agli applicativi si impegna ad osservare il presente regolamento e le altre norme disciplinanti le attività e i servizi che si svolgono via rete e si impegna a non commettere abusi e a non violare i diritti degli altri incaricati e dei terzi;

L'incaricato che ottiene l'accesso alla rete e agli applicativi si assume la totale responsabilità delle attività svolte sulla rete tramite le proprie credenziali (Username - Password);

Al primo collegamento alla rete e agli applicativi, l'incaricato (Interno od Esterno) deve modificare la password (parola chiave) comunicatagli dal custode delle password, che gliela concederà se sarà rispettato quanto di seguito descritto.

SOGGETTI CHE POSSONO AVERE ACCESSO ALLA RETE

Hanno diritto ad accedere alla rete Aziendale tutti gli incaricati, le ditte fornitrici di software per motivi di manutenzione e limitatamente alle applicazioni di loro competenza, collaboratori esterni impegnati nelle attività istituzionali per il periodo di collaborazione.

L'amministratore di sistema regolamenta l'accesso alla rete di determinate categorie di incaricati in base alla categoria di appartenenza secondo quanto indicato dal Delegato al trattamento dei dati – SATD.

Per garantire la sicurezza e il miglior funzionamento delle risorse disponibili, l'amministratore di sistema può proporre al titolare del trattamento l'adozione di appositi regolamenti di carattere operativo che gli incaricati si impegnano ad osservare.

In generale l'accesso agli applicativi è consentito agli incaricati che, per motivi di servizio, ne devono fare uso.

CREDENZIALI DI ACCESSO ALLA RETE INFORMATICA

Le credenziali sono strettamente personali.

È invece ammesso che ad una persona venga assegnata più di una credenziale di autenticazione, se richiesto dal Responsabile del Trattamento.

Lo Username deve essere associato in maniera univoca e non può essere riassegnato neanche in tempi successivi ad altro incaricato.

La disattivazione delle credenziali di autenticazione è immediata:

- nel caso in cui l'incaricato non sia più in servizio, o sia destinato ad altre funzioni rispetto a quella per cui era previsto l’accesso allo strumento;
- dopo tre mesi di mancato utilizzo, con l'unica eccezione delle credenziali che sono state preventivamente autorizzate per soli scopi di gestione tecnica, il cui utilizzo è quindi sporadico;
- dopo cinque tentativi falliti di accesso.

Elaborare in modo appropriato la password e conservarla con segretezza. Agli incaricati è imposto l'obbligo, automatizzato dal sistema, di provvedere a modificare la password, con la seguente tempistica:

- immediatamente, non appena viene consegnata loro da chi amministra il sistema;
- successivamente, ogni mese.

La password deve almeno

- avere una lunghezza minima di 12 caratteri, preferibilmente di 14 caratteri
- essere composte di caratteri alfanumerici con la presenza di caratteri maiuscoli e minuscoli
- contenere almeno un carattere speciale (!,?,$,&, ecc...)
- NON contenere nome/cognome proprio o informazioni personali come la data di nascita
- essere uniche per ciascun servizio o sito a cui si accede

La password non deve contenere riferimenti agevolmente riconducibili all'interessato (non solo nomi, cognomi, soprannomi, ma neppure date di nascita proprie, dei figli o degli amici), né consistere in nomi noti, anche di fantasia (pippo, pluto, paperino, etc.…).

Nel proprio interesse, l'incaricato deve immediatamente richiedere la sostituzione delle credenziali, qualora ne accertasse la perdita o ne verificasse una rivelazione surrettizia. Infatti, tutte le azioni riferibili ad una password saranno addebitate all'incaricato cui appartiene, che di conseguenza se ne dovrà assumere le responsabilità;

La password non deve essere comunicata a nessuno, né esposta su promemoria cartaceo, (non solo a soggetti esterni, ma neppure a persone appartenenti all'ASL, siano esse colleghi, delegati al trattamento dei dati – SATD. Può essere rilasciata temporaneamente, e poi ricambiata, all'Amministratore di Sistema per necessità contingenti di assistenza al profilo dell'incaricato.

ATTIVITÀ NON CONSENTITE NELL'USO DELLA RETE

A tutti è assolutamente fatto divieto di collegare alla rete qualsiasi strumento elettronico (PC, Stampanti, Scanner, Router Wi-Fi, Telefoni, …) non autorizzato all'amministratore di sistema ASL. Strumenti di terze parti possono essere collegati alla rete se previsti in un contratto di forniture e preventivamente autorizzati.

Non sono inoltre consentite le seguenti attività:

- Utilizzare le Risorse Tecnologiche per usare, archiviare, detenere, duplicare o diffondere in qualunque forma materiali tutelati da diritti d'autore o diritti connessi o sui quali terzi vantino diritti morali e patrimoniali (D.lgs. n. 68/2003, Legge 22 Aprire 1941 n.633 e successive modificazioni);
- Usare la rete in modo difforme da quanto previsto dalle leggi penali, civili e amministrative e da quanto previsto dal presente regolamento;
- Utilizzare la Rete e in generale le risorse informatiche dell'ASL per scopi incompatibili con l'attività istituzionale dell'ASL stessa;
- Conseguire l'accesso non autorizzato a risorse di rete interne ed esterne alla Rete;
- Violare la riservatezza di altri incaricati o di terzi;
- Agire deliberatamente con attività che influenzino negativamente la regolare operatività della Rete e ne restringano l'utilizzabilità e le prestazioni per altri incaricati;
- Effettuare o permettere ad altri trasferimenti non autorizzati di informazioni (software, dati, etc.…);

- Installare qualsiasi programma da parte dell'incaricato o di altri operatori, se non previa autorizzazione degli amministratori di sistema;
- Installare applicativi non compatibili con l'attività istituzionale:
- Disinstallare, cancellare, copiare o asportare programmi software per scopi personali;
- Installare componenti hardware senza preventiva autorizzazione degli amministratori di sistema;
- Rimuovere, danneggiare o asportare componenti hardware e software fornite dall'amministratore di sistema;
- Utilizzare qualunque tipo di sistema informatico o elettronico per controllare le attività di altri incaricati, per leggere, copiare o cancellare files e software di altri incaricati;
- Utilizzare software visualizzatori di pacchetti TCP/IP, software di intercettazione di tastiera, software di decodifica password e più in generale software rivolti alla violazione della sicurezza del sistema e della privacy;
- Inserire password locali alle risorse informatiche assegnate (come, ad esempio, password che non rendano accessibile il computer agli amministratori di rete), se non prima comunicate agli amministratori di sistema e da questi espressamente autorizzate;
- Abbandonare il posto di lavoro lasciandolo senza protezione da accessi non autorizzati.

POSTA ELETTRONICA

Il servizio di posta elettronica è concesso esclusivamente ai dipendenti e agli operatori dei quali sia riconosciuta l'attività coerente con i fini lavorativi e istituzionali dell'Ente. Ogni delegato al trattamento dei dati – SATD può richiedere l'assegnazione di una casella di posta elettronica per motivi di servizio per i propri collaboratori, compilando l'apposito modulo (Allegato 7 - Modulo richiesta posta elettronica) allegato al presente regolamento.

È anche possibile attivare indirizzi di posta elettronica per le strutture aziendali, condivisi dagli operatori assegnati a ciascuna di esse (es.: formazione.assistentisociali@asl.bari.it, pnrr.salute@asl.bari.it, ecc.).

Al singolo incaricato può essere assegnato un indirizzo e-mail personale del tipo: nome.cognome@asl.ba.it.

La "personalizzazione" dell'indirizzo non comporta la sua "privatezza", in quanto trattasi di strumenti di esclusiva proprietà aziendale, messi a disposizione del dipendente al solo fine dello svolgimento delle proprie mansioni lavorative.

Nei messaggi inviati tramite posta elettronica aziendale (di servizio e/o nominative) verrà accluso il seguente testo:

"Il presente messaggio, corredato degli eventuali allegati, contiene informazioni da considerarsi strettamente riservate e confidenziali. Ne è vietato l'uso improprio, la diffusione, la distribuzione o la riproduzione da parte di altre persone e/o entità diverse da quelle specificate. Qualora lo abbiate ricevuto per errore, vi preghiamo di distruggere il messaggio, comunicando l'errata ricezione tramite il reply all'indirizzo mittente.

ED IN INGLESE:

This e-mail, any attachments and the information contained there in ("this message") are confidential and intented solely for the use of the addressee (s). If you have received this message in error please send it back to the sender and delete it. Unauthorized publication, use, dissemination or disclosure of this message, either in whole or in part is strictly prohibited. .”

Il sistema è soggetto ad un controllo preventivo su ogni casella tramite gli strumenti di filtro di protezione antispam/antivirus.

La dimensione della casella di posta rilasciate dall’Amministrazione di Sistema è in funzione delle risorse disponibili e delle esigenze di servizio.

Le caselle di posta sono consultabili sia all’interno dell’Azienda, che dall’esterno, tramite il seguente link: https://outlook.office365.com/mail/inbox e digitando la propria casella di posta e la propria password.

Ogni incaricato, cui è concesso un indirizzo di Posta Elettronica deve rispettare le regole e i divieti che seguono.

REGOLE DI GESTIONE DELLA CASELLA DI POSTA

È fatto espressamente obbligo agli incaricati di Posta Elettronica di esercitare una corretta gestione sulla propria casella di posta. Pertanto, ogni incaricato è tenuto ad eliminare regolarmente i messaggi da cancellare;

Ogni incaricato si impegna a consultare con regolarità la propria casella di posta elettronica;

Gli amministratori di sistema, cui è demandato il compito di gestire le risorse assegnate al servizio di Posta Elettronica, disattiveranno, a seguito di controlli periodici, le caselle di posta non consultate da oltre 90 giorni, a meno che l'incaricato non abbia comunicato agli stessi, la giustificata impossibilità di consultarla per un periodo così lungo.

ATTIVITÀ NON CONSENTITE NELLA GESTIONE DELLA POSTA ELETTRONICA

Non sono consentite le seguenti attività di utilizzo della casella di posta aziendale e dei servizi di produttività manuale associati alla Suite:

* L'utilizzo della posta elettronica per fini diversi da quelli istituzionali;
* Un uso che possa in qualche modo recare qualsiasi danno all'ASL o a terzi, come l'apertura di allegati in messaggi di posta elettronica senza il previo accertamento dell'identità del mittente;
* Inoltrare "catene" di posta elettronica, anche se afferenti a presunti problemi di sicurezza;
* La trasmissione a mezzo di posta elettronica di dati sensibili, confidenziali e personali di alcun genere, salvo i casi espressamente previsti dalla normativa vigente in materia di protezione dei dati personali (come da disposizioni del vigente GDPR).

SOLUZIONI DI ACCESSO ALLE CASELLE DI POSTA PER GARANTIRE LA CONTINUITÀ LAVORATIVA

Ciascun incaricato può, anche da postazioni esterne all'azienda, utilizzare specifiche funzionalità di posta elettronica per inviare automaticamente, in caso di assenza, messaggi di risposta che informino il mittente della propria indisponibilità, e funzioni di inoltro automatico dei messaggi ricevuti verso indirizzi di altro personale dipendente.

Nel caso in cui un dipendente si assenti senza aver provveduto ad attivare i suddetti sistemi di inoltro automatico, un fiduciario, da lui preventivamente nominato, o, in sua assenza, il delegato al trattamento dei dati – SATD potrà accedere alla casella di posta al fine di garantire la continuità dell'attività lavorativa.

La nomina del fiduciario deve essere redatta in forma scritta, riportare la sottoscrizione del fiduciante e del fiduciario e dovrà essere consegnata al delegato al trattamento dei dati – SATD.

ACCESSO AD INTERNET ED USO RETE AZIENDALE

L'uso di Internet nelle sue numerose funzionalità è consentito esclusivamente per gli scopi attinenti al proprio lavoro.

Data la vasta gamma di attività aziendali, non è stato definito a priori un elenco di siti aziendali autorizzati; si è tuttavia optato per l'utilizzo di appositi strumenti di filtraggio, mediante i quali è stata bloccata la navigazione su categorie di siti i cui contenuti sono stati classificati come certamente estranei agli interessi ed alle attività aziendali.

Il divieto di accesso ad un sito appartenente alle categorie inibite viene visualizzato esplicitamente a video.

Viene altresì limitata la possibilità di scaricare (download) da Internet file musicali, video o software che non siano necessari alla propria attività aziendale.

ATTIVITÀ NON CONSENTITE NELL'UTILIZZO DELL'ACCESSO A INTERNET

Non sono consentiti i seguenti utilizzi della Rete di connettività dati aziendale:

* L'uso di Internet per motivi personali;
* Accedere direttamente ad Internet con modem collegato al proprio Personal Computer se non espressamente autorizzati dagli amministratori di sistema e per particolari motivi tecnici;
* L'accesso a siti inappropriati (esempio siti pornografici, di intrattenimento, home banking, social network, ecc.);
* Lo scaricamento (download) di software e di file non necessari all'attività istituzionale;
* Utilizzare programmi per la condivisione e lo scambio di file in modalità peer to peer;

* Accedere a flussi in streaming audio/video da Internet per scopi non istituzionali (ad esempio ascoltare la radio o guardare video o filmati utilizzando le risorse Internet).

MEMORIZZAZIONE FILE DI LOG DELLA NAVIGAZIONE INTERNET

Al fine di verificare la funzionalità, la sicurezza del sistema ed il suo corretto utilizzo, le apparecchiature di rete preposte al collegamento verso internet, memorizzano un elenco (file di log) contenente le informazioni relative ai siti visitati.

L'accesso a questi dati è effettuabile esclusivamente dall'Amministratore di Sistema. L'eventuale trattamento statistico dei dati sarà effettuato in forma anonima. L'identificazione dei dati riferiti ad un singolo incaricato potrà essere elaborata solo a seguito di specifica richiesta dell'Autorità Giudiziaria.

I sistemi software saranno programmati e configurati in modo da cancellare periodicamente i dati relativi agli accessi ad Internet ed al traffico telematico.

Eventuali deroghe ai tempi di conservazione saranno eccezionali e solo in relazione all'indispensabilità del dato rispetto all'esercizio, o alla difesa di un diritto in sede giudiziaria, oppure all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'Autorità Giudiziaria.

GESTIONE DI STRUMENTI ELETTRONICI / INFORMATICI INDIVIDUALI

Tutti i documenti prodotti e più in generale tutti i dati a valenza aziendale, possono essere memorizzati, per ciascuna struttura, attraverso due modalità:

1. sulle aree condivise del file server appositamente dedicate all'archiviazione documentale. La sicurezza dei documenti conservati sulle apposite aree del server è a cura della U.O.C. "Sistemi Informativi";
2. mediante lo spazio su cloud aziendale compreso nella Suite Office 365, **One Drive** e **SharePoint**, che mette a disposizione, dai 50 Gb ai 100 Gb per ogni utente, a seconda della tipologia di licenza (rispettivamente F3 o E1). **Questa modalità è caldamente raccomandata, consentendo maggiore flessibilità, portabilità e possibilità di collaboration nel pieno rispetto della sicurezza e della tutela dei dati**.

Viene tassativamente vietato l'utilizzo delle risorse dell'ambiente di File Sharing aziendale (il cosiddetto "File server" o "cartelle condivise") e delle postazioni di lavoro locali per la memorizzazione di materiale privato, personale o non attinente all'attività lavorativa.

È fatto divieto di salvare dati sensibili (ad esempio scansioni di cartelle cliniche, prestazioni sanitarie erogate ai pazienti, schede terapeutiche, ecc…) negli ambienti condivisi di File Sharing e nel cloud aziendale. per questi dati sono a disposizione gli appositi applicativi aziendali.

Eventuali deroghe a questa disposizione dovranno avere l'autorizzazione da parte del DPO aziendale e prevedere che i file siano crittografati con modalità per le quali il servizio U.O.C. "Sistemi Informativi" è a disposizione per il supporto.

Ulteriori dettagli sono nel paragrafo seguente "Gestione dell'ambiente di cartelle condivise"

Relativamente all'utilizzo dei singoli Personal Computer si precisa che l'assegnazione della risorsa non autorizza ad utilizzo personale, in quanto trattasi di strumento di esclusiva proprietà aziendale.

I file memorizzati sui singoli PC non sono né tutelati né garantiti dall'Azienda per qualsiasi causa. Non è previsto né il salvataggio, né il ripristino dei dati memorizzati in locale sui PC.

Per tutti gli incaricati cui è concesso l'accesso alla rete e agli strumenti elettronici dell'ASL, devono essere adottate le seguenti misure:

- divieto per gli utilizzatori di strumenti elettronici di lasciare incustodito, o accessibile il dispositivo affidato; l'incaricato in caso di allontanamento deve disconnettersi dal Sistema Operativo;
- divieto di installazione di software ed accessi remoti non autorizzati, se non da parte dell'Amministratore di Sistema;
- divieto di effettuare copie di dati dell'Ente su supporti esterni / estraibili;
- divieto assoluto di memorizzare dati personali e/o sensibili sulla propria postazione di lavoro.

GESTIONE DELL'AMBIENTE DI CARTELLE CONDIVISE

Per ogni Centro di Responsabilità (CdR) aziendale sarà disponibile, previa richiesta alla U.O.C. "Sistemi Informativi" secondo le modalità descritte nel paragrafo seguente, **un'unica cartella avente per nome il codice CdR.**

A tale riguardo si precisa che, in linea con le evoluzioni tecnologiche e con gli standard di sicurezza richiesti dalla normativa vigente, l'Azienda sta progressivamente migrando la gestione dei file e delle cartelle condivise dal tradizionale File Server aziendale alle piattaforme **OneDrive for Business** e **SharePoint Online**, già incluse nella suite Microsoft 365.

Questa transizione ha lo scopo di garantire:

- **maggiore sicurezza dei dati**, grazie a sistemi di cifratura, autenticazione a più fattori e monitoraggio centralizzato degli accessi;
- **continuità operativa**, con funzionalità di versioning, recupero file e sincronizzazione tra dispositivi;
- **collaborazione avanzata**, permettendo la modifica simultanea dei documenti, la condivisione sicura con colleghi interni e, se autorizzato, con partner esterni;

- **flessibilità di accesso**, da rete interna ed esterna, mantenendo i requisiti di riservatezza e integrità dei dati.

Durante la fase di transizione, che sarà comunicata con opportune istruzioni operative da parte della Direzione della Struttura, le cartelle condivise esistenti rimarranno disponibili in sola lettura per un periodo di tempo definito, al fine di consentire alle strutture aziendali di spostare i contenuti nei nuovi spazi cloud. La U.O.C. Sistemi Informativi fornirà supporto operativo ai referenti di ciascun Centro di Responsabilità (CdR) per la migrazione e per la corretta gestione dei permessi su OneDrive e SharePoint.

Il salvataggio di dati personali e particolari (sensibili), in particolare dati sanitari dei pazienti, rimane comunque **vietato** anche nei nuovi ambienti cloud, che devono essere utilizzati esclusivamente per documentazione amministrativa e operativa. Per il trattamento dei dati sanitari sono disponibili gli applicativi aziendali dedicati.

MODALITÀ DI RICHIESTA DI UNA NUOVA CARTELLA CONDIVISA

Le indicazioni che seguono fanno riferimento agli utenti che usano l'attuale sistema di File Sharing per finalità di produttività individuale e/o di reparto.

Non sono contemplati in questo paragrafo i casi relativi all'uso delle cartelle condivise per i software dei dispositivi elettromedicali.

Tali esigenze saranno valutate dall'Area ICT mediante apposita documentazione progettuale a sostegno da parte dei reparti interessati e/o dell'ingegneria Clinica.

Contestualmente all'attivazione della Cartella Condivisa, ogni Responsabile di CdR dovrà individuare ed autorizzare un **amministratore referente** della cartella stessa indicandone il nome via mail a supporto.ict@asl.bari.it. Il referente avrà la responsabilità di tutti i dati che verranno salvati sulla propria cartella e pertanto sarà l'unico autorizzato ad usare gli strumenti di amministrazione forniti a tale scopo.

Tale organizzazione è coerente con la nomina dei delegati al trattamento dei dati personali come da regolamento aziendale per il trattamento dei dati personali, ai sensi del D.lgs. n.101/2018 in attuazione del GDPR Regolamento Europeo 2016/679.

La U.O.C." Sistemi Informativi" fornirà ad ogni referente il supporto per gestirne i permessi di autorizzazione.

CAPIENZA DELLE CARTELLE CONDIVISE

Ogni Cartella Condivisa avrà una capienza standard di **5 Gigabyte**. Eventuali richieste di ampliamento dello spazio allocato, se opportunamente motivate, saranno valutate dalla U.O.C." Sistemi Informativi" in base alla disponibilità di risorse sui server e sulle unità di backup.

CONTENUTI E FORMATO DEI DOCUMENTI

Le nuove cartelle condivise dovranno essere utilizzate esclusivamente per il salvataggio dei documenti statici di office automation inerenti all'attività istituzionale e non per applicativi multi-utenza, quali ad esempio MS Access,

OO Base (Apache OpenOffice Base, in precedenza OpenOffice.org), etc., che richiedono specifici progetti e attrezzature informatiche. Non potranno altresì contenere dati sensibili, men che meno dei pazienti e non saranno consentite scansioni di cartelle cliniche, copie di esami, richieste di prestazioni sanitarie, immagini diagnostiche e quant'altro possa compromettere il diritto alla riservatezza dei dati sanitari verso il paziente.

Le cartelle condivise non possono in alcun modo essere utilizzate, nemmeno per brevi periodi, per scopi diversi da quelli istituzionali.

Potranno essere salvati solo documenti nei seguenti formati:

* .ods - .odt - .odp
* .docx -. xIsx - .pptx
* .zip - .rar - .7z
* .htm - .html
* .txt - .rtf - .pdf

Nel caso fosse necessario salvare documenti con formati diversi da quelli elencati, gli interessati dovranno inviare, in allegato alla richiesta di attivazione, una relazione in cui, per ogni formato richiesto, vengano esposti i motivi di tale necessità, al fine di permettere alla U.O.C. "Sistemi Informativi" di valutare la richiesta.

MODALITÀ ACCESSO UTENTE

L'accesso alle nuove cartelle condivise sarà consentito esclusivamente agli utenti in possesso delle credenziali del dominio "asl.bari.it" (vedi Posta elettronica) e autorizzati dagli amministratori delle cartelle condivise.

RISERVATEZZA ED INTEGRITÀ DEI DATI

I file presenti su una specifica cartella condivisa saranno fruibili solo dagli utenti espressamente autorizzati dall'amministratore, che potrà concedere privilegi di accesso differenziati (sola lettura e/o scrittura/modifica). Ogni cartella potrà contenere sotto-cartelle, ognuna delle quali potrà avere a sua volta privilegi di accesso diversi rispetto alla cartella madre (una sotto-cartella potrà, ad esempio, essere abilitata solo ad un sotto gruppo degli utenti abilitati all'accesso alla cartella madre).

Il nuovo regolamento UE sulla protezione dei dati personali (GDPR) impone dei limiti al trattamento di dati personali/particolari (sensibili).

Ricordando che la modalità corretta di gestione di questa tipologia di dati è l'utilizzo dei sistemi informativi aziendali preposti **è vietato il salvataggio di dati personali/particolari (sensibili) nelle cartelle condivise**.

Costituisce buona regola la periodica cancellazione (almeno mensile) di file obsoleti, di documenti non più necessari all'attività d'ufficio e l'uso di archivi compressi (file di tipo ".zip", ".7z") per i dati storici e/o raramente utilizzati, al fine di liberare spazio e velocizzare le operazioni di back-up.

La SC Area ICT si riserva la facoltà di procedere alla rimozione di qualsiasi file o applicazione memorizzata nelle unità di rete qualora ritenuto pericoloso per la sicurezza del sistema.

ASSISTENZA

Tutte le richieste di assistenza saranno accettate solamente se provenienti dai referenti delle cartelle condivise. Ogni quesito potrà essere esposto dal referente al servizio di 'HELP-DESK dell'Area ICT tramite mail supporto.ict@asl.bari.it e telefono 080 584 2900.

GESTIONE DELLE VPN

I dipendenti e/o i fornitori, attraverso una VPN (Virtual Private Network), possono accedere alle risorse aziendali autorizzate previa opportuna richiesta via mail all'indirizzo sicurezza.informatica@asl.bari.it e seguendo le indicazioni contenuto nella procedura aziendale relativa.

Per la richiesta di accesso da parte di dipendenti interni alla ASL Bari, è obbligatorio compilare il modulo di cui all'*Allegato 5 - Modulo richiesta VPN interni*, debitamente sottoscritto.

Per la richiesta di accesso da parte di fornitori o soggetti esterni autorizzati, è obbligatorio compilare il modulo di cui all'*Allegato 6 - Modulo richiesta VPN esterni*, debitamente sottoscritto. A tale riguardo, si ribadisce che l'accesso remoto tramite VPN da parte di terzi (fornitori) è consentito solo previa nomina formale come Responsabili del trattamento ai sensi dell'art. 28 GDPR.

Nota bene: per l'accesso VPN

- L'accesso VPN non è un modo per accedere alla rete aziendale da fuori, ma una misura di emergenza per accedere ad alcuni servizi dell'infrastruttura informatica. Questi servizi devono essere indispensabili ed utilizzati solo se non è possibile diversamente.
- Ogni servizio esposto con la VPN aumenta comunque i rischi di attacco dall'esterno. Pertanto, è indispensabile individuare i servizi vitali per le urgenze.
- L'accesso VPN alle singole postazioni di lavoro crea enormi problemi di sicurezza. I servizi vitali devono essere fruibili direttamente dalle postazioni remote tramite appositi portali (nati per fare solo quello). All'interno di questi portali ci sono tecnologie che permettono l'utilizzo di appositi gateway vedi ad esempio le tecnologie terminal server. Questi sistemi ovviamente non garantiranno l'accesso a tutti gli applicativi aziendali ma solo quelli certificati a livello di sicurezza. Gli applicativi non certificati potranno quindi essere utilizzati solo da rete locale.

La modalità di accesso prevede l'autenticazione a due fattori (MFA) e l'invio preventivo di una mail personale a cui inviare il codice temporaneo (OTP) di accesso.

L'accesso agli operatori sanitari è garantito a valle dell'autorizzazione da parte della Direzione Medica di Presidio e della Direzione Sanitaria.

È espressamente vietato utilizzare le risorse informatiche e la rete aziendale per scopi incompatibili con quelli stabiliti nel presente Regolamento. In particolare, a titolo esemplificativo e non esaustivo, è vietato:

- accedere all'infrastruttura del Titolare per conseguire l'accesso non autorizzato a risorse di rete interne od esterne al Titolare;
- fornire il servizio di connettività di rete a soggetti non autorizzati all'accesso all'infrastruttura;

- violare gli obblighi contrattualmente assunti dal Titolare per la realizzazione e la gestione della propria infrastruttura, particolarmente in materia di diritto d'autore, licenze d'uso di software e regolamenti dei fornitori di connettività di rete;
- svolgere attività che causino malfunzionamento, diminuiscano la regolare operatività, danneggino o restringano l'utilizzabilità o le prestazioni dei sistemi del Titolare;
- violare la sicurezza di archivi e banche dati, compiere trasferimenti non autorizzati di informazioni (software, basi dati, ecc.), intercettare, tentare d'intercettare o accedere a dati in transito sull'infrastruttura del Titolare, dei quali non si è destinatari specifici;
- compiere azioni in violazione delle norme a tutela delle opere dell'ingegno, del diritto d'autore e del software;
- distruggere o tentare di distruggere, danneggiare o tentare di danneggiare, intercettare o tentare di intercettare, accedere o tentare di accedere senza autorizzazione alla posta elettronica o ai dati di altri Utenti o di terzi, usare, intercettare o diffondere o tentare di intercettare o diffondere password o codici d'accesso o chiavi crittografiche di altri Utenti o di terzi, e in generale commettere o tentare di commettere attività che violino la riservatezza di altri Utenti o di terzi, così come tutelata dalle norme civili, penali e amministrative applicabili.

Il servizio tecnico della U.O.C. "Sistemi Informativi" e della U.O.S.V.D. "Cybersecurity" può disattivare, in qualsiasi momento, le credenziali o disconnettere un accesso VPN, senza necessità di preventivo avviso, qualora la disattivazione sia necessaria all'integrità o al funzionamento dei propri servizi ICT, oppure qualora vi sia fondato sospetto che l'utente VPN abbia violato il presente Regolamento. Il servizio tecnico della U.O.S.V.D. "Cybersecurity" utilizzerà sia sistemi di monitoraggio della rete che sistemi in grado di verificare che l'operato dell'Utente VPN risponda a quanto previsto dal presente Regolamento e nel rispetto delle normative vigenti.

L'uso delle credenziali è strettamente personale; è assolutamente vietato affidare e/o condividere le credenziali personali con più soggetti. Il Delegato al trattamento dei dati – SATD interno e il fornitore dovranno comunicare immediatamente eventuali situazioni in cui le credenziali debbano essere disattivate, soprattutto in caso di:

- licenziamento dell'utilizzatore della VPN;
- trasferimento dell'utilizzatore ad altre mansioni;
- cessazione del rapporto contrattuale;
- incidente di sicurezza (smarrimento password o altro evento che possa coinvolgere la confidenzialità degli accessi e dei dati trattati).

ASSISTENZA DA REMOTO E SERVIZI DI REPERIBILITÀ

Il personale tecnico della U.O.C. "Sistemi Informativi" effettua attività di help desk e assistenza sia on-site che da remoto. Entrambe le tipologie di attività sono attivabili dagli utenti dell'ospedale mediante:

- chiamata al numero interno 080 584 2900

- mail all'indirizzo: supporto.ict@asl.bari.it
- compilazione dell'apposito form del sistema di Trouble Ticketing aziendale "T-Quadro" (di prossima attivazione).

Le attività on-site sono relative alle Installazioni, Movimentazioni, Aggiunte e Cambi (IMAC) di hardware afferente alle PdL e/o alla infrastruttura di connettività aziendale (sia dati che fonia: router, switch, prese di rete, telefoni, ecc…).

Le attività da remoto sono relative ai seguenti ambiti:

- risoluzione di incident inerenti agli applicativi software in dotazione;
- gestione o risoluzione di problemi relativi alle PdL che non comportino le attività IMAC prima citate;
- richiesta di attivazione o riconfigurazione di utenze;
- richieste di accesso al dominio o risoluzione di problemi relativi ad esso;
- richieste di accesso alla posta elettronica o risoluzione di problemi relativi;
- gestione dell'infrastruttura di rete, sia dati che fonia che non comportino le attività IMAC prima citate.

Tali attività sono eseguite mediante opportuni sistemi di controllo remoto dei desktop e sempre previo consenso dell'operatore che effettua la segnalazione.

Gli operatori del servizio di help desk della U.O.C. "Sistemi Informativi", a seguito della segnalazione telefonica o dell'apertura del ticket secondo le modalità su indicate (mail o compilazione del form sulla Intranet):

1. procedono all'apertura del ticket a seguito della presa in carico della chiamata;
2. assegnano il ticket all'operatore disponibile o preposto all'attività richiesta;
3. eseguono l'intervento, nel caso sia sufficiente il primo livello di presa in carico;
4. contattano, in una logica di escalation verso il secondo livello, il servizio di help desk del fornitore responsabile dell'applicativo o dell'hardware oggetto della segnalazione, verificando che l'esecuzione dell'intervento da questi effettuata sia risolutiva;
5. chiude il ticket, avendo cura di dare riscontro all'utente che ha aperto la segnalazione e di corredare il ticket stesso con note esplicative della modalità di risoluzione.

Il supporto di assistenza viene fornito dal lunedì al venerdì: dalle 8,00 alle 17,00, con la presenza garantita di operatori in sede o da remoto se in smart working.

INDICAZIONI SUL SERVIZIO DI REPERIBILITÀ

Al momento della redazione del presente regolamento, la U.O.C. "Sistemi Informativi" non dispone di risorse in grado di garantire la reperibilità nel servizio di assistenza e supporto. Ai fini della copertura del servizio anche al di fuori degli orari di ufficio, è prevista entro l'anno 2025 l'attivazione di un servizio di reperibilità, nell'ambito di un contratto di gestione e manutenzione delle PdL, in modo da garantire le seguenti fasce orarie:

- dal lunedì al venerdì: dalle 20,00 alle 8,00 del giorno successivo, assistenza erogata da 1 unità di personale reperibile contattabile tramite le modalità indicate in precedenza;
- sabato e festivi: assistenza h24 erogata da personale reperibile contattabile tramite le modalità indicate in precedenza.

In particolare, è previsto un reperibile per i periodi menzionati con lo specifico compito di prendere in carico le segnalazioni pervenute, aprire i ticket relativi ed eseguire le attività di I livello con particolare riferimento ai seguenti ambiti:

- gestione o risoluzione di problemi relativi alle PdL che non comportino le attività IMAC, a meno di casi di necessità e urgenza;
- richiesta di attivazione o riconfigurazione di utenze;
- richieste di accesso al dominio o risoluzione di problemi relativi ad esso;
- richieste di accesso alla posta elettronica o risoluzione di problemi relativi;

Non sono generalmente comprese, a meno di casi di gravità e urgenza, attività di esecuzione di incident relativi a:

- applicativi in gestione a fornitori terzi (cartella clinica, sistema informativo di laboratorio, sistema informativo radiologico...);
- assistenza sull'infrastruttura di rete.

Per questi ambiti, l'operatore reperibile, a seguito della segnalazione e dell'apertura del ticket, attiva il secondo livello presso il servizio assistenza del fornitore relativo, che è tenuto a rispondere secondo gli SLA contrattuali predefiniti in base al livello di priorità assegnato dall'operatore di help desk reperibile.

GRADUALITÀ DEI CONTROLLI

Qualora si verificassero situazioni di rischio per la sicurezza del sistema informatico aziendale o un utilizzo improprio dei sistemi, nel rispetto dei principi di pertinenza e non eccedenza, le verifiche di eventuali situazioni anomale avverranno attraverso le seguenti fasi:

- Analisi aggregata del traffico di rete riferito all'intera struttura lavorativa e rilevazione della tipologia di utilizzo (e-mail, file audio, accesso a risorse estranee alle mansioni);
- Emanazione di un avviso generalizzato relativo ad un riscontrato utilizzo anomalo degli strumenti aziendali con l'invito ad attenersi scrupolosamente ai compiti assegnati ed alle istruzioni impartite. Il richiamo all'osservanza delle regole può essere circoscritto agli incaricati afferenti al settore in cui è stata rilevata l'anomalia;
- In caso di successivo permanere di una situazione non conforme, è possibile effettuare controlli circoscritti sulle singole postazioni di lavoro.

Con la stessa gradualità vengono effettuati controlli dello spazio di memorizzazione sui server aziendali attraverso le seguenti fasi:

- Analisi aggregata dei dati memorizzati sui server a livello di intera struttura lavorativa (strutture, servizi, ecc.), rilevazione della tipologia di utilizzo (file audio, file video, immagini, software non autorizzato) e relativa pertinenza con l'attività lavorativa;
- Emanazione di un avviso generalizzato relativo ad un riscontrato utilizzo anomalo degli strumenti aziendali, con l'invito ad attenersi scrupolosamente ai compiti assegnati ed alle istruzioni impartite. Il richiamo all'osservanza delle regole può essere circoscritto agli incaricati afferenti al settore in cui è stata rilevata l'anomalia;
- In caso di successivo permanere di una situazione non conforme, è possibile procedere con un'analisi puntuale ed una eventuale eliminazione del materiale non conforme anche sulle singole postazioni di lavoro.

VIOLAZIONE AL PRESENTE REGOLAMENTO

In caso di contravvenzione alle regole contenute nel presente regolamento da parte di un incaricato che possano mettere a rischio la sicurezza o compromettere il regolare funzionamento del sistema, l'Amministratore di Sistema è autorizzato a revocare le autorizzazioni ad accedere alla Rete Informatica ed ai servizi autorizzati con effetto immediato.

PROVVEDIMENTI DISCIPLINARI

Qualora, ad esito di controllo, l'Amministratore di Sistema rilevi delle anomalie sull'utilizzo dei sopracitati strumenti informatici di cui al paragrafo "GRADUALITÀ DEI CONTROLLI" che possano essere configurate quali attività non conformi, provvederà ad informare il delegato al trattamento dei dati – SATD della struttura presso la quale il dipendente presta la propria attività per effettuate le verifiche del caso.

Segnalerà inoltre l'accaduto al responsabile dell'Ufficio Procedimenti Disciplinare (della dirigenza o del comparto a seconda dell'interlocutore) per la valutazione di competenza. A seguito dell'accertamento della condotta illecita, e quindi dell'adozione del provvedimento disciplinale, l'Azienda procederà altresì a segnalare l'abuso all'Autorità competente.

ALLEGATI AL REGOLAMENTO

- Allegato 1 - Modulo nuovo HW
- Allegato 2 - Modulo spostamento HW
- Allegato 3 – Modulo manutenzione HW
- Allegato 4 – Modulo consegna HW
- Allegato 5 - Modulo richiesta VPN interni
- Allegato 6 – Modulo richiesta VPN esterni
- Allegato 7 – Modulo richiesta posta elettronica
- Allegato 8 – Modulo richiesta account dominio

REDAZIONE DOCUMENTO

	Nome e Cognome	**Ruolo**	**Data**	**Firma**
Redazione	Ing. Dario Ricci	Direttore f.f. U.O.C. “Sistemi Informativi”	29/10/2025	
Revisione	Ing. Francesco Dibattista	Direttore U.O.S.V.D. “Cybersecurity”	29/10/2025	

Elemento	**Prima versione**	**Nuova versione**
Data	30/09/2025	29/10/2025
Versione	1.0	1.1
Note	Prima emissione	Adeguamento al parere del DPO n. 78632/2025 del 15/10/2025

PROFILI CONTABILI

☐ RILEVANTE, a valere su: ☒ NON rilevante

ONERI DI PUBBLICAZIONE OBBLIGATORIA EX D. LGS. 33/2013:

☒ SOGGETTA a pubblicazione ☐ NON soggetta a pubblicazione

Sottosezione di Primo LIvello	Sottosezione di Secondo LIvello	Riferimento Normativo
Disposizioni generali	Atti generali	Art. 12, c. 1, d.lgs. n. 33/2013

ONERI DI RISERVATEZZA:

☐ CONTIENE dati personali da NON pubblicare ☒ NON contiene dati personali

DESTINATARI NOTIFICA/TRASMISSIONE

PROPOSTA N.RO 20250002567 APPROVATA CON DELIBERAZIONE N.RO 20250002242 DEL 06/11/2025

Con la sottoscrizione in calce al presente provvedimento, i firmatari di cui sopra, ciascuno in relazione al proprio ruolo come indicato e per quanto di rispettiva competenza, attestano che il procedimento istruttorio è stato espletato nel rispetto della normativa regionale e nazionale applicabile e che il provvedimento predisposto è conforme alle risultanze istruttorie agli atti d'ufficio.

I medesimi soggetti dichiarano, inoltre, di non versare in alcuna situazione di conflitto di interesse, anche potenziale, ex art. 6-bis, l. 241/90, artt. 6, 7 e 13, c. 3, D.P.R. 62/2013, vigente codice di comportamento aziendale e art. 1, c. 9, lett. e), l. 190/2012 – quest'ultimo come recepito, a livello aziendale, della vigente sezione Anticorruzione e Trasparenza del PIAO – tale da pregiudicare l'esercizio imparziale di funzioni e compiti attribuiti, in relazione al procedimento indicato in oggetto, così come di non trovarsi in alcuna delle condizioni di incompatibilità di cui all'art. 35-bis, D.L.gs. 165/2001.

RUOLO	NOME E COGNOME	FIRMA
Estensore	Paciello Margherita	*Firmato digitalmente il 04/11/2025 18:05*
Responsabile U.O.S. Affari Generali	Iorio Raffaele	*Firmato digitalmente il 04/11/2025 18:06*
Direttore f.f. U.O.C. Sistemi Informativi	Ricci Dario	*Firmato digitalmente il 05/11/2025 12:26*