	FONDAZIONE CASA DI DIO ETS	
FONDAZIONE CASA DI DIO ETS	**REGOLAMENTO UNICO PER IL TRATTAMENTO DEI DATI E L'UTILIZZO DEGLI STRUMENTI INFORMATICI** *Documento connesso al Modello di Organizzazione, Gestione e Controllo ex D.Lgs 231/01 e al Sistema Data Protection*	**Rev.02**

Revisione	Data	Motivo della revisione	Visto preparazione	Approvazione Consiglio Generale di indirizzo
00	13.12.2012	Prima emissione	DG Paolo Scalco	Delibera n°171
01	23.08.2019	Recepimento modifiche formali	SSDG	Direttore Generale Stefania Mosconi
02	07.09.2026	Recepimento trasformazione ETS, nuovo assetto organizzativo e nuove normative	Elena Sandrini Stefano Cumbo	Delibera n°40

PARTE I: PRINCIPI GENERALI E COMPORTAMENTI

1.1 Premessa, finalità e autorità

Il presente documento indica le regole di comportamento che i componenti degli organi istituzionali e di controllo, i dipendenti e i liberi professionisti sono tenuti a rispettare nell'ambito delle attività svolte per la Fondazione. Tali regole sono volte ad assicurare che la Fondazione operi nell'interesse degli ospiti, salvaguardandone i diritti, e che l'utilizzo degli strumenti informatici aziendali avvenga nel rispetto della sicurezza delle informazioni.

Nello svolgimento del proprio incarico, tutto il personale opera sotto la diretta autorità del Titolare del trattamento (Fondazione Casa di Dio ETS). Il presente Documento è subordinato e si adegua obbligatoriamente alle seguenti disposizioni di legge, regolamento e norme tecniche vigenti, che ne costituiscono la base giuridica e operativa:

- **Regolamento UE 2016/679 (GDPR)** relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali e alla libera circolazione di tali dati.
- **D.Lgs. 30 giugno 2003 n. 196 (Codice Privacy)**, come modificato e integrato dal **D.Lgs. 101/2018**.
- **D.Lgs. 8 giugno 2001 n. 231** in materia di responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni.
- **Legge 20 maggio 1970 n. 300 (Statuto dei lavoratori)**, con particolare riferimento all'**Art. 4** che disciplina le condizioni per l'installazione di impianti audiovisivi e altri strumenti di controllo a distanza.
- **Provvedimento del Garante per la protezione dei dati personali del 1° marzo 2007**, recante le "Linee guida sull'uso di posta elettronica e Internet nei luoghi di lavoro".
- **Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008** e successive modifiche e integrazioni in materia di adempimenti connessi alla figura degli "Amministratori di sistema".
- **Direttiva UE 2022/2555 (NIS2)** e relativo decreto nazionale di recepimento **D.Lgs. 138/2024** in materia di misure per un livello elevato comune di cybersicurezza nell'Unione.

- **Regolamento UE 2024/1689 (AI Act)** e **Legge 23 settembre 2025, n. 132** recante disposizioni e deleghe al Governo in materia di utilizzo dei sistemi di intelligenza artificiale.
- **Norme tecniche internazionali ISO/IEC 27001:2022 e ISO/IEC 27002:2022** relative ai requisiti e alle buone pratiche per i Sistemi di Gestione della Sicurezza delle Informazioni.

L'inosservanza di quanto prescritto nel presente testo unico equivale a un'inosservanza degli obblighi contrattuali e dei doveri d'ufficio verso la Fondazione.

1.2 Struttura del testo unificato

Ai fini di una corretta lettura, si specifica che le disposizioni del presente documento sono coordinate secondo un'articolazione in cinque macroaree logiche:

1. La prima parte concerne l'ambito applicativo, i riferimenti normativi e i doveri di comportamento e riservatezza degli esponenti aziendali, dei dipendenti e dei liberi professionisti.
2. La seconda parte delinea l'organizzazione interna, la ripartizione delle funzioni privacy, le modalità di esecuzione dei controlli aziendali e i tempi di conservazione dei log tecnici.
3. La terza parte disciplina i rapporti con l'utenza, la trasparenza informativa e la raccolta dei consensi.
4. La quarta parte stabilisce le norme di attuazione pratiche per la gestione degli archivi (cartacei e digitali), delle postazioni di lavoro e dei servizi di rete (e-mail, Internet, Cloud, dispositivi BYOD e Intelligenza Artificiale).
5. La quinta parte fissa le disposizioni speciali per la sicurezza fisica, i sistemi di videosorveglianza, le notifiche di incidenti e le regole in caso di cessazione del rapporto di lavoro.

1.3 Obblighi di riservatezza e circolazione delle informazioni

- **Segreto d'ufficio:** Tutti i soggetti destinatari sono tenuti a mantenere la massima riservatezza sulle informazioni di carattere confidenziale acquisite dagli ospiti o di cui comunque dispongano in ragione della propria funzione. È fatto assoluto divieto di rivelare a terzi o fare uso improprio delle informazioni riservate di cui siano venuti a conoscenza. Le suddette informazioni ove contenute nei supporti informatici di collaboratori esterni, devono essere protette secondo quanto stabilito dal reg. UE 2016/679.
- **Principio della necessità di conoscere:** Le informazioni aventi carattere confidenziale possono essere diffuse e circolare nell'ambito delle strutture e degli uffici della Fondazione solo ed esclusivamente nei riguardi di coloro che abbiano un'effettiva necessità di conoscerle per stretti motivi di lavoro.
- **Collaboratori esterni:** Le informazioni riservate eventualmente contenute o transitanti nei supporti e nei sistemi informatici dei collaboratori e professionisti esterni devono essere protette garantendo i medesimi standard di sicurezza richiesti al personale interno.
- **Quadro sanzionatorio:** L'inosservanza degli obblighi di riservatezza da parte delle figure sopra indicate costituisce violazione delle prescrizioni del Modello Organizzativo 231 della Fondazione. Essa comporta l'immediata attivazione delle procedure sanzionatorie e l'applicazione delle sanzioni disciplinari previste dal Codice Disciplinare (Capitolo 6 del MOG) e dai CCNL di categoria vigenti, ferma restando l'eventuale attivazione di responsabilità civili o penali qualora la condotta configuri un illecito di legge.

1.4 Operazioni personali e conflitto di interessi

- **Divieto di utilizzo informativo:** I componenti degli organi amministrativi, i dipendenti e i liberi professionisti non possono in alcun modo utilizzare le informazioni confidenziali ricevute dagli ospiti o apprese in ragione del proprio ufficio per effettuare operazioni finanziarie o personali, sia direttamente sia per interposta persona.
- **Obbligo di astensione:** È fatto divieto di effettuare operazioni o compiere atti gestionali nei quali gli operatori abbiano un interesse personale che si trovi in conflitto con quello dell'ospite. Il dipendente che ritenga di trovarsi in una situazione di conflitto di interessi, anche potenziale, deve darne immediata notizia ai propri responsabili di servizio, i quali provvederanno a valutare il caso e, se necessario, a sollevare formalmente il dipendente dallo specifico incarico o valutazione.

L'inosservanza dei precedenti commi da parte dei dipendenti e collaboratori configura una violazione dei doveri di fedeltà e delle disposizioni datoriali, comportando l'applicazione delle sanzioni disciplinari e dei rimedi contrattuali definiti nel sistema sanzionatorio del MOG (Capitolo 6) e dalle norme contrattuali applicabili.

1.5 Rapporti esterni: Mezzi di Informazione e Pubblica Amministrazione

- **Canali autorizzati:** I rapporti con la stampa e con gli altri mezzi di comunicazione di massa sono riservati in via esclusiva al Consiglio Generale di indirizzo, al Comitato di Amministrazione e al Direttore generale. Le comunicazioni esterne devono svolgersi unicamente secondo le procedure organizzative preventivamente fissate dalla Fondazione.
- **Diffusione dati particolari:** È assolutamente vietato diffondere dati appartenenti alle categorie particolari di dati, incluse le immagini e/o le videoregistrazioni riguardanti gli ospiti di tutti i servizi della Fondazione, senza che sia stato acquisito il preventivo consenso esplicito e scritto da parte dell'interessato stesso o del soggetto che ne esercita la tutela legale.
- **Integrità e indipendenza:** I rapporti con le pubbliche amministrazioni, le organizzazioni politiche, le rappresentanze sindacali e gli altri soggetti esterni devono essere improntati alla massima correttezza, integrità, imparzialità e indipendenza. Deve essere evitata qualsiasi condotta che possa dare l'impressione di voler influenzare impropriamente le decisioni della controparte o di richiedere trattamenti di favore.
- **Divieto di benefici indebiti:** Nei suddetti rapporti esterni, nonché in quelli commerciali con enti pubblici e privati, è tassativamente vietato promettere, offrire, erogare o ricevere favori, somme di denaro, regalie o benefici di altra natura volti a ottenere vantaggi impropri o corsie preferenziali per l'ente o per sé.

PARTE II: ORGANIZZAZIONE INTERNA, CONTROLLI E REGISTRI TECNICI

2.1 Funzioni di controllo e coordinamento

- La Fondazione organizza la protezione dei dati e la sicurezza dei sistemi informativi definendo compiti chiari per le funzioni di coordinamento e controllo interno, le quali operano secondo adeguati standard professionali:
- **RDSP (Rappresentante della Direzione del Sistema di Protezione dei Dati- Direttore Generale):** Costituisce la funzione di coordinamento interno dell'intero sistema di tutela dei dati personali.
- **Responsabili interni dei trattamenti:** Figure direttive designate all'interno dei singoli servizi o uffici che controllano operativamente la conformità dei trattamenti quotidiani.

- **DPO (Responsabile della Protezione dei Dati) esterno:** Soggetto indipendente incaricato di effettuare periodiche verifiche sulla conformità dei trattamenti rispetto alla normativa vigente, aggiornare la valutazione dei rischi informatici e controllare il rispetto delle procedure interne.
- **Amministratore di Sistema:** Persona fisica interna designata per le attività operative di gestione, manutenzione e controllo tecnico del sistema informativo aziendale, la quale può operare avvalendosi del supporto specialistico di consulenti esterni.

La Fondazione assicura che il personale addetto ai controlli disponga di adeguata esperienza, che le risorse siano proporzionate alla complessità delle attività dell'ente, e che le verifiche vengano pianificate regolarmente indirizzandole verso le aree caratterizzate da maggior rischio aziendale, documentando formalmente gli esiti in appositi verbali. L'elenco dei controlli e le frequenze degli stessi sono riepilogati nel documento del Sistema Data Protection.

2.2 Bilanciamento dei controlli e tutela dei lavoratori (Art. 4 Statuto dei Lavoratori)

La Fondazione ha il diritto di effettuare controlli volti a verificare il corretto utilizzo degli strumenti informatici aziendali per esclusive esigenze produttive, organizzative, per prevenire o risolvere malfunzionamenti, rilevare incidenti di sicurezza o contrastare utilizzi anomali e illeciti che potrebbero essere fonte di responsabilità civile o penale per l'ente.

In conformità all'articolo 4 della Legge 300/1970 e ai provvedimenti del Garante, le verifiche sono ispirate ai principi di liceità, minimizzazione e proporzionalità, ed escludono controlli di natura invasiva:

- **Limitazione sui contenuti:** Le attività di verifica non avvengono in modo sistematico, preventivo o continuativo sul singolo dipendente. Esse riguardano esclusivamente l'analisi delle componenti tecniche di traffico e dei parametri dei file di registro. **È tassativamente vietato analizzare il contenuto testuale delle comunicazioni, delle e-mail e dei messaggi scambiati dai lavoratori**; l'accertamento è limitato ai dati di instradamento, definiti anche metadati (ad esempio: orari, dimensioni dei file, indirizzi telematici dei siti visitati, numeri telefonici chiamanti/chiamati o indirizzi di posta elettronica di mittente/destinatario).
- **Informativa e gradualità:** I lavoratori sono informati preventivamente sulle modalità di effettuazione dei controlli. Qualora si rendano necessarie verifiche puntuali su un singolo utente a fronte di fondati sospetti di violazione, l'ispezione si svolge con modalità graduali, partendo da dati aggregati e scendendo nel dettaglio tecnico solo se strettamente indispensabile. L'accesso ai file di registro è consentito solo al personale tecnico autorizzato e ogni sessione di controllo viene tracciata.

Tempi di conservazione dei file di registro tecnici:

- **File di registro di traffico delle postazioni di lavoro**: Conservati per un periodo ordinario massimo di 7 giorni per finalità di sicurezza e manutenzione, trascorsi i quali vengono cancellati automaticamente. In presenza di incidenti informatici o procedimenti disciplinari formali, il termine di conservazione è estensibile fino a un massimo di 6 mesi complessivi, previa annotazione nel Registro dei Trattamenti.
- **Metadati di Posta Elettronica**: Conservati per un periodo massimo di 30 giorni per finalità di sicurezza informatica ordinaria. In presenza di specifici incidenti o esigenze di accertamento documentate, il termine può essere esteso fino a un massimo complessivo di 6 mesi totali, previa annotazione nel Registro dei Trattamenti.

- **File di registro di Navigazione Internet**: Registrati temporaneamente e conservati per un periodo ordinario massimo di 30 giorni per finalità di sicurezza. In presenza di incidenti, il termine è estensibile fino a un massimo complessivo di 6 mesi totali, previa annotazione nel Registro.

PARTE III: RAPPORTI CON L'UTENZA

3.1 Trasparenza, Informativa e Gestione dei Consensi

- **Accesso ai diritti:** Fermi restando gli obblighi informativi di legge, la Fondazione tiene a disposizione degli utenti adeguata documentazione illustrativa sui servizi offerti. Il personale incaricato ha il compito di rendere accessibile e illustrare i contenuti dell'Informativa sulla Riservatezza e le modalità operative con cui gli utenti (o i loro rappresentanti legali) possono esercitare i diritti di accesso, rettifica, cancellazione e limitazione previsti dagli articoli 15-18 del Regolamento Europeo.
- **Consensi per immagini e video:** Qualora lo svolgimento delle attività comporti un trattamento di dati personali attraverso riprese fotografiche o registrazioni video, il personale incaricato deve tassativamente assicurarsi – prima di effettuare qualsiasi ripresa – che gli interessati coinvolti o chi ne ha la legale tutela abbiano apposto la propria firma sullo specifico modulo di consenso scritto aziendale.

PARTE IV: REGOLE OPERATIVE PER GLI STRUMENTI DI LAVORO E ARCHIVI

4.1 Gestione degli archivi cartacei e dei documenti

- **Misure di protezione:** Deve essere prestata la massima attenzione ai documenti trattati quotidianamente al fine di prevenire rischi di distruzione, perdita accidentale o trattamenti non conformi alle finalità originarie. L'accesso agli archivi cartacei e ai locali di conservazione è rigorosamente ristretto al solo personale espressamente autorizzato in via permanente o occasionale. Qualsiasi copia cartacea o fotocopia deve essere gestita con la medesima diligenza e riservatezza riservata al documento originale.
- **Rigore sui Dati Particolari:** Il personale che tratta documenti cartacei contenenti dati sanitari o categorie particolari di dati deve applicare un controllo particolarmente rigoroso sull'accesso ai propri spazi di lavoro. Tali documenti devono rimanere al di fuori degli archivi o degli armadi protetti per il tempo minimo necessario all'operazione. È vietato allontanarsi momentaneamente lasciando i documenti incustoditi o visibili a terzi. Al termine dell'attività, ogni foglio deve essere immediatamente riposto negli schedari e negli armadi chiusi a chiave.
- **Archiviazione digitale e Classificazione:** Tutti i documenti informatici e i file di lavoro devono essere archiviati esclusivamente sui servitori (d'ora in avanti chiamati server) o depositi informatici aziendali centralizzati e autorizzati. È fatto divieto di salvare documenti o basi di dati locali sul piano di lavoro dello schermo (definito desktop) del computer o su dispositivi/dischi rigidi non cifrati. I dati digitali devono essere opportunamente classificati in base al livello di riservatezza stabilito
- **Infrastruttura di copia di sicurezza (definita backup) aziendale:** Gli archivi digitali e i documenti salvati sul server centrale rappresentano il patrimonio aziendale e vengono salvaguardati tramite copie di sicurezza automatiche eseguite quotidianamente e verificate dall'Amministratore di sistema. **Non viene effettuato alcun salvataggio di sicurezza dei dati personali o dei file memorizzati localmente sulle singole postazioni informatiche fisiche**. Ciascun incaricato ha

l'obbligo di trasferire i dati di importanza sostanziale per la Fondazione all'interno delle apposite cartelle condivise create sul server.

4.2 Sicurezza degli accessi, credenziali e applicativo di gestione delle password

- **Inviolabilità dell'account:** L'accesso ai computer, alla posta elettronica, ai software di lavoro e ai sistemi sanitari aziendali deve avvenire unicamente utilizzando le proprie credenziali personali, che sono protette da sistemi di autenticazione a più fattori ove disponibili. Le credenziali sono strettamente personali, non cedibili e non condivisibili. È vietato consentire ad altri utenti (inclusi i colleghi di reparto) di operare sui sistemi informatici sotto il proprio identificativo utente.

Regole per la gestione e la complessità delle password:

- È obbligatorio modificare la password predefinita assegnata dal Servizio Informatico alla prima connessione.
- La password deve essere modificata obbligatoriamente ogni 90 giorni, o immediatamente nei casi in cui vi sia il minimo dubbio inerente a una sua compromissione o furto.
- La password deve avere una lunghezza minima di 12 caratteri alfanumerici e includere, nella sua composizione, almeno un carattere numerico, uno maiuscolo e uno speciale. Non deve basarsi su informazioni facilmente deducibili (ad esempio: proprio nome, nomi di familiari, date di nascita o codici fiscali).
- È fatto assoluto divieto di trascrivere le password su supporti cartacei (ad esempio: foglietti adesivi) o all'interno di file di testo memorizzati sui dispositivi. L'utente è obbligato a utilizzare l'applicativo di gestione delle chiavi digitali (definito programma di gestione delle password) messo a disposizione dalla Fondazione per memorizzare in modo sicuro le proprie credenziali.

Procedura di ripristino per emergenza operativa: In caso di prolungata assenza imprevista o impedimento dell'utente che renda indispensabile intervenire per esclusive necessità operative e di sicurezza del sistema, il Dirigente dell'Area interessata richiede per iscritto all'Amministratore di Sistema il ripristino tecnico e la sostituzione della password del dipendente assente per garantire la continuità aziendale della Fondazione. Al termine del tempo strettamente necessario al recupero delle informazioni urgenti, il Dirigente dovrà richiedere una nuova sostituzione della password che verrà comunicata tempestivamente ed esclusivamente all'utente interessato al momento del suo rientro in servizio.

4.3 Postazioni fisiche e regime di virtualizzazione delle sessioni (Terminal Server)

- **Principi di utilizzo delle postazioni:** I computer sono assegnati in funzione del ruolo e sono destinati esclusivamente allo svolgimento delle attività connesse agli incarichi lavorativi; è vietata ogni attività o installazione per fini personali. L'accesso ai computer aziendali è riservato al personale della Fondazione (dipendente o in regime di libera professione); l'accesso di soggetti terzi (ad esempio: manutentori esterni) deve essere preventivamente autorizzato dall'Amministratore di sistema in accordo con il Titolare.
- **Obbligo di modalità di sessione virtuale centralizzata:** Gli operatori ai quali è stato prescritto l'obbligo esclusivo di lavorare tramite collegamento a un server centrale (sessione remota controllata dal server) devono operare unicamente all'interno dell'ambiente virtualizzato. **È tassativamente vietato esportare, salvare o scaricare file, basi di dati o archivi aziendali sui dischi fisici locali del computer o in spazi di archiviazione virtuali privati**. Il terminale fisico deve fungere esclusivamente da terminale leggero (ovvero da semplice tramite visivo). Qualora vi siano deroghe

documentate per esigenze operative, il dispositivo fisico locale deve essere obbligatoriamente protetto da password e interamente cifrato tramite sistemi crittografici attivi.

- **Integrità hardware e presidio:** Non è consentito aprire, manomettere o spostare le attrezzature informatiche senza autorizzazione del Servizio Informatico. È severamente vietato scollegare il cavo di rete dei computer aziendali per connettervi computer personali o di fornitori esterni. In caso di abbandono momentaneo della postazione di lavoro, il dipendente ha l'obbligo di bloccare lo schermo richiamando le funzioni di sicurezza del sistema operativo (funzione di blocco computer), per impedire utilizzi non autorizzati da parte di terzi. Al termine del turno lavorativo, tutte le postazioni e le relative periferiche (stampanti, dispositivi di scansione) devono essere spente.

4.4 Utilizzo corretto dei servizi di Posta Elettronica

- **Natura dello strumento:** Il servizio di posta elettronica aziendale costituisce uno strumento di lavoro e deve essere utilizzato per lo svolgimento di attività connesse alle mansioni affidate. Non è consentito l'utilizzo dell'indirizzo di posta della Fondazione per scopi personali, per l'iscrizione a portali web privati o commerciali, per l'invio di materiale pubblicitario o per la partecipazione a spazi di discussione telematica e liste di invio non professionali che possano sovraccaricare la rete. La Fondazione prevede l'utilizzo di due tipologie di caselle postali:
  - **Caselle postali mail nominative**: Questa tipologia di casella postale contiene, nell'indirizzo mail, il nome e cognome (anche "puntati) della persona. In caso di dimissioni del dipendente o collaboratore che ha in uso la casella postale, la Fondazione permetterà al dipendente di cancellare eventuali messaggi che contengono dati personali "propri" e si riserva di conservare solo i messaggi con contenuti di esclusivo interesse aziendale. La casella postale verrà successivamente disattivata e verrà attivato un risponditore automatico di "casella non più attiva".
  - **Caselle postali mail di funzione/condivise**: Questa tipologia di casella postale non contiene, nell'indirizzo mail, il nome e cognome (anche "puntati) della persona e può anche essere condivisa tra più dipendenti/collaboratori. In caso di dimissioni del dipendente o collaboratore che ha in uso la casella postale, l'Azienda permetterà al dipendente di cancellare eventuali messaggi che contengono dati personali "propri" e assegnerà l'accesso alla casella email ad un altro dipendente/collaboratore.
- **Scambio di dati sanitari via e-mail:** È vietato lo scambio e l'archiviazione di messaggi di posta elettronica idonei a rivelare categorie particolari di dati personali, salvo che tale scambio avvenga nell'esercizio delle funzioni istituzionali (ad esempio: gestione sanitaria degli ospiti), nel rispetto del sistema di protezione dei dati, previa autorizzazione del coordinamento interno (sentito il Responsabile della Protezione dei Dati) e adottando le misure di sicurezza obbligatorie, quali la cifratura del documento allegato.
- **Presidi di sicurezza e messaggi ingannevoli:** È fatto obbligo di verificare sempre l'attendibilità di una e-mail e dei suoi allegati prima di procedere alla loro apertura o di fare clic su collegamenti interni, prestando attenzione alla veridicità del nome del dominio del mittente (la parte a destra del carattere @) per evitare frodi o furti di credenziali. Gli allegati che avviano programmi automatici (definiti file eseguibili) possono essere aperti solo in caso di assoluta certezza della sorgente. È vietato inoltrare documenti dalla propria posta personale verso quella aziendale e viceversa, ed è illecito inviare messaggi sotto mentite spoglie impersonando un mittente diverso da quello reale.

- **Gestione delle caselle e-mail nominali e assenze programmate:** Le caselle di posta nominative contengono nell'indirizzo il nome e il cognome dell'operatore. In caso di assenza programmata (ad esempio: ferie), il lavoratore deve attivare i messaggi di risposta automatica messi a disposizione dal sistema, indicando il periodo preciso di assenza e i riferimenti della persona a cui rivolgersi per necessità lavorative.

Procedura di accesso formale in caso di emergenza lavorativa: Nel caso in cui, a seguito di un'assenza imprevista o prolungata del dipendente, sussistano improrogabili e documentate necessità operative aziendali che richiedano l'accesso a messaggi di posta elettronica nella sua esclusiva disponibilità, si applica la seguente e rigida procedura a tutela della riservatezza:

- L'accesso è consentito solo previa formale autorizzazione scritta del Titolare del Trattamento, su richiesta motivata del Dirigente del Servizio interessato.
- L'accesso è limitato ai soli messaggi di contenuto strettamente professionale necessari alla continuità operativa; è fatto assoluto divieto di accedere o visionare messaggi di natura personale o privata del dipendente.
- Prima di procedere, ove possibile, il dipendente assente deve essere preventivamente informato.
- L'accesso tecnico deve avvenire alla presenza obbligatoria di almeno due soggetti autorizzati: il Dirigente richiedente (o suo delegato) e un rappresentante del Servizio Informatico.
- Di tale accesso deve essere redatto un apposito verbale scritto che indichi: data, ora, soggetti presenti, motivazione e l'elenco analitico dei messaggi professionali consultati. Il verbale viene conservato e il dipendente viene informato dell'accesso avvenuto al suo rientro in servizio.

4.5 Limitazioni di Navigazione Internet

- **Finalità lavorative:** L’accesso alla rete internet aziendale deve avvenire per il perseguimento di finalità strettamente connesse agli incarichi lavorativi, presentandosi sempre con il proprio nome e senza registrarsi a siti i cui contenuti non siano legati all’attività lavorativa.
- **Restrizioni sui sistemi di condivisione e spazi virtuali privati:** È vietato trasferire, caricare o sincronizzare file dal proprio computer aziendale verso spazi di archiviazione virtuali esterni personali (servizi di memoria in rete non aziendali). Non è consentito scaricare, installare o utilizzare programmi applicativi gratuiti o in versione di prova prelevati da internet, salvo i casi esplicitamente autorizzati dal Servizio Informatico.
- **Protocolli di comunicazione e filtri automatici:** È fatto divieto di accedere a portali internet che utilizzino protocolli di comunicazione obsoleti e non protetti da cifratura, tra cui il protocollo di base HTTP (la navigazione deve avvenire esclusivamente su siti protetti identificati dalla sigla HTTPS). Al fine di ridurre i rischi informatici, la Fondazione utilizza filtri automatici di blocco per inibire l'accesso a categorie di siti considerate non correlate con la prestazione lavorativa o per prevenire il caricamento/scaricamento di file aventi caratteristiche di estensione o dimensioni pericolose.

4.6 Disciplina sull'uso lavorativo di dispositivi privati

- **Vigilanza sui dispositivi portatili:** I computer portatili e i telefoni cellulari aziendali presentano elevate vulnerabilità informatiche e rischio di smarrimento. È fatto obbligo di conservare i dispositivi in un luogo sicuro al termine della giornata lavorativa e di non lasciarli mai incustoditi qualora siano utilizzati all’esterno dell’ufficio.

- **Misure di protezione:** I dispositivi mobili aziendali devono essere protetti da codici di sblocco complessi. È obbligatorio impostare e non divulgare i codici di cifratura dei dischi rigidi per i computer portatili e non eliminare o alterare le impostazioni di protezione stabilite dall'Amministratore di sistema. Non devono essere conservate informazioni personali o private nella memoria dei dispositivi aziendali.
- **Divieto generale e regole di deroga:** L'utilizzo di risorse informatiche o dispositivi mobili privati (computer, telefoni, supporti di memoria) per lo svolgimento delle attività lavorative è espressamente vietato, salvo previa ed esplicita autorizzazione scritta. Nei casi eccezionali in cui venga concessa tale deroga, l'utente è obbligato a uniformarsi alle seguenti prescrizioni, pena l'applicazione di sanzioni:
  - I dati trattati devono risiedere esclusivamente sulle infrastrutture informatiche centralizzate dell'ente; è vietato scaricare, archiviare o trasferire file, dati o archivi della Fondazione sulla memoria locale del dispositivo personale o su servizi di archiviazione virtuale privati.
  - L'accesso al dispositivo privato deve essere rigorosamente protetto da credenziali forti (codice numerico o sistemi biometrici) e disporre della funzione di blocco automatico dello schermo attiva.
  - È fatto divieto di utilizzare o configurare la posta elettronica aziendale su dispositivi personali se non espressamente autorizzati.
  - Nel caso in cui il dispositivo privato autorizzato venga venduto o trasferito a terzi, l'utente deve provvedere alla cancellazione irreversibile di ogni traccia di dato aziendale.

4.7 Utilizzo di Sistemi di Messaggistica Istantanea e Reti Sociali

- **Account e finalità aziendali:** L'utilizzo di sistemi di messaggistica istantanea (es. Whatsapp o equivalenti) tramite utenze o profili aziendali deve essere limitato esclusivamente alle finalità di servizio per comunicare con referenti interni, ospiti o fornitori dell'ente. L'eventuale utilizzo di canali e reti sociali (quali piattaforme di condivisione di profili o immagini pubblicitarie) o la pubblicazione di contenuti a nome dell'ente deve essere preventivamente ed esplicitamente autorizzato dalla Fondazione.
- **Divieto sui dati sensibili e sanitari:** È tassativamente vietato l'invio di dati personali o dati sanitari degli ospiti tramite sistemi di messaggistica non approvati formalmente. Le informazioni scambiate non devono in alcun modo ledere i diritti o la dignità delle persone, né violare i principi di tutela della proprietà o dei progetti interni dell'ente.
- **Tracciabilità formale delle operazioni:** L'uso di messaggi rapidi per trasmettere informazioni operative rilevanti o modifiche agli accordi deve essere obbligatoriamente seguito da una successiva conferma formale inviata via posta elettronica aziendale o registrata sui sistemi informatici ufficiali dell'ente, al fine di garantirne la storicità.

4.8 installazione di software sui dispositivi aziendali

I dipendenti sono tenuti a utilizzare esclusivamente software, programmi, utility o altri componenti informatici preventivamente approvati e installati dall'Azienda.

L'uso di software non autorizzati, inclusi strumenti freeware, shareware, open source o di prova, è espressamente vietato, anche qualora l'intento sia quello di migliorare la produttività o agevolare le attività lavorative.

Richiesta di nuovi software: Nel caso in cui un dipendente ritenga indispensabile l'utilizzo di un nuovo software o applicazione per lo svolgimento delle proprie mansioni, deve inoltrare una richiesta motivata al proprio Responsabile o al Servizio informatico della Fondazione.
L'eventuale approvazione e successiva installazione potranno avvenire solo dopo la valutazione tecnica e di sicurezza da parte dell'Azienda, che ne verificherà la compatibilità con i sistemi aziendali, la conformità normativa (inclusa la licenza d'uso) e l'assenza di rischi per la sicurezza informatica.

4.9 Limitazioni stringenti sull'uso dell'Intelligenza Artificiale (AI)

L'uso di strumenti, piattaforme o applicazioni basate su Intelligenza Artificiale – inclusi i programmi di conversazione automatica (definiti chatbot), i generatori di testo o immagini, i traduttori automatici e gli analizzatori di dati informatici, sia accessibili via web sia integrati nei software per l'ufficio – è consentito esclusivamente per finalità lavorative e nel rispetto delle norme sulla riservatezza.
Divieto assoluto di immissione dati: È fatto assoluto divieto di inserire, trattare o condividere all'interno dei comandi testuali (definiti prompt) o dei sistemi di Intelligenza Artificiale dati, informazioni o documenti che riguardino:

- Persone fisiche identificabili o identificabili anche indirettamente (ad esempio: nomi, contatti, codici fiscali, cartelle cliniche, dati sanitari o amministrativi di ospiti, dipendenti, utenti o collaboratori).
- Persone giuridiche, società, enti o fornitori, qualora tali informazioni aziendali non siano già di pubblico dominio.
- Situazioni particolari, relazioni di servizio, eventi interni o casi clinici che possano ricondurre, anche indirettamente attraverso dettagli di contesto, a soggetti fisici o partner della Fondazione.

Condizioni vincolanti per l'uso: L'utilizzo di strumenti di Intelligenza Artificiale è ammesso solo se avviene tramite profili aziendali autorizzati e se la piattaforma garantisce contrattualmente che i dati inseriti non vengano utilizzati per l'addestramento dei modelli esterni, non vengano conservati o condivisi fuori dai limiti tecnici dell'elaborazione e siano protetti da sistemi di autenticazione forte. Ogni utilizzo non rispondente a tali criteri deve essere preventivamente sottoposto alla Direzione per le verifiche di conformità alle norme europee.
Il dipendente o collaboratore è personalmente responsabile dell'uso corretto di tali strumenti e del rispetto delle presenti disposizioni. L'Azienda potrà effettuare verifiche periodiche o mirate per controllare l'utilizzo delle piattaforme di Intelligenza Artificiale e garantire la protezione dei dati trattati.

PARTE V: DISPOSIZIONI SPECIALI E APPLICAZIONE FINALE

5.1 Accesso alla Cartella Clinica Informatizzata e servizi regionali sanitari

- **Accesso Esterno alla Cartella Sanitaria:** Per gli operatori appositamente incaricati ai quali è concesso l'accesso alla cartella sanitaria informatizzata degli ospiti al di fuori delle sedi della Fondazione, è richiesta una particolare attenzione per mitigare il rischio di diffusione non autorizzata. È tassativamente vietato accedere alla cartella dall'esterno se non per necessità assistenziali comprovate ed è vietato esportare o salvare dati al di fuori dell'applicazione della cartella stessa senza autorizzazione della Fondazione.
- **Obblighi per i titolari di tessere sanitarie di accesso ai servizi regionali:** Gli operatori sanitari titolari di carta di accesso ai servizi telematici regionali devono custodire la tessera a microprocessore e i relativi codici di sblocco (definiti codici PIN e PUK) in modo sicuro e separato. I codici di accesso sono strettamente personali e non devono essere per nessun motivo comunicati

a terzi o trascritti in chiaro su carta o supporti digitali. L'operatore deve modificare il proprio codice qualora ritenga compromessa la riservatezza e deve comunicare prontamente all'ente emettitore e al Servizio Informatico lo smarrimento, il furto o eventuali violazioni di sicurezza della tessera.

5.2 Gestione dei sistemi di Videosorveglianza

Gli impianti di videosorveglianza sono installati e utilizzati esclusivamente per finalità di sicurezza del lavoro, protezione del patrimonio aziendale ed esigenze organizzative e produttive, ai sensi dell'articolo 4, comma 1, della Legge 300/1970, in stretta conformità con l'accordo sindacale stipulato con le rappresentanze dei lavoratori in data 08.02.2018 e successive modifiche e integrazioni:

- **Conservazione ordinaria:** Le immagini videoregistrate sono conservate per un periodo massimo di **24 ore** dall'acquisizione, trascorso il quale vengono sovrascritte e cancellate in modo completamente automatico dal sistema.
- **Prolungamento dei termini per incidenti:** In caso di reati, furti, sinistri o esigenze di accertamento debitamente documentate, le immagini possono essere isolate e conservate per il tempo strettamente necessario alla gestione dell'evento, e comunque non oltre il termine massimo di **15 giorni**, fatte salve diverse e specifiche disposizioni dell'Autorità Giudiziaria.
- **Custodia e Accesso:** Le immagini sono archiviate su dispositivi di registrazione protetti all'interno di armadi chiusi a chiave, accessibili esclusivamente al personale formalmente autorizzato e indicato nel Registro dei Trattamenti. La visione e l'accesso ai dati sono tracciati e verbalizzati.
- **Informativa minima:** I lavoratori e i visitatori sono informati della presenza delle telecamere mediante apposita cartellonistica conforme alle indicazioni del Garante, collocata ben visibile in prossimità delle aree riprese, prima dell'ingresso nelle stesse.

5.3 Sicurezza fisica: Tessere magnetiche di presenza e Chiavi aziendali

Le tessere magnetiche (definite anche badge) per la rilevazione delle presenze e le chiavi fisiche di accesso ai reparti, ai magazzini o agli armadi d'archivio protetti costituiscono strumenti di lavoro di proprietà aziendale affidati in custodia all'operatore. L'assegnatario si impegna a proteggerli da furto, perdita o danneggiamento, con il divieto assoluto di lasciarli in luoghi incustoditi o di cederli a colleghi o terzi. Lo smarrimento o il furto devono essere segnalati immediatamente al Titolare per consentire la tempestiva disattivazione logica dei permessi. Alla cessazione del rapporto di lavoro, tutti i dispositivi di accesso e le chiavi devono essere riconsegnati al Titolare.

5.4 Obbligo di segnalazione degli incidenti e furti (Violazione dei dati personali)

Nel caso si verifichi lo smarrimento, il furto o la compromissione di strumenti informatici aziendali (computer portatili, telefoni cellulari, supporti di memoria removibili) o di documentazione cartacea contenente dati personali o dati sanitari relativi agli ospiti o ai dipendenti, **l'utente ha l'obbligo tassativo di informare immediatamente e senza alcun ritardo la Fondazione (Direzione e referente interno del sistema di protezione dei dati)**. La segnalazione immediata è un obbligo normativo critico che permette all'ente di verificare la problematica, disporre il blocco degli accessi, eseguire la cancellazione dei dati a distanza e attivare la procedura interna di valutazione del rischio per verificare la necessità di notificare l'evento (configurabile come violazione dei dati personali) all'Autorità Garante entro il termine perentorio di 72 ore previsto dalle norme europee. Per i dispositivi informatici e i beni della Fondazione, l'utente è inoltre obbligato a sporgere immediata e regolare denuncia alla competente autorità giudiziaria, inviandone tempestivamente copia all'Amministratore di sistema.

5.5 Archiviazione e classificazione dei dati

Tutti i documenti e i file devono essere archiviati esclusivamente su server o repository aziendali autorizzati (es. file server, SharePoint, NAS).

È vietato salvare documenti su desktop o dispositivi non cifrati (se al di fuori di sessioni Remote Desktop, Citrix o similari)

I dati devono essere classificati in base al livello di riservatezza (pubblico, interno, riservato, confidenziale).

5.6 Gestione della cessazione del rapporto di lavoro

In caso di cessazione del rapporto di lavoro o di collaborazione a qualunque titolo, l'utente deve mettere immediatamente a completa disposizione della Fondazione qualsiasi risorsa assegnata, incluse le dotazioni informatiche fisiche e tutte le informazioni di interesse aziendale in suo possesso:

- **Divieto di cancellazione dei dati:** L'utente non può in alcun modo cancellare, sovrascrivere o distruggere le informazioni, i file, i documenti o i registri informatici di interesse aziendale presenti sulle postazioni di lavoro e/o sulla rete aziendale, senza l'esplicita autorizzazione scritta del Responsabile del Servizio di appartenenza.
- **Chiusura delle caselle di posta elettronica:** La casella di posta elettronica individuale sarà mantenuta attiva esclusivamente per il tempo strettamente necessario a gestire il passaggio di consegne e concludere eventuali contatti di lavoro aperti. Successivamente, l'account viene disattivato e viene impostato un messaggio di risposta automatica di sistema ("casella non attiva") che rifiuta i nuovi messaggi in entrata e indirizza i mittenti verso i nuovi riferimenti operativi della Fondazione.
- **Rimozione dati extra-aziendali:** Qualora l'utente abbia lasciato sulle postazioni di lavoro o sulla rete informazioni di interesse strettamente personale e non aziendale, le stesse verranno rimosse e cancellate definitivamente dai tecnici della Fondazione all'atto della chiusura del profilo, senza alcuna responsabilità di conservazione a carico dell'ente.

5.7 Approvazione, efficacia e piani di formazione

Il presente testo unificato costituisce parte integrante del Modello di Organizzazione, Gestione e Controllo ai sensi del Decreto Legislativo 231/2001 e del Sistema di Protezione dei Dati attuato in adempimento alle norme vigenti. Qualsiasi modifica, integrazione o aggiornamento del presente regolamento può essere adottato esclusivamente attraverso una specifica delibera formale da parte del Consiglio Generale di Indirizzo, previo parere dell'Organismo di Vigilanza (OdV).

Il Codice è costantemente pubblicato e consultabile sulla rete informatica interna aziendale ed è consegnato formalmente al personale dipendente e ai collaboratori esterni al momento dell'assunzione in servizio o dell'avvio della collaborazione. I piani di formazione obbligatoria del personale sulle materie della sicurezza informatica e della protezione dei dati personali seguono le medesime scadenze, modalità di informazione e tracciamento previste per il Modello Organizzativo istituzionale.