Fondazione I.R.C.C.S.
Istituto Neurologico Carlo Besta

Sistema Socio Sanitario
Regione Lombardia

DISCIPLINARE PER L'UTILIZZO RISORSE ICT 2023 (Information and Communication Technology)

INDICE

1. DEFINIZIONI

Nome	Definizione
Antivirus	Programma che individua, previene e disattiva/rimuove programmi dannosi, come virus e worm.
Archivio	Raccolta ordinata logica o fisica di informazioni.
Asset	Può essere un archivio o più in generale una risorsa o un bene o un servizio. Anch'esso può avere natura fisica o logica.
Autorizzato	Ogni incaricato, come identificato di seguito, che nell'ambito dell'attività assegnatagli utilizza credenziali di accesso a strumenti informatici per il trattamento di dati.
Backup	Copia di riserva di un disco, di una parte del disco o di uno o più file su supporti di memorizzazione diversi da quello in uso.
Chat	Servizio offerto da Internet, che permette mediante apposito software una 'conversazione' fra più interlocutori costituita da uno scambio di messaggi scritti che appaiono in tempo reale sul monitor di ciascun partecipante.
Chiave USB	Detta anche unità flash USB o penna USB (in inglese: USB flash drive, o pendrive) è una memoria di massa portatile di dimensioni molto contenute che si collega al computer mediante la porta USB.
Client	Computer o programma collegato ad un altro (computer o programma) a cui inoltra le richieste dell'incaricato.
Data Breach	Violazione di sicurezza che comporta, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati (Regolamento UE 2016/679–GDPR)
Dati	L'insieme di informazioni - non solo i "dati personali" intesi a norma di legge - di cui un dipendente o un collaboratore (a prescindere dal rapporto contrattuale con l'Azienda) può venire a conoscenza e di cui deve garantire la riservatezza e la segretezza.
Dati personali	Informazioni riguardanti una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale (art. 4 GDPR).
Device (dispositivo)	Personal Computer e altra unità hardware quale periferica/dispositivo elettronico, anche ad alta tecnologia e di piccole dimensioni (smartphone, e-book reader, tablet, PC etc.).
Dipendente	Personale dell'Ente assunto con tipo di forma contrattuale, anche di stage o tirocinio.
File	Porzione di memoria (fissa o mobile) che contiene un insieme organizzato di informazioni omogenee.

File sharing	Condivisione di file all'interno di una rete di calcolatori che tipicamente utilizza una delle seguenti architetture: client-server, peer-to-peer (rete informatica in cui i nodi sono gerarchizzati sotto forma di nodi equivalenti o paritari - in inglese peer - che possono cioè funzionare da server verso gli altri nodi della rete).
GDPR	General Data Protection Regulation - Regolamento Generale sulla Protezione dei Dati - Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016.
Incaricato	Ogni dipendente, come sopra identificato, ed ogni consulente esterno che, nell'ambito dell'attività assegnatagli, tratta dati (nell'accezione del capitolo seguente) riferiti all'Azienda ed è autorizzato dal titolare o dal responsabile al trattamento dei dati personali.
LAN	È l'acronimo del termine inglese Local Area Network, in italiano rete locale. Identifica una rete costituita da computer collegati tra loro, dalle interconnessioni e dalle periferiche condivise in un ambito fisico delimitato.
Malware	Abbreviazione del termine malicious software (che significa letteralmente software malintenzionato, ma di solito tradotto come software dannoso), indica un programma informatico usato per disturbare le operazioni svolte da un computer, rubare informazioni sensibili, accedere a sistemi informatici privati, o mostrare pubblicità indesiderata.
Postazione di lavoro (PdL)	Luogo attrezzato per svolgere un'attività lavorativa dotato di personal computer ed eventuali altre unità hardware.
Phishing	Tipo di truffa effettuata su Internet attraverso cui un malintenzionato cerca di ingannare la vittima convincendola a fornire informazioni personali, dati finanziari o codici di accesso, fingendosi un ente affidabile in una comunicazione e-mail.
Repository	In un repository sono raccolti dati e informazioni in formato digitale, valorizzati e archiviati sulla base di metadati che ne permettono la rapida individuazione, anche grazie alla creazione di tabelle relazionali. Grazie alla sua peculiare architettura, un repository consente di gestire in modo ottimale anche grandi volumi di dati.
RPU	Responsabile Privacy di unità operativa
Rete locale	Una Local Area Network (LAN) (in italiano rete locale) è una rete informatica di collegamento tra più computer, estendibile anche a dispositivi periferici condivisi, che copre un'area limitata, come un'abitazione, una scuola, un'azienda o un complesso di edifici adiacenti.
Server	Computer o programma a cui altri (computer o programmi) si collegano per l'elaborazione delle richieste dell'incaricato.
SSR	Sistema Sanitario Regionale
Titolare	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del

	trattamento di dati personali. Nel nostro caso il Titolare dei dati dei pazienti e dei dipendenti e collaboratori è la Fondazione.
Virus	Programma appartenente alla categoria dei malware che, una volta eseguito, infetta dei file in modo da arrecare danni al sistema, rallentando o rendendo inutilizzabile il dispositivo infetto.

2. INTRODUZIONE

Il presente disciplinare detta le regole per l'utilizzo di sistemi informativi, di internet e della posta elettronica per la Fondazione I.R.C.C.S. Istituto Neurologico "Carlo Besta" tenuto conto che la pervasiva diffusione delle nuove tecnologie e l'accesso ad internet espone l'Istituto a possibili rischi di assoluta rilevanza in termini anche di sicurezza e di tutela del patrimonio informatico.

Per dati si intende l'insieme delle informazioni di cui un utente o un collaboratore può venire a conoscenza nell'ambito della propria attività lavorativa e di cui deve garantire la riservatezza e la segretezza, limitandosi al solo utilizzo dei dati necessari all'espletamento dell'attività lavorativa.

Nell'utilizzare gli strumenti informatici e telematici messi a disposizione dall'azienda l'utente è tenuto ad usare la massima diligenza, nel rispetto degli obblighi di cui agli articoli 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 civile, penale ed amministrativo.

A tutti gli utenti è richiesto di attenersi scrupolosamente alle leggi vigenti in termini di protezione dei dati personali quali il Reg. UE 2016/679 ed il D.Lgs. 101/18, compresa la Legge 547/93 ed il D.Lgs. 231/01 sulla criminalità informatica per quanto concerne abusi, danneggiamenti e alterazioni di software, falsi e frodi informatiche, spionaggio informatico, intercettazione ed uso abusivo di codici d'accesso, uso improprio di informazioni ottenute con mezzi illeciti.

Copia del presente Disciplinare è consegnata a ciascun Autorizzato all'atto dell'assunzione e/o ad inizio attività ed è reperibile sulla intranet aziendale. L'osservanza delle disposizioni regolate dalla normativa sopra citata deve considerarsi parte essenziale delle obbligazioni contrattuali dei dipendenti ai sensi e per gli effetti di cui all'art. 2104 codice civile. L'inosservanza delle norme sulla privacy può comportare, inoltre, sanzioni di natura civile e penale per l'Autorizzato e per la Fondazione, motivo per cui si raccomanda di prestare la massima attenzione nella lettura delle disposizioni di seguito riportate.

Le disposizioni contenute nel presente disciplinare sono dirette a garantire la sicurezza, la disponibilità e l'integrità dei sistemi informatici nel rispetto del contesto normativo di riferimento di seguito riportato:

- "Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE", che sarà direttamente applicabile in tutti gli Stati dell'Unione Europea a partire dal 25 maggio 2018 (d'ora in poi "GDPR");
- Misure Minime per la Sicurezza Informatica della Pubblica Amministrazione (CIRCOLARE AGID 18 aprile 2017, n. 2/2017);
- D.Lgs. 65/2018 n.65 – Attuazione Direttiva (UE) del Parlamento Europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione;

- D.Lgs. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali" (d'ora in poi "Codice") e s.m.i;
- Provvedimenti del Garante per la protezione dei dati personali in materia di "misure di sicurezza", in particolare con riguardo agli Amministratori di Sistema (Provvedimento generale del 27 novembre 2008);
- Garante della privacy "Linee guida per posta elettronica e internet" del 01.03.2007;
- Direttiva n. 2/2009 del Dipartimento Funzione Pubblica ad oggetto "Utilizzo di internet e della casella di posta elettronica istituzionale sul luogo di lavoro".

3. AMBITO APPLICAZIONE

Il presente disciplinare si applica a tutti gli utenti della Fondazione, ossia:

a) dipendenti, a qualsiasi titolo inseriti nell'organizzazione aziendale, senza distinzione di ruolo e/o livello;
b) Soggetti prestanti servizio per la Fondazione, a prescindere dal rapporto contrattuale.

In particolare, si rivolge a chiunque utilizzi risorse messe a disposizione dalla Fondazione stessa, quali ad esempio:

- Patrimonio informativo;
- Sistemi di elaborazione centrale;
- Servizi informatici erogati dalla Fondazione;
- PC fissi e portatili;
- Software per la comunicazione;
- Telefoni fissi e cellulari.

4. PRESA IN CARICO E RICONSEGNA DEGLI ASSET

La Fondazione si impegna a tenere traccia di tutti gli strumenti forniti in utilizzo a ciascun lavoratore.

All'atto della consegna, la Fondazione ed il lavoratore sottoscrivono apposito modulo MOD_SIA 02 *"Presa in carico e riconsegna asset"*, tramite il quale le due parti si impegnano a rispettare quanto previsto sul presente documento.

Per qualunque informazione inerente alla gestione degli asset, si rimanda all'istruzione operativa IOSIA_03 inerente alla gestione degli asset fisici.

Come esplicitamente specificato sul documento di cui sopra, la riconsegna degli asset da parte del lavoratore deve obbligatoriamente avvenire al termine del rapporto lavorativo o in qualunque altro momento, previa richiesta da parte della Fondazione, che deve essere inoltrata almeno 48 ore prima.

5. CREDENZIALI E MECCANISMI DI AUTENTICAZIONE

Ogni strumento messo a disposizione dei collaboratori dalla Fondazione (e-mail o credenziali per l'accesso a software e servizi) è da intendersi unicamente come strumento di lavoro, quale archivio per la corrispondenza da e verso soggetti terzi alla Fondazione e/o mero strumento organizzativo delle informazioni di lavoro: a tal proposito la Fondazione affida al dipendente ed ai collaboratori le credenziali di accesso ed autenticazione.

5.1. Gestione delle Credenziali di autenticazione ed accesso alla rete

Le credenziali di accesso alle risorse ed alla posta elettronica vengono assegnate dalla SC Sistemi Informativi Aziendali e per quanto riguarda gli applicativi l'abilitazione avviene, previa formale richiesta del Responsabile della Struttura Complessa o Semplice a cui è assegnato l'utente. Lo stesso Responsabile provvede, nei casi di trasferimento o cessazione del rapporto di lavoro o di collaborazione di un utente, a richiedere alla SC Sistemi Informativi Aziendali la disattivazione delle relative credenziali.

Le credenziali di autenticazione vengono disattivate una volta che la SC Sistemi Informativi Aziendali riceve la comunicazione della cessazione del rapporto di lavoro.

Le credenziali consistono in una utenza (USER) ed una password di dominio composta con la naming convention: <*cognome "." iniziale del nome*> (ad esempio: ROSSI MARIO avrà user: *rossi.m*).

Le credenziali di autenticazione devono essere custodite dagli utenti con la massima cura e in nessun caso divulgate, pertanto è fatto divieto di trascrivere o memorizzate le password su supporti facilmente intercettabili da utenti terzi. La password deve corrispondere anche al principio di segretezza e pertanto non deve essere svelata o condivisa con altri soggetti, tenuto conto che la trascuratezza nella conservazione delle credenziali può causare gravi danni al proprio lavoro e alla Fondazione nel suo complesso.

Le credenziali di autenticazione costituiscono de facto una firma elettronica, pertanto fanno presumere che le attività svolte con tale utenza siano riconducibili esclusivamente all'assegnatario.

L'azienda ha implementato dei sistemi che supportano gli utenti nella corretta gestione della password, individuando e suggerendo, ove possibile, lunghezze di minima ricorsività e scadenza.

Ciascun utente nella gestione delle password deve rispettare alcune precise regole. La password di prima assegnazione deve essere cambiata al primo accesso dagli utenti, che devono aver cura di crearla con caratteristiche di "robustezza" secondo le regole stabilite di seguito:

- deve essere lunga almeno 8 caratteri e deve contenere lettere minuscole, maiuscole, caratteri speciali e numeri;
- deve essere cambiata ogni 60 giorni;
- è assolutamente personale e non deve essere comunicata ad altri;
- deve essere sostituita immediatamente quando si presume che possa essere diventata poco sicura;
- non deve essere memorizzata su alcun tipo di supporto (cellulare, post-it, etc.);
- non deve contenere nome, cognome o loro parti;
- deve essere diversa dalle 3 precedenti.

Le nuove policy di sicurezza prevedono l'autenticazione tramite MFA (Multi Factor Authentication) che richiede:

- → autenticazione al portale MFA;
- → protezione account tramite inserimento numero di cellulare;
- → inserimento codice a 6 cifre inviato del cellulare indicato.

Per ogni informazione inerente all'autorizzazione, rilascio e revoca delle credenziali elettroniche si faccia riferimento alla istruzione operativa IO33.

Presso la Fondazione è implementato un meccanismo che consente all'autorizzato fino ad un massimo di 2 tentativi errati di inserimento della password, dopodiché il tentativo di accesso verrà considerato malevolo e di conseguenza l'account verrà bloccato.

La SC Sistemi Informativi Aziendali è autorizzata, in caso di oggettive ed urgenti necessità e su richiesta del Dirigente Responsabile della Struttura Complessa, a variare la password di un utente impossibilitato ad accedere alla propria postazione di lavoro (per esempio, in caso di assenza lunga non programmata) per consentire l'accesso al Responsabile stesso, nel pieno rispetto dei diritti del lavoratore interessato e con le peculiari modalità di protezione di seguito descritte al par. 9.

Non appena possibile, il predetto Responsabile deve avvertire l'utente sull'accesso effettuato; quest'ultimo, al primo accesso, dovrà nuovamente provvedere al cambio password.

L'autenticazione a livello applicativo verrà progressivamente migrata a modalità con autenticazione a 3 fattori con OTP rilasciate secondo le procedure standard SSR

6. ISTRUZIONI PER LO SVOLGIMENTO DELLE OPERAZIONI CARATTERIZZANTI IL PROCESSO DI TRATTAMENTO

Gli ambiti di trattamento previsti per i dati, attraverso gli strumenti elettronici in uso presso la Fondazione, sono i seguenti:

- ***identificazione dell'interessato:*** al momento della raccolta dei dati personali, qualora sia necessario individuare l'identità del soggetto che fornisce le informazioni, è obbligatorio richiedere un documento di identità o di riconoscimento, al fine di verificarne l'identità e procedere correttamente alla raccolta e alla registrazione delle informazioni;
- ***raccolta:*** prima di procedere alla raccolta dei dati personali deve essere fornita l'informativa all'interessato o alla persona presso cui si raccolgono i dati (sarà cura del Titolare decidere le modalità per adempiere a questo obbligo); occorre procedere alla raccolta dei dati con la massima cura, verificandone l'esattezza, la pertinenza, la completezza e la non eccedenza rispetto alle finalità del trattamento in conformità a quanto previsto dalla legge e dai regolamenti, seguendo le istruzioni del Titolare del trattamento;
- ***registrazione*:** nel caso di inserimento in uno dei sistemi informativi aziendali, è necessario operare con la massima attenzione al fine di non omettere dati o inserire dati non corretti; durante tali operazioni fare particolare attenzione a non lasciare CD, fogli, cartelle e quant'altro a disposizione di estranei;
- ***conservazione:*** i documenti o gli atti che contengono categorie particolari di dati vanno conservati in archivi ad accesso controllato. È quindi necessario garantire che armadi, schedari e contenitori siano muniti di serratura e che l'Autorizzato del trattamento, che riceve Clienti ed utenti, sia sempre presente nella propria stanza o luogo di lavoro avendo cura di evitare che le informazioni trattate possano essere visualizzate e rese conoscibili a terzi. Sarà cura del Titolare del trattamento adottare i provvedimenti

necessari affinché venga escluso un accesso ad archivi ed a dati da parte di soggetti che non siano Autorizzati al trattamento;

- ***utilizzo:*** i dati possono essere utilizzati solo da coloro che sono stati espressamente autorizzati al trattamento. L'utilizzo dei dati deve avvenire solo per scopi determinati, espressi e legittimi, avendo cura di evitare un utilizzo per scopi che non coincidano o che non siano compatibili con quelli istituzionali della Fondazione, in riferimento alle attività affidate e di competenza dell'unità di trattamento di appartenenza;
- ***limitazione:*** questa operazione può essere conseguenza di una espressa richiesta da parte dell'interessato ossia può essere ordinata direttamente dal Garante per la protezione dei dati personali;
- ***comunicazione:*** con tale espressione, secondo quanto previsto dalla legge, si intende "il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, in qualunque forma, anche mediante la loro messa a disposizione o consultazione". Ciò che caratterizza l'operazione di comunicazione è il fatto che, considerato il rapporto diretto tra Titolare (la Fondazione) e l'interessato (ad esempio un cittadino utente, un dipendente o un'impresa), un soggetto determinato (in posizione di terzietà rispetto a questo rapporto bilaterale) possa in qualunque forma conoscere dati personali riferiti all'interessato medesimo;
- ***diffusione:*** per diffusione si intende "il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione". È espressamente vietata la diffusione di dati personali idonei a rivelare lo stato di salute.

7. UTILIZZO DELLE RISORSE AZIENDALI

7.1. Postazioni di lavoro

La Fondazione mette a disposizione dei dipendenti postazioni di lavoro fisse o portatili adeguatamente predisposte da parte della SC Sistemi Informativi Aziendali; le stesse sono dotate di software antivirus e configurate per essere utilizzate in modo sicuro all'interno della rete della Fondazione.

I dipendenti sono personalmente responsabili delle attività svolte utilizzando le apparecchiature assegnate e i software installati sulle stesse; l'utilizzo delle risorse hardware e software deve sempre rispettare il principio di diligenza e correttezza ed essere attinente all'attività lavorativa assegnata dall'Ente all'utente. L'utente è altresì responsabile della corretta custodia dei PC portatili assegnati, pertanto dovrà prevedere la custodia in ambiente protetto (ad esempio cassetto con chiave o armadio) alla fine della giornata lavorativa.

Le postazioni di lavoro sono uno strumento lavorativo e possono essere utilizzate esclusivamente per tale fine, pertanto non devono essere utilizzate per finalità private e diverse da quelle aziendali. Si ricorda che ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, rallentamenti del sistema, costi di manutenzione e minacce per la sicurezza delle informazioni.

Le PdL assegnate agli utenti possono essere, per esigenze organizzative, riassegnate ad altre persone all'interno della Fondazione: in questi casi la PdL viene formattata e ripristinata alle configurazioni iniziali. Eventuali dati, anche di carattere personale (inclusi i messaggi di posta elettronica inviati o ricevuti, i file di immagini o video ed altre tipologie di file) devono essere rimossi dall'incaricato prima della restituzione del dispositivo. La Fondazione non assume responsabilità circa la perdita di dati personali dell'Incaricato contenuti nei dispositivi aziendali.

A seguito di una cessazione del rapporto lavorativo o di consulenza dell'Incaricato con la Fondazione o comunque al venir meno, ad insindacabile giudizio della Fondazione, della permanenza dei presupposti per l'utilizzo delle PdL aziendali, gli utenti hanno i seguenti obblighi:

- Procedere immediatamente alla restituzione alla SC Sistemi Informativi Aziendali dei dispositivi in uso, con la compilazione del MODSIA_02 per la riconsegna degli asset.
- Divieto assoluto di formattare o alterare o manomettere o distruggere i dispositivi assegnati o rendere inintelligibili i dati in essi contenuti tramite qualsiasi processo.

Le stesse regole si applicano anche in caso di restituzione del dispositivo in seguito a richiesta di manutenzione per guasto o in caso di controlli che la Fondazione è tenuta ad effettuare.

Gli utenti della Fondazione, responsabili della propria postazione di lavoro, dovranno sottostare ai seguenti obblighi:

- non creare e diffondere intenzionalmente o per negligenza programmi idonei a danneggiare l'Azienda (quali ad esempio virus, malware, trojian, etc.);
- non effettuare in autonomia attività manutentive e/o di configurazione di qualsiasi tipologia;
- non utilizzare programmi diversi da quelli distribuiti e installati ufficialmente dall'Amministratore di Sistema, in particolare non installare software non licenziati. L'inosservanza di questa disposizione, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre la Fondazione a gravi responsabilità civili ed anche penali in caso di violazione della normativa a tutela dei diritti d'autore sul software (D.Lgs. 518/92 sulla tutela giuridica del software e L. 248/2000 nuove norme di tutela del diritto d'autore) che impone la presenza nel sistema di software regolarmente licenziato o comunque libero e quindi non protetto dal diritto d'autore (copyright);
- non modificare le caratteristiche impostate sul proprio PC, salvo previa autorizzazione esplicita dell'Amministratore di Sistema;
- non lasciare sulla scrivania informazioni riservate e/o qualunque supporto in cui esse siano archiviate (carta, CD, chiavi USB, etc.);
- richiamare le funzioni di sicurezza del sistema operativo (con la sequenza dei tasti CTRL+ALT+CANC) ed assicurarsi della attivazione della funzione "Blocca" in caso di abbandono momentaneo del proprio PC e, in alternativa, impostare lo screen saver con password in modo che si attivi dopo al massimo 5 minuti di inattività;
- non lasciare il computer portatile incustodito sul posto di lavoro (al termine dell'orario lavorativo, durante le pause di lavoro o durante riunioni lontane dalla propria postazione);
- non lasciare incustoditi cellulari o tablet;
- non utilizzare fax e/o telefono per trasmettere informazioni riservate e personali se non si è assolutamente certi dell'identità dell'interlocutore o del destinatario o se esso non è legittimato a riceverle. Si consiglia, qualora si nutrano dubbi sull'identità di chi è dall'altra parte dell'apparecchio, di richiedere identità e qualifica dell'interlocutore, al fine di richiamarlo successivamente per avere certezza sulla sua identità.

Le postazioni di lavoro sono gestite a livello manutentivo dai tecnici della SC Sistemi Informativi Aziendali, pertanto:

- Gli utenti operano attraverso l'utilizzo dei software installati dalla SC Sistemi Informativi Aziendali e non dispongono dell'autorizzazione necessaria per effettuare altre installazioni o disinstallazioni; in caso

di necessità devono rivolgersi alla SC Sistemi Informativi Aziendali con richieste motivate di installazione di altri applicativi. La SC Sistemi Informativi Aziendali, responsabile della sicurezza dell'infrastruttura aziendale, può rifiutare richieste che considera rischiose o non necessarie.

- La SC Sistemi Informativi Aziendali effettua le necessarie verifiche relative alla compatibilità tecnica e al tipo di licenza necessaria per il software richiesto, a garanzia della sicurezza dei sistemi e del rispetto della normativa a tutela dei diritti d'autore.
- Gli aggiornamenti del software antivirus e dei sistemi operativi sono possibili solo attraverso la connessione della postazione (fissa o portatile) alla rete telematica della Fondazione: è pertanto indispensabile che i dipendenti provvedano ad accendere e collegare alla rete le apparecchiature in dotazione, anche se portatili, con frequenza almeno quindicinale.
- I tecnici della SC Sistemi Informativi Aziendali e dei fornitori afferenti allo stesso Servizio sono autorizzati ad effettuare, ove possibile e previa informazione degli utenti delle postazioni di lavoro, interventi di carattere sistemistico sulle stesse per necessità legate al loro corretto funzionamento e alla sicurezza, interventi che potranno anche comportare, se necessario, l'accesso ai dati trattati dagli utenti delle postazioni, oppure a verifiche su messaggi di posta elettronica ricevuti o siti internet visitati potenzialmente responsabili di malfunzionamenti o indebolimento della sicurezza operativa.
- La stessa facoltà, sempre ai fini della sicurezza complessiva del sistema e per garantire la normale attività della Fondazione, si applica anche in caso di assenza o impedimento prolungato dell'utente. Analogamente in caso di prolungata assenza dell'utente il Responsabile del Trattamento dei dati contenuti nella postazione può, per fini istituzionali, richiedere alla SC Sistemi Informativi Aziendali di effettuare un accesso alla postazione e le eventuali attività necessarie sulla stessa.
- I tecnici della SC Sistemi Informativi Aziendali sono altresì autorizzati, al fine di garantire il corretto funzionamento dei sistemi e una adeguata sicurezza della rete telematica, a collegarsi da remoto alle postazioni di lavoro visualizzandone i contenuti in modalità di tele-assistenza.
- L'intervento viene effettuato di norma su richiesta dell'utente oppure in casi di particolare urgenza legati alla rilevazione di problemi tecnici nel sistema informatico o telematico avvertendo, ove possibile e compatibilmente con l'urgenza in atto, gli utenti delle postazioni interessate.
- In caso di danneggiamento, furto o smarrimento di apparecchiature informatiche o supporti removibili su cui sono memorizzati dati attinenti le attività dell'Ente, l'utente utilizzatore deve darne tempestiva informazione al proprio responsabile, alla SC Sistemi Informativi Aziendali e alle autorità di pubblica sicurezza, seguendo quanto definito dal nuovo GDPR in materia di Data Breach.
- Non è consentito connettere la propria postazione di lavoro (fissa o portatile) a reti diverse da quella della Fondazione, neppure attraverso l'utilizzo di modem, router, smartphone o apparati WI-FI all'interno della rete aziendale e comunque previa autorizzazione della SC Sistemi Informativi Aziendali.

Nei casi di smarrimento, furto accertato o manomissione dei dispositivi assegnati l'utente dovrà effettuare tempestiva segnalazione a:

- Autorità giudiziaria;
- Direttore della struttura di appartenenza;
- Direttore della SC Sistemi Informativi Aziendali;
- DPO, per le valutazioni propedeutiche agli adempimenti di cui agli artt. 33 e 34 GDPR.

Non è consentito effettuare accessi alla rete o ai software della Fondazione con credenziali appartenenti ad altri utenti, anche nell'ambito della stessa unità organizzativa. Gli identificativi utente e le corrispondenti password sono personali, riservate e non cedibili.

Gli utenti devono effettuare la fase di login per l'autenticazione sulla postazione di lavoro e connettersi al sistema informativo aziendale o ad una parte di esso. Verranno effettuate altre operazioni di login per accedere ad ulteriori ambienti di lavoro (applicativi web, sistemi dipartimentali, posta elettronica, etc.).

Il personale addetto alla assistenza tecnica della SC Sistemi Informativi Aziendali può in qualunque momento - e senza alcuna preventiva autorizzazione - procedere alla rimozione di ogni file o applicazione che riterrà essere pericoloso per la sicurezza, cosi come procedere alla eventuale rimozione di software non autorizzato.

7.1.1. Antivirus

I virus possono essere trasmessi tramite scambio di file via internet, supporti removibili o file-sharing. La Fondazione installa su tutte le PdL un sistema antivirus che si aggiorna automaticamente. L'attività viene descritta nel dettaglio nella procedura PR SIA_04 "Procedura di aggiornamento antivirus".

Nel caso in cui l'antivirus rilevi la presenza di un virus, l'utente deve effettuare immediata segnalazione alla SC Sistemi Informativi Aziendali.

L'utilizzo di chiavi USB è consentito solo previa scansione - prima del suo utilizzo - mediante il programma antivirus.

7.2. Server centrali

Il sistema informatico aziendale è composto da un insieme di unità server centrali connesse alla rete aziendale, installate presso i data center della Fondazione o disponibili in cloud, comunque messe a disposizione dall'Azienda agli utenti per svolgere i compiti assegnati.

La Fondazione non effettua backup dei dati memorizzati localmente, pertanto i file creati, elaborati o modificati sul dispositivo assegnato e di cui risulta necessario assicurare l'integrità dei dati in caso di rottura del dispositivo stesso, devono essere salvati nei server aziendali messi a disposizione dalla Fondazione. È indispensabile che gli utenti memorizzino i propri file sui predetti server, in quanto il backup degli stessi viene regolarmente effettuato con appositi software dalla SC Sistemi Informativi Aziendali e viene messo a disposizione dell'utente in caso di necessità, fermo restando l'attribuzione sul trattamento dei dati afferente a ciascun Responsabile individuato. Si ricorda che anche tutti i dischi o altre unità di memorizzazione locali (es. disco C: interno al PC) non sono soggette a salvataggio da parte del personale incaricato dell'assistenza tecnica della SC Sistemi Informativi Aziendali, pertanto tutti i documenti per cui si renda necessaria la garanzia della conservazione devono essere posizionati sui server o copiati sugli stessi periodicamente.

Risulta opportuno che, con regolare periodicità (almeno ogni mese), ciascun utente provveda alla pulizia di tali archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati, essendo infatti necessario evitare un'archiviazione ridondante, in ossequio al principio della minimizzazione del trattamento dei dati.

Le cartelle-utenti presenti nei server della Fondazione sono aree di condivisione di informazioni strettamente professionali e non è in alcun modo consentito l'utilizzo per motivi di carattere personale: gli autorizzati all'uso di tali archivi sono quindi responsabili del corretto utilizzo degli stessi, secondo le istruzioni ricevute. Pertanto, qualunque file che non sia legato all'attività lavorativa, non può essere dislocato, nemmeno per brevi periodi, in queste unità.

Su richiesta del Responsabile dell'Unità Organizzativa interessata, le cartelle messe a disposizione sul server per memorizzare i file necessari allo svolgimento dell'attività lavorativa possono essere condivise tra diversi utenti oppure essere riservate al singolo utilizzatore. Nei casi di cessazione del rapporto lavorativo e/o indisponibilità prolungata del membro della Fondazione e/o in casi di urgenza, il titolare del trattamento può incaricare un soggetto specificamente ed esplicitamente autorizzato affinché acceda all'archivio unicamente per il tempo necessario a risolvere le necessità oggetto dell'esigenza lavorativa in atto. In nessun caso l'accesso agli archivi avviene per fini di controllo del lavoratore.

7.3. Utilizzo dispositivi di fonia fissa e mobile

La Fondazione è provvista di dispositivi di comunicazione fissa e mobile (cellulari) e di schede telefoniche di tipo "dati" che mette a disposizione, secondo le modalità di cui al presente disciplinare, del personale utente. I telefoni fissi sono assegnati secondo le seguenti classi di abilitazioni:

ABILITAZIONI LINEE TELEFONICHE	DESCRIZIONE
CAT 0	INTERNAZIONALE + CELL + N. VERDI
CAT 2	NAZIONALE + CELL + ESCLUSO N. VERDI
CAT 3	URBANO
CAT 4	URBANO + N. VERDI + ESCLUSO CELL
CAT 5	NAZIONALE + CELL + N. VERDI
CAT 6	INTERNAZIONALE (CON ESCLUSIONE LISTA VIETATA)
CAT 8	NAZIONALE + N. VERDI + ESCLUSO VERDI
CAT 9	SOLO INTERNI

Per la richiesta di una linea di telefonia fissa è necessario compilare ed inoltrare alla SC Sistemi Informativi Aziendali il MOD 269 *"Modulo richiesta telefonia fissa",* disponibile sulla intranet aziendale.

Si precisa che:

- L'uso di dispositivi di comunicazione mobile di servizio (cellulari) può essere concesso, per la durata dell'incarico e il permanere delle condizioni, al personale aziendale per cui si applicano particolari modalità di lavoro quali reperibilità, assistenza agli impianti etc.
- L'accesso al servizio può avvenire soltanto previa individuazione nominativa e provvedimento motivato del competente Dirigente e dal capo dipartimento.
- La richiesta di concessione del telefono cellulare, sottoscritta dal Dirigente del Servizio, da compilare utilizzando il MOD 270 *"Modulo richiesta di nuovo apparecchio per telefonia mobile"* disponibile sulla intranet aziendale, dovrà essere inoltrata alla SC Provveditorato-Economato. La concessione potrà avvenire in base ad uno o più criteri di seguito riportati, limitatamente al periodo necessario allo svolgimento delle particolari attività che ne richiedono l'uso:
  - esigenze di reperibilità da parte dei vertici della struttura amministrativa di riferimento e/o dal personale interno;
  - servizi fuori sede;
  - frequenti spostamenti tra sedi diverse anche nella stessa giornata, in relazione alla peculiarità del servizio espletato;
  - particolari esigenze tecniche di comunicazione di altra natura, tra le quali servizi che non possono essere altrimenti soddisfatti con impianti di telefonia fissa e/o altri strumenti di comunicazione quali

la posta elettronica.

- Le SIM ed i dispositivi sono messi a disposizione dei dipendenti secondo due diverse modalità:
  - schede e dispositivi "personali" messi a disposizione specificamente di un solo utilizzatore;
  - schede e dispositivi "a rotazione" messi a disposizione specificamente di più utilizzatori a seconda dei casi e delle necessità del momento. Le schede ed i dispositivi "a rotazione" sono attribuiti al Dirigente del Servizio. In tal caso la struttura dovrà tenere nota degli effettivi utilizzatori per tutta la durata della concessione.
- I telefoni cellulari sono di uso personale e non possono essere ceduti a colleghi o terzi.
- I telefoni cellulari possono essere utilizzati soltanto per ragioni di servizio e viene fatto tassativo divieto di effettuare chiamate personali o per scopi diversi da quelli di servizio.
- Gli utilizzatori dei telefoni cellulari hanno l'obbligo di mantenere in funzione il telefono cellulare durante le ore di servizio, durante le ore di reperibilità, ove previste, ed in tutti i casi in cui le circostanze concrete lo rendano opportuno o indispensabile, e ciò affinché essi possano essere immediatamente rintracciati nei casi di necessità.
- La durata delle chiamate, verificata la relativa necessità, deve essere la più breve possibile in relazione alle esigenze di servizio e di mandato.
- Qualora tecnicamente possibile, in base al contratto vigente stipulato dalla Fondazione, si potrà conservare la numerazione della SIM personale trasferendola alla SIM assegnata dalla Fondazione, previa attivazione del servizio di dual billing (doppia fatturazione).
- Gli utilizzatori di SIM assegnate dalla Fondazione, nell'ipotesi di cessazione della carica o del rapporto di lavoro, potranno richiedere di conservare la numerazione del cellulare di Servizio, qualora tecnicamente possibile, trasferendola sul cellulare personale senza oneri a carico dell'Azienda.
- Il consegnatario del dispositivo di comunicazione mobile e di scheda SIM è il responsabile del corretto utilizzo e della corretta tenuta del cellulare dal momento della firma del verbale di prima assegnazione fino ad eventuale revoca e/o restituzione. Ogni variazione delle norme di utilizzo d'uso rispetto a quelle in vigore al momento della consegna sarà diversamente segnalata.
- È fatto assoluto divieto di cessione a terzi sia del cellulare che della SIM. Il Dirigente del Servizio può revocare l'assegnazione, sia per non corretto utilizzo dell'apparato mobile sia per motivi di servizio.
- Ogni possessore di un telefono cellulare è tenuto all'uso appropriato e alla diligente conservazione di questo, alla piena conoscenza di tutte le funzioni e modalità di utilizzo previste, nonché all'autonoma tenuta della relativa documentazione.
- In caso di furto o smarrimento l'utilizzatore dovrà prontamente provvedere alla denuncia presso l'autorità competente. In tali evenienze e nell'ipotesi di danneggiamento dei telefoni cellulari o di necessità varie, l'utilizzatore dovrà prontamente darne comunicazione alla SC Provveditorato-Economato, osservando le disposizioni impartite. Per i dispositivi noleggiati il riferimento è alle modalità di sostituzione previste dai singoli contratti.
- L'utilizzatore, dal momento della consegna del telefono, è responsabile nei confronti della Fondazione proprietario dell'apparato ricevuto - telefono cellulare e scheda - con contratto intestato comprensivo degli accessori del telefonino.
- Ciascun Dirigente è il responsabile sull'uso dei dispositivi di comunicazione fissa per il relativo personale assegnatario.

- L'utilizzo degli apparecchi telefonici per ragioni non riconducibili all'attività di servizio o con modalità difformi da quelle previste dal presente disciplinare costituisce condotta sanzionabile sotto il profilo disciplinare, fermo restando l'eventuale responsabilità penale ed amministrativa.

I dispositivi mobili richiedono livelli di prudenza e diligenza particolarmente elevati: essi assumono peculiare rilevanza nel momento in cui l'attività lavorativa è espletata anche con l'uso di questi strumenti (ad esempio nei casi di sincronizzazione della casella di posta elettronica istituzionale), essendo gli stessi esposti a rischi maggiori di perdita, sottrazione o danneggiamento. Nel caso in cui ricorrano queste due condizioni (utilizzo per attività lavorativa e uno tra sottrazione, perdita e danneggiamento), il titolare del *device* deve tempestivamente riportare l'accaduto alle funzioni competenti secondo quanto disposto nella Procedura di gestione del *data breach*.

È fatto divieto di archiviare dati personali o altre tutte le altre informazioni attinenti all'attività lavorativa sulla memoria del dispositivo mobile: questi dati dovranno essere archiviati sugli share messi a disposizione dall'Istituto (File server o software aziendali).

7.4. Utilizzo di dispositivi di memorizzazione

Gli utenti che per particolari necessità utilizzano supporti ottici o magnetici removibili, quali chiavi USB, CD, DVD, Hard Disk portatili etc., devono custodirli in luoghi sicuri e, dopo l'uso, non lasciarli collegati alla propria postazione di lavoro, interconnessa con la rete aziendale. I dati personali o sensibili eventualmente memorizzati per esigenze temporanee su detti supporti devono essere cancellati immediatamente. I dispositivi di memorizzazione devono essere dotati di crittografia e centralmente dovrebbe essere custodita la chiave di recupero in caso di smarrimento delle credenziali.

8. UTILIZZO DELLA RETE TELEMATICA

La rete aziendale è una risorsa a disposizione di tutti e rappresenta una infrastruttura critica per l'erogazione di tutti i servizi.

La normativa introdotta da AgID, Agenzia per l'Italia Digitale, prevede che ogni apparato collegato alla rete informatica sia tracciato e ne siano registrate le caratteristiche principali (I.P., Sistema Operativo, presenza di Antivirus etc.). Il presente disciplinare si prefigge, già dalla prima installazione, di mettere in opera un dispositivo conforme a quanto indicato dalla normativa, registrando eventuali eccezioni dettate dalle funzioni del dispositivo. Per questa ragione si ritiene indispensabile che l'allestimento dell'apparecchiatura, sia essa server, PdL, apparecchiatura speciale, sia seguito dalla SC Sistemi Informativi Aziendali.

La SC Sistemi Informativi Aziendali provvede ad attivare le prese di rete necessarie agli uffici e servizi e a verificare preventivamente le apparecchiature di nuova acquisizione destinate all'installazione in rete attraverso la gestione di appositi moduli.

Le unità organizzative che rilevano la necessità di attivazione di nuovi punti rete ne fanno richiesta motivata alla SC Sistemi Informativi Aziendali, che effettua le verifiche preliminari per l'evasione della richiesta e, ove necessario, si raccorda con l'Ufficio Tecnico per le attività di carattere impiantistico.

È disponibile anche la rete Wi-Fi che supporta la connessione "senza fili" alla rete aziendale per alcune tipologie di apparecchiature quali computer portatili, tablet, smartphone etc.

L'utilizzo di questo tipo di connessione è consentito esclusivamente, previa richiesta alla SC Sistemi Informativi Aziendali da parte del proprio Responsabile di struttura, agli utenti che ne hanno necessità per la

tipologia dell'attività svolta all'interno della Fondazione, utenti per i quali la SC Sistemi Informativi Aziendali effettuerà opportuna configurazione.

È disponibile una rete Wi-Fi privata per ospiti, esterna all'infrastruttura della Fondazione e destinata agli ospiti ed ai pazienti, avente funzione di hotspot e meccanismi automatici di gestione delle credenziali e di cui è disponibile una guida aggiornata sulla Intranet aziendale.

9. POSTA ELETTRONICA

Le caselle di posta elettronica, concesse in uso all'utente, sono esclusivamente destinate ad un utilizzo pertinente l'attività lavorativa: pertanto è fatto divieto esplicito di utilizzarle per fini personali e/o per l'iscrizione a siti web non pertinenti l'attività lavorativa. Gli utenti assegnatari della casella di posta elettronica sono responsabili del corretto utilizzo delle stesse e la casella di posta istituzionale rappresenta unico strumento per le comunicazioni di ambito aziendale.

E' pertanto fatto esplicito divieto di utilizzare per le comunicazioni istituzionali indirizzi di posta che non siano quelli @istituto-besta.it.

Il Forward della posta istituzionale verso caselle di posta di differente dominio è inibito

È fatto assoluto divieto l'utilizzo di caselle di posta elettronica personali per comunicazioni lavorative.

Le caselle di posta hanno la seguente naming convention: nome.cognome@istituto-besta.it

Pertanto l'utente non potrà utilizzare la posta per:

- invio/ricezione di allegati contenenti fotografie filmati e o brani musicali;
- invio/ricezione di messaggi personali per la partecipazione a dibattiti forum, mailing list non legate ad attività lavorativa;
- invio/ricezione messaggi a contenuto offensivo o discriminatorio;
- inoltro a indirizzi mail esterni alla Fondazione di comunicazioni ricevute sulla posta elettronica di dominio;
- apertura messaggi insoliti o provenienti da utenti sconosciuti;
- provvedere alla manutenzione per evitare la eccessiva espansione;
- inviare in modo ingiustificato a destinatari plurimi messaggi che esulano da fini istituzionali, come le cosiddette catene di sant'Antonio;
- pubblicità;
- comunicare i propri codici di accesso (nome utente e password) in risposta a richieste pervenute via e-mail (phishing);
- trasmettere messaggi a tutti i dipendenti in assenza delle necessarie autorizzazioni.

In caso di assenza dovrà essere attivata la risposta automatica ai messaggi ricevuti, con indicazione del periodo di assenza, nonché altro indirizzo e-mail della Fondazione da contattare in caso di urgenze, al fine di evitare la necessità di accesso alla mail nel periodo dell'assenza e/o ritardo nella gestione di comunicazioni indirizzate alla Fondazione. Qualora l'Utente sia impossibilitato ad attivare la procedura di cui sopra, perdurando l'assenza, la Fondazione potrà, avvalendosi di personale appositamente incaricato e formato della SC Sistemi

Informativi Aziendali, procedere all'attivazione di un analogo accorgimento (risposta automatica), dandone avviso all'assente.

La Fondazione si riserva di filtrare la corrispondenza in entrata mediante appositi filtri antispam e antivirus.

Inoltre sono filtrati in ricezione i file - provenienti da qualsiasi fonte - con estensioni particolari tipo .exe, .bat .cmd .mdb.

L'abilitazione per l'utilizzo del servizio di posta elettronica della Fondazione deve essere richiesta dal Responsabile della SC di appartenenza dell'utente alla SC Sistemi Informativi Aziendali; analogamente in caso di cessazione del rapporto di lavoro di un utente il predetto Responsabile deve segnalarlo alla SC Sistemi Informativi Aziendali per la gestione delle necessarie attività di chiusura della casella di posta elettronica corrispondente. In particolare, fin dal primo giorno di cessazione, la SC provvederà a disabilitare la ricezione di messaggi in entrata, inserendo un messaggio automatico di risposta per i tentativi di messaggi in arrivo con cui si invita l'utente a contattare altri indirizzi della Fondazione. Si ricorda che per ogni utente la casella di posta elettronica potrà essere mantenuta solo per 30 giorni e non oltre la data di cessazione del rapporto lavorativo, rappresentando anche un costo per l'Azienda.

I dipendenti autorizzati all'uso del servizio di posta elettronica della Fondazione devono fruirne nel rispetto del principio di diligenza e correttezza, per trasmettere esclusivamente comunicazioni professionali, utilizzando linguaggio e toni appropriati.

Per le comunicazioni inviate ad altri dipendenti all'interno della Fondazione, gli utenti del servizio e-mail dovranno di norma seguire le vie gerarchiche, fatti salvi i casi di esigenze legate al tipo di attività svolta. La posta elettronica non va comunque considerata come il mezzo esclusivo con il quale avvengono le comunicazioni tra colleghi, all'interno della stessa SC o SS, non potendo considerarsi come sostitutiva di colloqui, riunioni, telefonate, videoconferenze.

L'invio di documenti all'esterno dell'Azienda deve avvenire utilizzando formati dei file che proteggano gli stessi da modifiche indesiderate da parte di terzi (p.e. protetti da password). L'invio di allegati di dimensioni superiori a 50 Megabyte non è consentito e può essere effettuato solo previa autorizzazione della SC Sistemi Informativi Aziendali, che verifica quando effettivamente necessario e preferibile ad altri tipi di trasmissione (p.e. basate su protocolli FTP, FTPS, etc.).

In ogni caso è vietato trasmettere in chiaro allegati contenenti dati sensibili o personali; gli utenti devono proteggere tali file con tecniche di crittografia secondo le indicazioni della SC Sistemi Informativi Aziendali. Per l'invio di documentazione contenente dati sensibili ai pazienti si faccia riferimento alle istruzioni operative IO SIA_06 "Condivisione di file tramite posta elettronica" e IO SIA_07 "Condivisione di file tramite SharePoint" in cui viene fatto riferimento alla corretta procedura di condivisione della documentazione personale di un paziente. Si ricorda, infatti, che trasmettere e condividere documenti con dati personali, specialmente se trattano l'ambito della salute, tramite posta elettronica costituisce un rischio rilevante per la riservatezza delle informazioni e costituirebbe una violazione della normativa vigente in materia di protezione dei dati personali se non utilizzate le metodologie corrette.

L'account di posta aziendale non è uno strumento privato in uso esclusivo del lavoratore: al fine di ribadire agli interlocutori la natura esclusivamente aziendale della casella di posta elettronica, i messaggi contengono un avvertimento standardizzato inserito in automatico dal sistema, in cui viene chiarita la natura non personale degli stessi precisando, pertanto che, il personale debitamente incaricato della Fondazione potrà accedere al contenuto del messaggio di risposta.

In caso di impedimento prolungato da parte dell'utente ad accedere alla sua casella di posta elettronica, se si rendesse necessario accedere ai messaggi per garantire il regolare svolgimento delle attività, la Fondazione stessa ove possibile chiederà all'interessato di delegare un altro lavoratore (fiduciario) per verificare il

contenuto della e-mail ed inoltrare al Responsabile interessato le informazioni rilevanti per lo svolgimento dell'attività lavorativa. Nei casi in cui non sia possibile contattare l'utente assente - o lo stesso non deleghi un fiduciario - il Responsabile interessato può richiedere alla SC Sistemi Informativi Aziendali di accedere alla casella di posta elettronica dell'utente assente, in modo che si possa prendere visione delle informazioni e dei documenti necessari all'attività della Fondazione. In tali casi, la Fondazione procederà alla cancellazione della password ed all'inserimento di una nuova, temporanea, al fine di poter accedere al contenuto. Il cambiamento della password è garanzia, per l'utente assegnatario della casella di posta, del pieno controllo sugli eventuali accessi di terzi. Il Responsabile dovrà redigere apposito verbale e informare l'utente assente appena possibile, nonché limitarsi alla lettura delle e-mail necessarie per le finalità aziendali.

Non è consentito modificare le impostazioni del proprio software per l'accesso alla posta elettronica, così come la condivisione della propria mailbox con soggetti esterni alla Fondazione.

In caso di ricezione di messaggi potenzialmente pericolosi, l'utente dovrà evitarne l'apertura e darne tempestiva informazione alla SC Sistemi Informativi Aziendali tramite l'apertura della segnalazione a: cybersecurity@istituto-besta.it

A titolo esemplificativo non vanno aperti i messaggi che:

- hanno un oggetto non perfettamente chiaro;
- risultano di dubbia provenienza;
- chiedono un'azione o una risposta urgente con delle motivazioni ingannevoli come, ad esempio, solleciti di pagamento fatture, pagamento multe, ritiro di pacchi presso corrieri o uffici postali, richiesta di password da parte di banche o enti pubblici.

Le caselle e-mail con natura impersonale sono assegnate di default alle Strutture o ai servizi di staff (URP, RSPP, Formazione, etc.); l'assegnazione di altre caselle impersonali, richiesta dal responsabile della struttura/servizio, deve comunque essere approvata dal capo dipartimento/direttore di competenza. Le caselle saranno comunque assegnate ad una persona fisica, che sarà incaricata come responsabile del corretto utilizzo delle stesse e la nomenclatura sarà attribuita dalla SC Sistemi Informativi Aziendali su richiesta degli interessati e sulla base della destinazione dell'ufficio.

Il personale autorizzato è tenuto ad apporre ai messaggi di posta elettronica una firma in calce formata da: nome, cognome, struttura d'appartenenza, numeri di telefono, indirizzo sede fisica, evitando di aggiungere altre informazioni non attinenti all'incarico lavorativo.

Prima della cessazione di ogni tipologia di rapporto con l'Azienda, è fatto obbligo all'utente di trasmettere al Responsabile del reparto/ufficio di appartenenza i messaggi di posta elettronica rilevanti per il prosieguo dell'attività istituzionale.

Con riferimento all'utilizzo di indirizzi di posta elettronica certificata (PEC), si precisa che la PEC è uno strumento destinato ai fini esclusivi di opponibilità a terzi della comunicazione intrattenuta con soggetti esterni alla Fondazione e che non costituisce elemento di comunicazione ordinaria tra uffici, né informale né formale. Il suo utilizzo deve svolgersi in accordo alle regole sopra descritte. L'assegnazione e revoca delle caselle PEC compete a [da completare].

10. INTERNET

Le PdL assegnate all'utente sono abilitate alla navigazione internet e la connessione alla rete internet è ammessa esclusivamente per lo svolgimento dell'attività lavorativa.

L'accesso e l'utilizzo degli strumenti digitali è consentito nel rispetto dei principi di correttezza e diligenza per perseguire esclusivamente finalità di tipo istituzionale.

La Fondazione, al fine di tutelare la rete aziendale ed il patrimonio informativo, filtra e inibisce l'accesso ai siti ritenuti non idonei a garantire la sicurezza e la pertinenza agli scopi istituzionali. A tal scopo è previsto l'utilizzo di parole chiave o di appositi filtri informatici "black list", ossia di controlli random successivi non associabili direttamente all'utente.

L'utente non può accedere ad internet per perseguire scopi privati e/o vietati dalla legge pertanto è fatto espresso divieto di:

- effettuare l'upload o il download di filmati, file musicali o software gratuiti (freeware, shareware, etc.) nonché l'utilizzo di documenti provenienti da siti web, se non strettamente attinenti all'attività lavorativa e previa verifica dell'attendibilità dei siti utilizzati (in caso di dubbio, dovrà venir a tal fine contattato il personale della SC Sistemi Informativi Aziendali);
- partecipare a forum non professionali, l'utilizzo di social network, chat line e di bacheche elettroniche, nonché ogni forma di registrazione a siti i cui contenuti non siano strettamente legati all'attività lavorativa;
- accedere a siti che abbiano contenuto contrario a norme di legge e tutela dell'ordine pubblico, rilevanti ai fini della realizzazione di una fattispecie di reato;
- effettuare ogni genere di transazione finanziaria, acquisti on-line e simili, fatti salvi i casi direttamente autorizzati dalla Direzione (o eventualmente dal Responsabile della SC previa richiesta alla SC Sistemi Informativi Aziendali);
- iscriversi a mailing list spendendo il nome o il marchio della Fondazione, salvo specifica autorizzazione;
- memorizzazione di documenti informatici di natura oltraggiosa diffamatoria e/o discriminatoria;
- effettuare azioni di superamento o disabilitazione dei sistemi adottati dalla Fondazione per bloccare accessi non conformi;
- utilizzare software o altri strumenti che consentano la navigazione anonima;
- utilizzare i mezzi pubblici di divulgazione delle informazioni (per esempio i social network) per la diffusione di contenuti diffamatori o offensivi per la Fondazione. La pubblicazione online di contenuti di tale natura costituisce diffamazione aggravata a norma dell'articolo 595, III comma del Codice penale, commessa con mezzo di pubblicità. Possono essere diffamatori anche contenuti insinuanti o allusivi che vadano oltre il lecito diritto di critica.

In conformità con quanto stabilito dal Dipartimento della Funzione Pubblica con la Direttiva n. 2/2009, l'utilizzo di internet per svolgere attività che non rientrano tra i compiti istituzionali è eccezionalmente consentito ai dipendenti per assolvere a incombenze amministrative e burocratiche senza allontanarsi dal luogo di lavoro (ad esempio, effettuare adempimenti on-line nei confronti di pubbliche amministrazioni e di concessionari di servizi pubblici, ossia per tenere rapporti con istituti bancari e assicurativi), purché sia contenuto nei tempi strettamente necessari allo svolgimento delle transazioni. In tali casi andrà prestata la massima attenzione per non mettere a rischio l'integrità e la riservatezza dei dati e del sistema informatico dell'Ente e a non provocare allo stesso danni di immagine.

L'utente è considerato direttamente responsabile per un eventuale accesso illecito e per il danneggiamento della rete aziendale a causa di virus introdottisi in seguito ad un uso non accorto degli strumenti informatici

messi a disposizione. È fatto salvo il diritto della Fondazione di chiedere ulteriore risarcimento del danno. Le medesime violazioni possono altresì dar luogo a responsabilità di natura civile, contabile e penale, secondo le norme vigenti.

Sono tenuti al rispetto del presente disciplinare anche i soggetti terzi che si trovano ad operare a vario titolo con la Fondazione, inclusi i collaboratori in servizio con contratto di prestazione d'opera professionale.

La Fondazione si riserva controlli anonimi tramite utilizzo di file di log sul corretto utilizzo di internet basandosi su dati aggregati riferiti all'intera struttura aziendale o a sue aree o gruppi di utenti. Solo in seguito al verificarsi di ripetute anomalie possono essere eseguiti controlli a livello individuale.

Nel caso si presentasse l'esigenza di accedere ai siti che risultassero bloccati, l'utente provvederà a richiedere il supporto tecnico alla SC Sistemi Informativi Aziendali.

Per la riabilitazione di siti bloccati per questione di sicurezza dallo strumento di firewall aziendale perché potenzialmente dannosi per la rete, si rende indispensabile una richiesta formale da parte di RPU corredata, ove necessario, di documento DPIA (Data Protection Impact Assessment).

11. ACQUISTO DI FORNITURE HARDWARE E SOFTWARE

Al fine di implementare sistemi aziendali interdipartimentali la cui conformità ai requisiti logici e fisici stabiliti ed individuati dalla SC Sistemi Informativi Aziendali siano salvaguardati e nell'ottica di garantire una continuità operativa necessaria per gli applicativi sanitari è vincolante ottenere la liberatoria all'implementazione delle soluzioni da parte della SC Sistemi Informativi Aziendali, a prescindere dalla forma di finanziamento e dalla voce di bilancio (assistenza e/o ricerca).

11.1.Progettazione

La progettazione e lo sviluppo di soluzioni che necessitino l'introduzione in azienda di apparati HW e soluzioni SW comporta la negoziazione delle specifiche in fase preliminare con gli esperti individuati dal responsabile della SC Sistemi Informativi Aziendali. Le specifiche da negoziare devono comunque riguardare i seguenti ambiti operativi:

1. definizione delle competenze ed individuazione degli amministratori di sistema con nomina formale dei responsabili, tramite compilazione dell'apposita modulistica;
2. individuazione delle responsabilità relativamente alla gestione della manutenzione;
3. definizione delle caratteristiche di connettività fisica e logica: protocollo, indirizzamento, definizione degli utenti;
4. definizione degli standard (sistemi operativi, etc.);
5. definizione ed integrazione con gli eventuali sistemi aziendali;
6. sicurezza informatica: patching ed antivirus aziendali.

11.2.Forniture di hardware e software

L'acquisto di qualunque tipologia di apparecchiatura hardware e software deve essere preventivamente concordata con l'SC Sistemi Informativi Aziendali al fine di poter dare parere tecnico sulla conformità rispetto

alle attuali configurazioni ed integrazioni tra i sistemi. Per ogni acquisto è comunque valida la normativa attualmente in vigore per le pubbliche Amministrazioni e le procedure in essere alla base del sistema gestionale amministrativo. Ogni apparecchiatura hardware deve essere acquistata con una copertura di garanzia di almeno tre anni, on-site, con intervento declinato a seconda delle differenti esigenze e comunque non superiore al next business day.

Per l'acquisto di moduli software occorre compilare debitamente il MOD 267 "*Modulo richiesta per acquisizione e installazione di nuove componenti software"* disponibile sulla intranet aziendale.

Grande attenzione deve essere posta nei casi di trattamento di dati sensibili: se il software tratta dati di questo tipo, la SC SIA non ha la responsabilità della gestione del dato, ma deve essere interpellato il DPO aziendale per comprendere la corretta modalità di gestione delle informazioni e quali accorgimenti prendere. Solo a seguito del nullaosta del DPO sarà possibile acquistare e/o acquistare il software appena descritto.

Il modulo correttamente compilato e comprensivo di indicazioni del DPO deve essere consegnato tramite mail all'indirizzo fleetmanagement@istituto-besta.it per ricevere il nullaosta del Responsabile dei Sistemi Informativi Aziendali.

Saranno accettate unicamente richieste di fornitura di materiale hardware non previste dalla gestione globale dei sistemi informativi aziendali solo se accompagnate da motivazione e/o progetto nell'ambito del quale si rende necessario acquisire quanto indicato, una volta che la copertura economica per l'acquisto risulta garantita, solo di seguito a corretta compilazione del MODSIA_10 "*Modulo di raccolta dati per componenti hardware"*. Le apparecchiature hardware, di qualunque genere nell'ambito informatico, non devono essere in contrasto con il presente disciplinare e con le regole di Sicurezza dei Sistemi Informativi.

Si ricorda che anche in caso di acquisto di dispositivi elettromedicali deve sempre essere presa comunicazione con la SC Sistemi Informativi Aziendali nei casi in cui sia necessario un pc per comprendere le corrette caratteristiche necessarie per la messa in rete del dispositivo sull'infrastruttura aziendale.

12. INTEGRAZIONE CON I SISTEMI INFORMATIVI

Il Servizio della Fondazione che ha necessità di collegare apparecchiature in rete (Ingegneria Clinica, Servizio Tecnico, etc.) dovrà compilare il modulo MOD 268 *"Scheda di richiesta per la messa in rete di nuovi sistemi"* disponibile sulla intranet aziendale ed accordarsi con la SC Sistemi Informativi Aziendali per procedere - di concerto con il Fornitore - all'allestimento, all'assegnazione di eventuali I.P. fissi se richiesti, all'installazione del S.O. richiesto, etc.

I responsabili di unità operativa devono compilare il modulo e trasmetterlo in formato elettronico all'indirizzo e-mail: fleetmanagement@istituto-besta.it

Il modello "Scheda di richiesta per la messa in rete di nuovi sistemi" è concepito per raccogliere tutti i dati necessari alla preparazione dei dispositivi e deve essere correttamente compilato e, solo a seguito del nullaosta della SC SIA, si potrà procedere alla messa in rete di nuovi sistemi. La SC SIA si riserva la possibilità di bloccare richieste considerate incomplete o non idonee.

Esulano dalla presente procedura le richieste di attivazione delle eventuali prese di rete necessarie che, come di consueto, verranno attivate tramite ticket fornendo tutte le indicazioni necessarie (Padiglione, Piano, n° di presa, etc.).

12.1. Integrazione con la rete aziendale

Il Fornitore che necessita integrarsi con la rete aziendale della Fondazione deve effettuare la perfetta integrazione di quanto fornito con il sistema informativo in essere presso la stessa.

La connessione alla rete aziendale di qualsiasi apparecchiatura deve essere preventivamente autorizzata dalla SC Sistemi Informativi Aziendali e deve uniformarsi alle policy adottate dalla Fondazione (indirizzi IP, naming convention, antivirus, accesso al dominio, etc.). In particolare non devono assolutamente essere installati e collegati all'infrastruttura aziendale modem, hub, Access Point o qualsiasi altra apparecchiatura non preventivamente autorizzata dalla SC Sistemi Informativi Aziendali.

È possibile accedere da remoto alla rete aziendale per attività di manutenzione e/o tele assistenza sulle apparecchiature installate; tale connessione dovrà rispettare le policy aziendali definite dalla SC Sistemi Informativi Aziendali.

La connessione remota prevede l'utilizzo di un client sicuro (fornito dalla Fondazione) che, sfruttando standard IPsec e/o SSL in connessione VPN, permette al fornitore il collegamento alle apparecchiature di propria competenza presenti sulla Intranet aziendale. Per la corretta attivazione della connessione in VPN è necessario che il fornitore compili il modulo MOD_SIA 04 o MOD_SIA 05 in base alla tipologia di connessione da attivare "Modulo richiesta accesso da remoto VPN_IPSEC" o "Modulo richiesta accesso da remoto VPN_SSL". Si specifica che all'interno di questi moduli viene richiesta anche la firma del Responsabile della SC o SS richiedente del servizio, cioè l'Ufficio interno con cui il fornitore ha stipulato il contratto per la Fondazione IRCCS Istituto Neurologico C. Besta. oltre a ciò sarà necessario ricevere una copia di un documento d'identità valido di tutti gli esterni che si devono collegare da remoto, così da verificarne l'identità.

Presso i locali destinati ad ospitare l'apparecchiatura in oggetto è presente un sistema di cablaggio rispondente agli standard nazionali ed internazionali in merito alle caratteristiche elettriche, fisiche, trasmissive, meccaniche e di installazione. Qualora, per motivi logistici, dovesse rendersi necessario lo spostamento/aggiunta di alcuni punti rete, l'attività è da ritenersi a carico del Fornitore. Quest'ultimo deve inoltre provvedere alla certificazione dei punti rete secondo quanto indicato nel documento "Specifiche cablaggio realizzazione e collaudo", consegnato su richiesta ed in caso di necessità alla società fornitrice.

La rete aziendale è stata progettata e implementata per garantire alle sue utenze un'infrastruttura sempre allineata allo stato dell'arte. La disponibilità dei servizi offerti è assicurata grazie ad un costante presidio di tecnici specializzati che, attraverso un continuo monitoraggio dell'impianto, segnalano eventuali anomalie.

Tuttavia, per garantire elevati livelli di sicurezza, limitare la propagazione di virus informatici e ottimizzare l'utilizzo di banda verso internet, è indispensabile che ogni nuova apparecchiatura connessa alla rete aziendale si uniformi alle politiche definite dalla SC Sistemi Informativi Aziendali.

Il pieno rispetto delle politiche è vincolante per ottenere il benestare alla connessione in rete dell'apparecchiatura.

Si ricorda che per ogni apparecchiatura che permetta lo scambio di dati che fuoriescono dalla Fondazione IRCCS Istituto Neurologico C. Besta è necessario nominare il responsabile esterno al trattamento dei dati, tramite apposita modulistica. La responsabilità della compilazione di tali moduli è demandata al Responsabile Privacy della struttura che farà uso dell'apparecchiatura o, in alternativa, al DEC del contratto in essere con il fornitore dell'apparecchiatura stessa.

In assenza della evidenza della avvenuta nomina verso i fornitori esterni non si procederà alla creazione delle utenze per la connessione da remoto.

12.2. Integrazione componenti applicative

Tutte le applicazioni che presumono la produzione di documenti di tipo sanitario (ad esempio referti, prescrizioni, etc.) devono prevedere una piena integrazione e compatibilità con il Sistema Informativo Socio Sanitario.

Tale integrazione deve garantire almeno le seguenti funzioni minime soggette all'evoluzione tecnologica regionale e nazionale:

- gestione firma attraverso carta operatore/OTP
- utilizzo dell'anagrafica regionale NAR tramite NPRI aziendale verso la quale deve essere disponibile piena e completa integrazione;
- invio dei documenti clinici elettronici DCE al Repository Aziendale e conseguente notifica al FSE 2.0;
- utilizzo dei nomenclatori SISS;
- integrazione applicativa attraverso il middleware della NPRI e/o successive modifiche ed evoluzioni tecnologiche;
- invio dei documenti elettronici verso la piattaforma aziendale di conservazione a norma dei documenti digitali.

12.3. Requisiti minimi richiesti

Si elencano qui di seguito le caratteristiche di minima della Postazioni per le quali è fatta richiesta di interconnessione alla rete aziendale.

12.3.1. Antivirus

La strumentazione deve essere dotata di Antivirus della Fondazione; la versione utilizzata è Sophos EndPoint Security and Control 10.8 o superiore, fornita dalla SC Sistemi Informativi Aziendali, e configurata per effettuare gli aggiornamenti direttamente attraverso il server della Fondazione. Volta per volta saranno valutati i singoli casi in cui l'apparecchiatura è dotata di una propria versione di Antivirus.

12.3.2. Join al dominio

Allo scopo di facilitare la condivisione delle informazioni tra le PdL, i server della Fondazione e le apparecchiature fornite dai fornitori, può essere opportuno effettuare la join al dominio dell'Istituto Besta. Necessarie ed ulteriori indicazioni verranno illustrate al bisogno dal personale della SC Sistemi Informativi Aziendali.

Sempre nell'ottica di facilitare l'accesso alle apparecchiature fornite, è fortemente consigliabile che il Fornitore integri i propri elaboratori con Active Directory Aziendale (Active Directory 2016 FFL 2012).

12.3.2.1. Condivisione ed elaborazione dati

Qualora si debbano condividere o trasmettere dati con/alle postazioni di lavoro gestite dalla SC Sistemi Informativi Aziendali, è necessario definire le modalità considerando che:

- il parco macchine gestito dalla SC Sistemi Informativi Aziendali è prevalentemente costituito da PC con S.O. Windows 10;
- gli utenti accedono al PC autenticandosi al dominio dell'Istituto Besta, utilizzando proprie credenziali nominali;
- l'installazione di un nuovo software su macchine gestire dalla SC Sistemi Informativi Aziendali può essere effettuato solo da personale afferente alla SC stessa;
- la configurazione delle postazioni di lavoro può essere effettuata solo da personale tecnico ingaggiato tramite apertura di apposito ticket all'indirizzo sd@sntx.it;
- non è ammessa l'installazione e l'attivazione autonoma di linee o collegamenti da e verso l'esterno;
- non sono ammesse connessioni LAN-to-LAN;
- non sono ammesse aperture di firewall, compresi i forward dall'interno verso l'esterno;
- non sono ammessi indirizzamenti IP non facenti parte del network gestito dalla SC Sistemi Informativi Aziendali.

Si ribadisce che anche l'installazione di eventuali software su PdL della SC Sistemi Informativi Aziendali deve avvenire previa verifica di compatibilità da parte della SC stessa.

Si specifica che il software e tutti i suoi componenti non devono utilizzare privilegi di amministratore locale (sono ammessi soltanto utente User o Power User).

Deve essere garantito l'aggiornamento ai sistemi operativi in caso di rilascio di versioni più aggiornate da parte delle ditte fornitrici.

Preventivamente alle attività da svolgere, il fornitore deve far pervenire alla SC Sistemi Informativi Aziendali una scheda tecnica delle attività da approntare per il corretto funzionamento delle apparecchiature di sua fornitura. Solo dopo un'analisi di questa documentazione tecnica e previo il benestare della SC Sistemi Informativi Aziendali, sarà possibile procedere con l'inizio lavori; nel caso in cui il fornitore - o chi per esso - proceda all'implementazione degli strumenti senza benestare, la SC Sistemi Informativi Aziendali si riserva la facoltà di disattivare ogni possibile forma di connettività alla rete aziendale dei macchinari collegati impropriamente.

La SC Sistemi Informativi Aziendali si riserva la facoltà di rifiutare applicazioni informatiche che in fase di installazione e/o di utilizzo presuppongano l'abuso di privilegi per l'account utente o computer; a tal proposito si evidenzia che le postazioni client in nessun caso possiedono privilegi amministrativi. Analogo divieto potrà essere opposto in caso di applicazioni che dialogano attraverso la rete utilizzando protocolli non pensati ai fini di una corretta pianificazione della sicurezza.

13. CONNESSIONE DA REMOTO PER INTERNI

Per quanto concerne la connessione da remoto per il personale interno, è possibile attivare la VPN previa autorizzazione del proprio Responsabile tramite corretta compilazione del MOD_SIA 09 "Modulo richiesta attivazione VPN – personale interno", seguendo le indicazioni e le informazioni contenute nell'istruzione operativa IOSIA_09 "Autorizzazione al collegamento in VPN all'infrastruttura aziendale" che descrive nel dettaglio tutti i passaggi necessari per un corretto utilizzo della risorsa.

Si ricorda che, siccome si tratta di licenze che rappresentano un costo per l'Azienda, la richiesta di attivazione della connessione in VPN deve essere fatta solo nei casi di estrema necessità. Tutti gli utenti che non provvederanno alla sua attivazione nei tempi corretti, descritti nella manualistica, verranno disattivati.

14. CONTROLLI

È vietato l'uso delle risorse aziendali per scopi diversi da quelli specificati nel mansionario e nelle istruzioni operative impartite dalla Fondazione: gli autorizzati all'uso di tali strumenti dalla Fondazione sono quindi responsabili del corretto utilizzo degli stessi, secondo le istruzioni ricevute. Anche nel caso in cui la prestazione lavorativa, svolta per la Fondazione venga effettuata in sede diversa da quella aziendale e/o con strumenti personali, ogni diritto sul lavoro svolto (es. codice, progetto, processo) ivi incluso il diritto intellettuale, copyright, brevetto, resta unicamente di proprietà del titolare.

Al fine di contenere possibili rischi di attacchi informatici ed azioni fraudolente, la Fondazione può attivare a distanza i controlli necessari al monitoraggio del flusso di dati dalla postazione di lavoro, in ottemperanza dell'art. 4 L. 300/70 comma 1 e 3 e con le seguenti finalità:

- verificare le funzionalità del sistema e degli elementi del sistema informativo aziendale nell'ottica di garantire il corretto esercizio;
- evitare che siano commessi illeciti o per esigenze di carattere difensivo o in ottica preventiva;
- tutelare la sicurezza e l'integrità del patrimonio informativo.

Ciò potrà anche comportare ad esempio la verifica, saltuaria o secondo necessità, delle informazioni di navigazione del browser, della e-mail, dei log e degli altri strumenti.

Le attività di controllo potranno avvenire, anche con ausilio di soggetti esterni, tramite monitoraggio audit e ispezioni del sistema informatico dei dispositivi aziendali e collegati alla rete.

I controlli vengono svolti nel pieno rispetto dei principi di necessità, pertinenza e non eccedenza - di cui alla normativa vigente sulla Privacy - ed evitando ogni interferenza ingiustificata sui diritti e sulle libertà dei lavoratori. I controlli saranno eseguiti, come sopra premesso, in primo luogo con modalità aggregate e anonime, in accordo al principio di gradualità. Il controllo anonimo può concludersi con un avviso generalizzato relativo ad un rilevato utilizzo anomalo degli strumenti aziendali e con l'invito ad attenersi scrupolosamente a compiti assegnati e istruzioni impartite. L'avviso può essere circoscritto a dipendenti afferenti alla Struttura o al Dipartimento in cui è stata rilevata l'anomalia. In assenza di successive anomalie non è di regola giustificato effettuare controlli su base individuale. Qualora, invece, l'anomalia dovesse ripetersi e riguardare lo stesso ambito lavorativo si procederà con l'effettuazione di controlli più puntuali e su base individuale.

Avendo fornito al lavoratore un'adeguata informativa sulle regole previste per l'utilizzo lavorativo degli strumenti di cui si tratta e sulle modalità e i casi in cui potranno effettuarsi i controlli, la Fondazione può eseguire controlli sugli strumenti informatici utilizzati dal lavoratore per rendere la prestazione lavorativa (personal computer, tablet, telefoni e smartphone), senza la necessità di accordi sindacali preventivi. A tal riguardo, si dà atto che l'informativa ai lavoratori, di cui sopra, viene garantita dalla Fondazione mediante la diffusione del presente Disciplinare.

La Fondazione promuove ogni opportuna misura organizzativa e tecnologica volta a prevenire il rischio di usi impropri e volto a prevenire il trattamento illecito sui dati trattati con strumenti informatici.

15. RESPONSABILITA E SANZIONI

L'utente è responsabile del corretto utilizzo delle risorse informatiche che la Fondazione mette a disposizione per svolgere le attività istituzionali e in particolare:

- è tenuto ad utilizzare le risorse a sua disposizione esclusivamente per le finalità d'ufficio, nel rispetto e nei limiti delle autorizzazioni ricevute, oltre che del presente disciplinare, astenendosi da ogni attività che possa compromettere il corretto funzionamento del sistema;
- è tenuto a mantenere un'adeguata riservatezza sui dati, sulle misure di sicurezza adottate e sulle modalità di accesso ai servizi, astenendosi da ogni attività che possa compromettere o porre in pericolo tale riservatezza;
- risponde personalmente di eventuali danni cagionati con il proprio comportamento al patrimonio o all'immagine della Fondazione.
- È tenuto ad utilizzare esclusivamente software licenziati sotto la propria responsabilità.

Tutti gli utenti sono tenuti ad osservare e a far osservare, secondo il ruolo rivestito in Fondazione, le disposizioni contenute nel presente Disciplinare, la cui violazione, che costituisce inadempimento contrattuale, è fonte di responsabilità disciplinare da accertare nei tempi e nei modi previsti dalla legge e dalla contrattazione collettiva. Le medesime violazioni possono altresì dar luogo a responsabilità di natura civile, contabile e penale, secondo le norme vigenti.

Sono tenuti al rispetto del presente disciplinare anche tutti i soggetti terzi che si trovano ad operare a vario titolo nell'ambito della Fondazione, inclusi i collaboratori in servizio con contratto di prestazione d'opera professionale.

16. VALIDITÁ E PUBBLICAZIONE

Il presente disciplinare ha validità a decorrere dalla deliberazione di adozione del provvedimento ed a partire dalla data di adozione della deliberazione tutte le disposizioni precedentemente adottate sono abrogate e sostituite dalla presente. Sono fatte salve e si fa espresso rinvio alle disposizioni contenute in norme di legge, regolamentari o contrattuali.

Del presente disciplinare sarà fornita la massima pubblicità e diffusione mediante la pubblicazione sulla intranet aziendale. Data la pregnanza di tale documento, si diffonde anche alla SC Risorse Umane in modo da darne visibilità a tutti i neoassunti in fase di forma del contratto.