REGOLAMENTO AZIENDALE PER L'UTILIZZO DELLE RISORSE E DEI SERVIZI ICT/TLC

U.O.C. SISTEMI INFORMATIVI

UNITED ACCREDITATION FOUNDATION
ISO 27001:2022 Certified
n. 241217053901

V.4.00 – febbraio 2025

Sommario

Premessa

Premesso che l'utilizzo delle risorse e dei servizi informatici e telematici deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito dei rapporti di lavoro, l'Azienda Ospedaliera "S. Giuseppe Moscati" (di seguito AO) adotta il presente Regolamento interno, a far data dall'atto di approvazione, con la finalità di definire i criteri di buon uso delle risorse e dei servizi ICT/TLC, allo scopo di tutelare l'integrità degli asset aziendali e massimizzarne l'efficienza e l'efficacia.

L'Azienda Ospedaliera 'S. Giuseppe Moscati' si impegna a garantire un elevato livello di sicurezza informatica e protezione delle infrastrutture critiche, in conformità con le normative internazionali ed europee. In particolare, l'azienda adotta le best practices di sicurezza informatica stabilite dalla norma ISO/IEC 27001:2022 (avendo ottenuto la certificazione ISO/IEC 27001:2022 per il Sistema di Gestione della Sicurezza delle Informazioni – ISMS – dei Sistemi Informativi Aziendali, https://www.iafcertsearch.org/certified-entity/cLZpdGl3LwirU4qxgYz30AUq) e rispetta le disposizioni della Direttiva UE 2022/2555 (NIS 2). Questi standard e direttive forniscono un quadro normativo completo per la gestione della sicurezza delle informazioni, assicurando la protezione dei dati sensibili e la continuità operativa. L'Azienda Ospedaliera "S. Giuseppe Moscati" è impegnata a mantenere la conformità a queste normative attraverso l'implementazione di misure tecniche e organizzative adeguate, la formazione continua del personale e la collaborazione con le autorità competenti.

Il presente regolamento vuole essere un agile strumento di supporto agli utenti del Sistema Informativo Aziendale nell'utilizzo dei servizi resi dall'U.O.C. Sistemi Informativi, nel rispetto delle sopracitate normative.

Si rimanda alle disposizioni di legge e regolamentari per tutto ciò che concerne le prescrizioni in materia di GDPR.

1. Normativa di riferimento

Di seguito i principali rimandi normativi di riferimento nella stesura del presente Regolamento:

- D.Lgs. n.196/2003 – *"Codice in materia di protezione dei dati personali"*
- D.Lgs. n.82/2005 – *"Codice dell'amministrazione digitale"*
- Deliberazione del Garante per la Protezione dei Dati personali n.13 del 1/3/2007 – *"Lavoro: le linee guida del Garante per posta elettronica e internet"*
- Direttiva n. 2/2009 della Presidenza del Consiglio dei ministri – *"Utilizzo di Internet e della casella di posta elettronica istituzionale sul luogo di lavoro"*
- Regolamento U.E. n.679/2016 – *"General Data Protection Regulation"*
- D.lgs 101/2018 – *"Adeguamento al Regolamento UE 2016/679"*
- Provvedimento del Garante per la Protezione dei Dati personali del 13/10/08 – *"Rifiuti di apparecchiature elettriche ed elettroniche (Raae) e misure di sicurezza dei dati personali"*
- Circolare AgID n° 1/2017 – *"Misure minime di sicurezza ICT per le pubbliche amministrazioni"*
- Regolamento U.E. n.2017/745 relativo ai dispositivi medici
- Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio del 14/12/2022 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione - "*Direttiva NIS 2*"
- Decreto legislativo n.138 – Recepimento direttiva UE 2022/2555 (NIS2)
- ISO/IEC 27001:2022 - *Information security management systems*

In allegato, con riferimento alla certificazione ISO27001:2022:

1) Politica per la sicurezza delle informazioni
2) Elencazione del corpus documentale (procedure, registri, politiche, piani, etc.) di certificazione ISO27001:2022 (i documenti elencati sono visionabili presso l'U.O.C. Sistemi Informativi, secondo i privilegi di accesso riportati a margine)

2. Ambito e destinatari

Il presente regolamento disciplina le modalità di utilizzo ed ingaggio delle risorse e dei servizi informatici e di telecomunicazione aziendali e si applica ai dipendenti e collaboratori dell'A.O. San Giuseppe Moscati di Avellino a vario titolo autorizzati all'accesso e all'utilizzo del Sistema Informativo Aziendale, nonché agli utilizzatori esterni (es.: cittadini, pazienti) aventi titolo all'accesso alle risorse informatiche ad essi destinate: nel seguito si farà riferimento ai primi con i termini "dipendenti", "utenti" o "utenti interni", ai secondi con il termine "utenti esterni"

3. Risorse informatiche

Con il termine risorse informatiche si intendono tutte le risorse fisiche e logiche (hardware, pc, server, apparati di rete, dispositivi di telecomunicazione, telefoni, numerazioni telefoniche, software di base, software applicativo, etc.) che costituiscono il Sistema Informativo Aziendale, come insieme dei servizi di raccolta, gestione automatizzata e condivisione delle informazioni di supporto ai processi aziendali.

Premesso che l'U.O.C. Sistemi Informativi non ha, tra le proprie attribuzioni, l'acquisizione di beni e servizi, le richieste in tal senso vanno indirizzate all'U.O.C. Acquisizione Beni e Servizi che predispone gli atti di gara sulla base di relazioni, istruttorie e capitolati redatti e sottoscritti dall'U.O.C. Sistemi Informativi, per quanto di competenza.

La riassegnazione di risorse informatiche è richiesta dal Direttore o Dirigente responsabile dell'U.O./Dipartimento ed approvata dalla Direzione di competenza (Amministrativa o Sanitaria).

Le risorse informatiche insistono sul centro di costo di assegnazione.

SI precisa che l'individuazione dei diritti di accesso ai sistemi informativi non rientra nelle attribuzioni tecniche dell'U.O.C. Sistemi Informativi e, richiamata la normativa in materia, è autorizzata dal Direttore o Responsabile dell'Unità Operativa di competenza ovvero dal Direttore Sanitario o dal Direttore Amministrativo nel caso in cui l'autorizzazione sia pertinente ad area di competenza differente da quella afferente alla struttura richiedente: l'U.O.C. Sistemi Informativi individua il profilo di accesso sulla base delle autorizzazioni consentite come innanzi detto.

L'U.O.C. Sistemi Informativi esercita, nell'ambito delle attribuzioni proprie, la funzione di monitoraggio dei livelli di performance e sicurezza del sistema ICT/TLC nel suo complesso; pertanto, è necessaria la sua preventiva validazione tecnica in caso di:

- connessione di dispositivi, comunque acquisiti, alla rete dati aziendale
- installazione di software
- accesso a servizi informativi e/o applicativo/gestionali
- attivazione, comunque acquisita, di ogni altro servizio o sistema per il trattamento automatico dell'informazione

L'U.O.C. Sistemi informativi, infine, è responsabile dell'implementazione delle best practices di sicurezza informatica necessarie per garantire l'efficienza operativa del sistema ICT/TLC dell'organizzazione, nel

rispetto della normativa vigente. Questo implica, inter alia, la definizione e implementazione di un adeguato processo di patch management e di aggiornamento del software. Per ulteriori informazioni si faccia riferimento al documento *"PR23 Procedura di change & patch management"*.

3.1. Accesso al sistema informativo

Di regola, l'accesso dei dipendenti al sistema informativo aziendale, inteso come l'insieme dei programmi e servizi software destinati alla gestione dei processi aziendali, è consentito entro il perimetro fisico dei plessi dell'AO, fatti salvi i servizi disponibili in intranet / extranet su protocollo https; eventuali ulteriori accessi destinati all'utilizzo da parte del personale dipendente e/o dei collaboratori, possono essere consentiti esclusivamente previa autorizzazione del Direttore dell'U.O.C. di competenza ed esclusivamente attraverso l'utilizzo di Oplon Secure Access. Inoltre, l'accesso remoto al sistema informativo aziendale richiede l'autenticazione a due fattori (2FA) per verificare l'identità degli utenti che accedono da remoto, riducendo il rischio di accessi non autorizzati.

La normalizzazione della situazione pregressa è nelle attribuzioni dell'U.O.C. Sistemi Informativi.

Gli accessi remoti di natura tecnica di diretta pertinenza dell'U.O.C. Sistemi Informativi (es. ditte manutentrici del software) sono gestiti in autonomia dall'U.O.C. medesima, nel rispetto della vigente normativa; gli accessi remoti di natura tecnica di pertinenza di altri servizi (es. ditte manutentrici di elettromedicali) sono autorizzati dall'U.O.C. Sistemi Informativi su richiesta protocollata del Direttore dell'U.O. di competenza (U.O.C. Ufficio tecnico o UU.OO. su cui insistono i sistemi cui accedere), secondo le prescrizioni di legge. In entrambi i casi, per garantire il rispetto della normativa vigente, gli accessi remoti da parte di aziende fornitrici avvengono previo collegamento in VPN LanToLan (IPSec) e, nel caso in cui, per motivazioni comprovate, l'azienda fornitrice sia impossibilitata alla configurazione di una VPN IpSec, l'U.O.C. provvederà a fornire accesso in VPN ClientToLan fino ad un massimo di cinque licenze con autenticazione a due fattori garantita (utilizzo di token via app su telefono).

Il primo livello di autenticazione per l'accesso dei dipendenti alle risorse del sistema informativo aziendale è costituito dalle credenziali di accesso al pc che identificano univocamente l'utente, nel formato *nome.cognome@aornmoscati.it*.

Per pc utilizzati normalmente da gruppi di utenti per il solo utilizzo delle procedure informatiche aziendali (ad es. i pc di reparto da cui si accede al sistema informativo sanitario) sono previsti account di reparto (nel formato *acronimoreparto@aornmoscati.it*); tali account consentono il mero accesso al pc: ogni ulteriore funzionalità è presidiata da un successivo livello di autenticazione, di carattere individuale, opportunamente profilato secondo il ruolo del dipendente.

All'atto dell'immissione in servizio, successivamente all'assegnazione del numero di matricola e dell'ufficio o reparto di destinazione, l'U.O.C. Gestione Risorse Umane invia a mezzo protocollo informatico, a firma del Direttore dell'U.O.C. in parola o di un funzionario incaricato, la richiesta di accesso ai servizi informatici di base, compilata sulla piattaforma aziendale di gestione dei flussi documentali (amministrazione.aornmoscati.it, link *"DgsWebOS"*).

Per i casi non previsti al capoverso precedente, la richiesta, come innanzi emarginata, dovrà pervenire dal Direttore / Dirigente responsabile, con le medesime modalità.

All'utente vengono assegnate le credenziali per l'accesso a:

- personal computer
- posta elettronica ordinaria
- servizi intranet al dipendente
- programmi software di competenza

tutte le credenziali assegnate vengono comunicate all'utente tramite la mail indicata dal medesimo, nel rispetto della normativa GDPR e norme collegate; l'attivazione delle credenziali avviene tramite la procedura di reimpostazione password a cura esclusiva dell'utente.

La richiesta di accesso a servizi informativi aggiuntivi è presentata dal Direttore dell'U.O. di appartenenza del dipendente tramite l'utilizzo della piattaforma aziendale di gestione dei flussi documentali (amministrazione.aornmoscati.it, link *"DgsWebOS"*); è possibile richiedere:

- PEC ulteriore rispetto a quella di struttura (è richiesta l'autorizzazione del Direttore Amministrativo o Sanitario, secondo competenza)
- accesso ad internet
- firma digitale per il dipendente (per i medici: la firma è assegnata senza preventiva richiesta; per gli altri dipendenti: se il dipendente non è un Direttore o Dirigente Responsabile di Struttura, è richiesta l'autorizzazione del Direttore Amministrativo o Sanitario, secondo competenza)
- accesso al sito web bloccati (è richiesta l'autorizzazione solo del Direttore di Struttura)
- abilitazione al Sistema Tessera Sanitaria (è richiesta l'autorizzazione solo del Direttore di Struttura)
- abilitazione a procedure le quali non è possibile assegnare l'accesso in fase di immissione in servizio del dipendente (ad es.: trasferimento del dipendente, ulteriori assegnazioni, profili a sistema legati a specifiche mansioni assegnate dal Direttore dell'U.O. di appartenenza, etc.); è richiesta l'autorizzazione solo del Direttore di Struttura

È responsabilità del Direttore di Struttura chiedere la revoca degli accessi di cui innanzi è detto, qualora non sussistano più le condizioni per cui sono stati assegnati (es.: cessazione dal servizio, trasferimento, passaggio ad altre mansioni, etc.).

Quanto definito nel presente paragrafo è approfondito nell'apposita procedura relativa al controllo degli accessi fisici e logici (rif. PR14 Controllo degli accessi fisici e logici).

Al momento della stesura di questo regolamento, ciascun sistema richiede il proprio account di accesso; è in fase di completamento l'unificazione degli account mediante un sistema di Single-sign-on.

3.2. Modifiche di dati e di programmi

3.2.1. Modifiche di dati

L'U.O.C. Sistemi Informativi non interviene nella gestione ordinaria di tipo "data entry" (modifica / inserimento / cancellazione) dei dati di competenza di altre strutture: la gestione dei dati è nell'attribuzione dell'U.O. che ne è responsabile.

Eventuali richieste, ad es. di creazione di centri di costo e/o creazione di nuove strutture, nel rispetto dell'Atto Aziendale vigente, non vanno indirizzate all'U.O.C. Sistemi Informativi ma alla Direzione Strategica, che provvede per il tramite delle strutture preposte (es. Controllo di Gestione) con il supporto, eventuale, della ditta manutentrice, nei limiti di quanto innanzi è detto.

In caso di creazione / modifica / cancellazione di centri di costo e/o strutture in applicazione dell'Atto Aziendale vigente, le UU.OO. competenti (es. Controllo di Gestione, DMP) devono darne comunicazione all'U.O.C. Sistemi Informativi che provvede all'aggiornamento dei sistemi tecnici (es. Active Directory).

In caso di mobilità, cessazione, immissione in servizio di dipendenti, le UU.OO.CC. Gestione Risorse Umane e DMP ne danno comunicazione all'U.O.C. Sistemi Informativi che provvede all'aggiornamento dei sistemi tecnici (es. Active Directory, posta elettronica, etc.).

3.2.2. Modifiche di programmi

Salva l'applicazione di disposizioni/deliberazioni della Direzione Strategica o diversi accordi intervenuti con l'U.O.C. Sistemi Informativi, le richieste di modifiche o di analisi (anche preliminare) relative ai programmi software gestionali non vanno indirizzate alle ditte manutentrici ma all'U.O.C. Sistemi Informativi che, fatte le opportune valutazioni tecniche, le sottopone, secondo competenza, alla Direzione Amministrativa o alla Direzione Sanitaria (o, per delega della Direzione Sanitaria, all'U.O.C. Direzione Medica di Presidio) per autorizzazione; in caso di riscontro assertivo, l'U.O.C. Sistemi Informativi interviene per l'eventuale implementazione.

3.2.3 Audit e monitoraggio delle modifiche

Le modifiche ai dati e ai programmi devono essere controllate mediante l'implementazione di un processo di audit e monitoraggio continuo, nel rispetto della normativa vigente (Direttiva (UE) 2022/2555 (NIS 2)). Questo processo prevede la registrazione dettagliata di tutte le modifiche apportate ai dati e ai programmi, inclusi chi ha effettuato la modifica, quando è stata effettuata e quale è stata la natura della modifica. L'audit continuo consente di tracciare e verificare tutte le attività, garantendo la trasparenza e l'integrità dei dati. Il monitoraggio continuo, invece, permette di rilevare tempestivamente eventuali anomalie o attività sospette, facilitando una risposta rapida e appropriata agli incidenti di sicurezza.

L'implementazione di tali misure è a carico dell'U.O.C. Sistemi Informativi.

3.3. Gestione dell'account

3.3.1. Accesso al pc, ad intranet e ad internet

Ogni utente interno ha un account sul dominio aziendale di Active Directory; tale credenziale consente l'accesso a tutte le risorse cui l'utente è abilitato, ad es.:

- qualunque pc aziendale connesso al dominio
- internet
- intranet (compresi i servizi al dipendente, es. cedolino)
- programmi applicativi

questa password è soggetta a scadenza periodica di 90 giorni; alla scadenza è possibile cambiarla accedendo ad un pc a dominio con le credenziali aziendali oppure accedendo ad intranet (*intranet.aornmoscati.it*) con le stesse credenziali ed attivando la procedura di *"recupera password".* Tale procedura invia un SMS sul cellulare comunicato dal dipendente (al momento dell'assunzione o inserito, anche successivamente, nella propria area del portale del dipendente).

In nessun caso è possibile la reimpostazione della password per contatto telefonico a voce o per conto di terzi.

La gestione delle credenziali individuali (*nome.cognome@aornmoscati.it* [1]) è nella responsabilità dell'assegnatario ed è conforme alle regole di compliance al GDPR (es. scadenza, lunghezza, complessità, etc.).

Le credenziali di reparto si rendono necessarie per consentire l'accesso al sistema informativo aziendale sanitario da postazioni di lavoro ad utilizzo non individuale; esse vengono fornite in maniera non modificabile dall'utente e consentono il mero accesso al pc, nel rispetto della normativa GDPR e collegati. L'utilizzo di ogni altro sistema o servizio richiede un successivo livello di autenticazione individuale.

Qualunque accesso non utilizzato per più di 180 giorni viene automaticamente disabilitato. È, in ogni caso possibile riattivare l'accesso, ove ricorrano i presupposti di fatto e di diritto, attraverso il sistema di help desk descritto nel presente regolamento.

Ulteriori informazioni relative alla corretta gestione delle password sono consultabili nella relativa procedura (rif. *"PR15 Criteri Password"*).

3.3.2. Accesso alle procedure gestionali

La reimpostazione della password su qualsiasi procedura informatica aziendale è possibile attraverso l'opzione di recupero password che invia un SMS sul cellulare del dipendente (da inserire nella propria area del portale del dipendente).

3.4. Accessi dall'esterno della rete aziendale

L'accesso degli utenti alle risorse informatiche ed informative aziendali dall'esterno della rete aziendale è consentito esclusivamente tramite connessione Oplon Secure Access / Zero Trust Network (Oplon), ad eccezione dei servizi disponibili su protocollo https per il cittadino e per il dipendente.

L'accesso via Oplon, da richiedere tramite la piattaforma di gestione dei flussi documentali (amministrazione.aornmoscati.it, link *"DgsWebOS"*), nel rispetto della normativa vigente, è subordinato ad un sistema di autenticazione a due fattori costituito dalle credenziali rilasciate in fase di registrazione alla piattaforma "Oplon" ed integrato con l'app che l'utente installa sul proprio smartphone. Al momento della stesura del presente Regolamento è in corso di estensione l'applicazione del secondo fattore di autenticazione (codice OTP / token) anche all'accesso di tutti i sistemi ed applicativi aziendali.

L'utente che accede via Oplon deve utilizzare, sotto la sua responsabilità, dispositivi (pc o altro) che siano conformi ai requisiti di sicurezza individuati dall'U.O. Sistemi Informativi;

L'accesso via Oplon è assegnato all'avente diritto a mezzo di credenziali nominative del tipo *nome.cognome@aornmoscati.it* che lo identificano.

3.5. Postazioni di lavoro

La consegna dell'hardware e la relativa presa in carico avviene con una scheda di consegna numerata e datata che viene firmata dal dipendente cui l'hardware è assegnato o dal responsabile del gruppo (es. responsabile

[1] Le omonimie vengono gestite con le lettere inziali del nome

dell'ufficio, CPSE, Direttore U.O., etc.), se l'hardware è assegnato ad un gruppo di dipendenti (es. pc di reparto).

Se il dipendente viene trasferito ad altro ufficio o unità o incarico, l'hardware assegnato non segue il dipendente (salvo accordo tra uffici o unità e con il consenso dell'U.O.C. Sistemi Informativi), ma rimane in carico alla Funzione d'origine, a coprire la finalità per cui è stato assegnato, o, se non più necessario, viene restituito all'U.O.C. Sistemi Informativi, accompagnato da relativa scheda di ritiro.

Nel caso in cui il personal computer debba essere fisicamente trasferito ad altra collocazione, anche in capo allo stesso ufficio o allo stesso dipendente, è necessario informare l'U.O.C. Sistemi Informativi (mediante compilazione di apposito modulo), che provvederà alle eventuali verifiche relativamente all'infrastruttura ICT/TLC, all'abilitazione del nuovo punto rete ed alla verifica della corretta connessione; ai fini del trasloco fisico delle apparecchiature l'U.O.C. Sistemi Informativi potrà chiedere il supporto della ditta incaricata del facchinaggio (in caso di spostamenti massivi).

La sostituzione dell'hardware avviene, secondo le risorse disponibili, esclusivamente previa validazione tecnica dell'U.O.C. Sistemi Informativi che deve accertare lo stato di funzionamento del dispositivo e l'effettiva impossibilità di ripristino.

Al fine di garantire la stabilità e la sicurezza delle postazioni di lavoro, gli account utente sono configurati con diritti limitati. Tra le principali funzionalità non consentite all'utente:

- installare software sul pc
- modificare il registro di sistema
- installare periferiche attive
- modificare le impostazioni di data e ora
- modificare le impostazioni dei software di sicurezza
- utilizzare software di controllo remoto
- utilizzare le porte usb (salvo casi particolari da definire volta per volta)
- utilizzare piattaforme pubbliche di condivisione files

non è consentita l'abilitazione delle funzionalità di cui al precedente elenco, pena il detrimento della disponibilità, dell'affidabilità e della sicurezza delle risorse informatiche a supporto dell'attività lavorativa.

Con particolare riferimento alla disabilitazione delle porte usb, per lo scambio di files è possibile utilizzare:

1) per scambio di files anche con l'esterno:
    a. posta elettronica (aornmoscati.it)
    b. pec (pec.aornmoscati.it)
    c. area personale intranet
    d. file sharing (MS OneDrive aziendale, attivabile a richiesta del Direttore U.O.C.)
2) solo per condivisione interna:
    a. cartelle condivise sul file server aziendale
3) eventuali richieste di abilitazione di porte USB, per specifiche e comprovate motivazioni, dovranno essere autorizzate formalmente dal Direttore dell'U.O.C. di appartenenza e saranno valutate dall'U.O.C. Sistemi Informativi per l'abilitazione di uno specifico dispositivo usb (preventivamente controllato dall'U.O.C. Sistemi Informativi) allo specifico utente ed alla specifica porta USB del pc aziendale (la porta USB sarà attiva solo per quel dispositivo USB, solo per quell'utente e solo su quel pc).

Lo scambio di file M2M è gestito caso per caso, secondo specificità.

Al fine del salvataggio dei dati (ad es. di tipo Word o Excel) e della condivisione per l'Unità Operativa, sono disponibili aree di archiviazione apposite, per ciascun utente e per ciascuna Unità Operativa: alle prime può accedere esclusivamente il singolo utente, alle seconde tutti gli utenti afferenti alla medesima Unità, con livelli di autorizzazione paritetici. Tali aree risiedono su server collocati nel data center aziendale e perimetrati con gli stessi livelli di sicurezza fisica e logica di tutta la componente server dell'infrastruttura ICT (backup, controllo accessi, UPS, gruppo elettrogeno, antiincendio, antiallagamento, videosorveglianza, etc.). Su ciascun pc nelle *"risorse del computer"* è accessibile il collegamento per ciascuna area, personale e di Unità. È a cura dell'utente l'utilizzo di tali aree.

Con le stesse modalità è possibile assegnare la condivisione di aree tra più UU.OO., a richiesta dei Responsabili delle medesime.

Non è consentita la condivisione di cartelle tra postazioni desktop ma solo tra file server e pc, come sopra descritto.

Sono in carico all'utente il salvataggio dei dati eventualmente residenti sui pc (Word, Excel, etc.), ancorché utilizzati per esigenze di lavoro, il loro recupero a seguito di guasto, il loro trasferimento ad altro supporto o pc; in caso di perdita di tali dati, l'U.O.C. Sistemi Informativi potrà tentarne il recupero in modalità best effort, senza garanzia di tempi o di soluzione.

In caso di sostituzione del pc, l'U.O.C. Sistemi Informativi comunica all'utente o al Direttore / Dirigente Responsabile dell'U.O. il calendario di intervento, concordandone, se possibile, la data; il trasferimento alla nuova unità degli eventuali dati documentali (Word, Excel, etc.) residenti sul pc da sostituire è nella responsabilità dell'utente e non può, in nessun caso, costituire motivazione ostativa all'intervento di sostituzione.

Il personal computer, in quanto strumento funzionale all'attività lavorativa, non può ospitare dati di natura personale né essere strumentale ad attività non collegate alle mansioni ed ai compiti assegnati.

Le risorse informatiche assegnate (pc, periferiche, etc.) devono essere custodite con cura prevenendo ogni possibile forma di danneggiamento.

In caso di deterioramento delle risorse hardware riconducibili, a insindacabile giudizio dell'U.O.C. Sistemi Informativi, a colpa o dolo, gli eventuali costi di riparazione e/o sostituzione insisteranno sul budget dell'U.O. assegnataria. In caso di necessità di smaltimento di una parte o della totalità della risorsa deteriorata è necessario attivare il processo di distruzione in conformità con la procedura smaltimento e distruzione dei dispositivi (rif. PR06 Procedura smaltimento e distruzione dispositivi).

In nessun caso è consentito l'uso di programmi diversi da quelli ufficialmente installati dall'Azienda tramite l'U.O.C. Sistemi Informativi, ne è consentito agli utenti di installare autonomamente programmi software; l'U.O.C. Sistemi Informativi adotta tutte le soluzioni tecniche necessarie a prevenire l'installazione autonoma di software da parte degli utenti e l'uso di programmi non ufficialmente installati.

L'U.O.C. Sistemi Informativi adotta ogni utile sistema di monitoraggio e controllo attivo finalizzato a prevenire il collegamento alla rete aziendale di dispositivi non preventivamente autorizzati, fatti salvi i servizi di accesso al pubblico entro sezioni logiche presidiate della rete dati.

Ulteriori informazioni utili ad una corretta gestione delle postazioni di lavoro sono consultabili nel documento *"PR22 Politica di clear desk and clear screen"*.

3.6. Dispositivi medici

L'Operation Technology (e, con essa, la gestione dei dispositivi medici) rientra tra le attribuzioni dell'U.O.C. Tecnico – Patrimonio – Ingegneria Clinica; l'U.O.C. Sistemi Informativi, che ha in capo l'Information Technology, si occupa dell'integrazione dei dispositivi OT/IoT/IoMT nell'ambito del sistema informativo aziendale e dell'infrastruttura di rete e collabora con l'U.O.C. Tecnico – Patrimonio – Ingegneria Clinica per quanto di competenza.

In caso di dispositivi medici collegati a pc gestiti dall'U.O.C. Sistemi Informativi, tale è la distinzione delle attribuzioni:

1) il dispositivo medico, compreso il pc direttamente collegato (etichetta bianca), è nella responsabilità del Servizio di Ingegneria Clinica
2) il pc gestionale (etichetta gialla) che, tramite il software gestionale, acquisisce i dati dal dispositivo medico, è nella responsabilità dell'U.O.C. Sistemi Informativi
3) la connessione tra i due è nella responsabilità dell'U.O.C. Sistemi Informativi: le ditte manutentrici del dispositivo garantiscono l'adattamento del connettore del dispositivo rispetto al connettore del pc gestito dall'U.O.C. Sistemi Informativi

I pc di ingegneria clinica, come detto, sono identificati dall'etichetta bianca e non sono a dominio; i pc dell'U.O.C. Sistemi Informativi hanno l'etichetta gialla e sono a dominio.

L'U.O.C. Sistemi Informativi propone al Servizio di Ingegneria Clinica i requisiti di sicurezza informatica che i dispositivi in rete devono soddisfare.

Problematiche attinenti ai dispositivi medici vanno instradate verso il Servizio di Ingegneria Clinica; nel caso in cui venissero, per errore, sottoposte al servizio di Help Desk informatico, di cui al cap.8, queste verranno trasferite al servizio di Ingegneria Clinica, ferma la collaborazione alla soluzione, per quanto, come detto, di competenza.

4. Internet

L'accesso ad internet avviene esclusivamente a mezzo delle credenziali individuali ed è assegnato all'utente per motivate esigenze lavorative, su richiesta del Direttore dell'U.O.C. di appartenenza, inoltrata all'U.O.C. Sistemi Informativi, che provvede a configurare opportunamente il profilo dell'account utente nell'ambito del servizio di Directory Aziendale.

La revoca dell'accesso ad internet può avvenire d'ufficio, ad es. per cessazione del rapporto di lavoro, ovvero su richiesta motivata del Direttore dell'U.O.C. di assegnazione del dipendente.

Al fine di prevenire il rischio di utilizzi impropri della rete, l'Azienda utilizza un sistema di filtri che impediscono l'accesso diretto a siti che non hanno natura istituzionale (black list). La black list è preconfigurata dai sistemi di sicurezza automatici; salve le esigenze di tutela della sicurezza ed integrità dei sistemi, individuate dall'U.O.C. Sistemi Informativi, la black list è modificabile, individualmente o per gruppi di dipendenti, su richiesta del Direttore dell'U.O., autorizzata dal Direttore Sanitario o Amministrativo, secondo competenza.

Laddove, per motivi strettamente collegati all'attività lavorativa, fosse necessario l'accesso ad un sito che risultasse bloccato per evidente misconfiguration (ad es. per errata categorizzazione del sito), l'U.O.C. Sistemi Informativi provvederà, d'ufficio, all'eventuale sblocco dell'accesso su richiesta motivata del direttore dell'U.O.C. segnalante.

L'utente è direttamente responsabile dell'uso del servizio di accesso a Internet, dei contenuti che ivi vi ricerca, dei siti che contatta, delle informazioni che vi immette e delle modalità con cui opera.

Salvi i servizi forniti dall'U.O.C. Sistemi Informativi, all'utente è interdetta la possibilità di:

- servirsi o dar modo ad altri di servirsi della stazione di accesso a internet per attività non istituzionali, per attività poste in essere in violazione del diritto d'autore o altri diritti tutelati dalla normativa vigente
- utilizzare sistemi Peer to Peer (P2P), di file sharing, podcasting, webcasting, messaging o similari, così come connettersi ai siti che trasmettono programmi streaming (come radio o TV via WEB)
- scaricare software dalla rete: eventuali necessità devono essere appositamente richieste all'U.O.C. Sistemi Informativi
- utilizzare metodi di connessione ad Internet difformi dal provider aziendale (ad esempio a mezzo di internet key personali)
- utilizzare anonimizzatori
- utilizzare servizi di remote desktop non validati dall'U.O.C. Sistemi Informativi

L'U.O.C. Sistemi Informativi adotta ogni utile soluzione tecnica atta ad impedire l'uso delle funzionalità innanzi elencate e di ogni altra attività collegata che possa costituire fattore di rischio per la sicurezza informatica; eventuali soluzioni informatiche utili al superamento, in sicurezza, di tali limitazioni verranno adottate previa valutazione dell'U.O.C. Sistemi Informativi.

5. Intranet

Intranet è l'insieme delle risorse e dei servizi informativi disponibili ai dipendenti con accesso autenticato su piattaforma web, all'indirizzo *intranet.aornmoscati.it* o sul portale *www.aornmoscati.it* al link *"Accesso: area dipendenti"*; l'accesso alla intranet è consentito sia dall'interno della rete aziendale che dall'esterno.

Oltre ai contenuti informativi dedicati ai dipendenti, sono disponibili in intranet i seguenti servizi (secondo i propri requisiti di autorizzazione):

- servizi al personale (cedolini e timbrature)
- rassegna stampa
- archivio albo pretorio
- rischio clinico
- regolamenti
- modulistica
- link alla mail aziendale
- link alla pec aziendale
- servizi applicativi, ad es.:
    - contabilità e magazzino
    - fascicolo del personale
    - sistema informativo ospedaliero
    - protocollo
    - gestione risorse umane

Sono disponibili, inoltre, i seguenti servizi di web collaboration di base, aperti anche ad utenti esterni, purché registrati a cura dell'U.O.C. Sistemi Informativi, su richiesta qualificata (Direzione Strategica, Direzione di Dipartimento / U.O.C. / U.O.S.D. / U.O.S.):

- Chat
- Drive
- Gestione collaborativa di gruppi di lavoro, attività, progetti e compiti

È disponibile anche la funzione di check-in / check-out, utilizzabile per la registrazione dell'ora di inizio e fine dell'attività in smartworking, salve le attribuzioni dell'U.O.C. Gestione Risorse Umane.

I servizi di web collaboration di cui è detto sono offerti su piattaforma aziendale, nel rispetto del Regolamento UE 679/2016; è inibito, all'interno della rete aziendale, l'utilizzo di analoghi strumenti ad accesso pubblico detenuti da soggetti terzi (es. social) non rientranti in specifica contrattualizzazione con l'Azienda, salvo esigenze eccezionali che verranno valutate di volta in volta dall'U.O.C. Sistemi Informativi.

Per i Direttori delle UU.OO., sono disponibili servizi evoluti di web collaboration nell'ambito della piattaforma Office365 aziendale cui l'utente può accedere tramite le credenziali aziendali (*nome.cognome@aornmoscati.it*).

6. WiFi

È attivo il Wi-Fi aziendale, per entrambi i plessi dell'Azienda; in particolare, sono disponibili i seguenti service set identifier (SSID):

- AORNMoscati-Azienda:
  consente l'utilizzo delle procedure informatiche aziendali (es. sistema informativo ospedaliero); si accede con le credenziali di Active Directory *nome.cognome* (quelle usate anche per l'accesso al pc e per i servizi intranet al dipendente)
- AORNMoscati-Guest:
  consente l'accesso ad internet per gli ospiti (es. professionisti di ditte esterne), ma non l'uso delle procedure informatiche aziendali (es. Sistema Informativo Ospedaliero); si fa richiesta dal captive portal di accesso. La richiesta è vagliata dall'U.O.C. Sistemi Informativi che, ove il caso occorra, concede credenziali valevoli per la durata richiesta
- AORNMoscati-Pazienti:
  consente l'uso di internet esclusivamente per i pazienti ricoverati per la durata del ricovero, secondo le indicazioni date dal captive portal al momento dell'accesso, con una sola connessione alla volta per paziente (il secondo accesso contemporaneo chiude la sessione precedente)
- AORNMoscati-Social:
  consente l'accesso ad internet nelle zone di attesa con account social (Google, Facebook, Twitter), valevoli fino al logout
- AORNMoscati-Dispositivi:
  consente l'accesso automatico ai dispositivi autorizzati (es. tablet, dispositivi medici, etc.)

L'accesso al wi-fi è, comunque, soggetto alle misure di sicurezza ed alle policies di gestione individuate dall'U.O.C. Sistemi Informativi, nel rispetto della normativa (in particolare in materia di GDPR) e dei regolamenti e disposizioni aziendali.

7. Posta elettronica

L'uso della posta elettronica è un preciso obbligo lavorativo del dipendente, in ossequio alla direttiva del 27/11/2003 della Presidenza del Consiglio, recante disposizioni circa *l'"impiego della posta elettronica nelle pubbliche amministrazioni"* che prescrive che *"le pubbliche amministrazioni provvedano a dotare tutti i*

dipendenti di una casella di posta elettronica … e ad attivare, inoltre, apposite caselle istituzionali" e che si deve "*procedere alla tempestiva lettura, almeno una volta al giorno"* della posta elettronica.

L'uso della posta elettronica, sia ordinaria che certificata, è consentito esclusivamente in relazione alle attività lavorative; il dipendente, pertanto dovrà astenersi dall'utilizzo della posta elettronica aziendale per scopi privati.

L'utente dovrà utilizzare, pertanto, la posta elettronica (non certificata) quale strumento di comunicazione ordinaria interaziendale, salvo l'uso del protocollo aziendale secondo le previsioni dell'apposito regolamento e della posta elettronica certificata, quest'ultima nei casi in cui rilevi l'esigenza di opponibilità a terzi (es. altre Amministrazioni o persone fisiche o giuridiche non afferenti all'Azienda) della comunicazione.

L'uso di caselle di posta elettronica non appartenenti al dominio di posta aziendale (del tipo, ad esempio, *nomeuo@gmail.com*) non è consentito in quanto espone l'Azienda a rischi di sicurezza informatica (ad es. non sono presidiate dai sistemi di sicurezza aziendali né sono conformi alle policies aziendali in materia), di inappropriatezza giuridico – amministrativa (ad es. non garantiscono in alcun modo l'identità del mittente), di censurabilità in materia di GDPR (ad es. possono essere di uso promiscuo personale / aziendale). Pertanto, l'accesso alle caselle di posta elettronica su dominio non aziendale non è supportato dall'U.O.C. Sistemi Informativi.

In caso di rischio per la sicurezza informatica, l'U.O.C. Sistemi Informativi può inibire, d'ufficio, l'accesso alla posta personale nell'ambito del perimetro logico della rete aziendale.

L'U.O.C. Sistemi Informativi non accede, né è legittimata a farlo, alle caselle di posta elettronica aziendale degli utenti; pertanto, costoro si devono astenere dal richiedere all'U.O.C. Sistemi Informativi qualunque attività manutentiva del contenuto (es. cancellazione messaggi, svuotamento, anche parziale della casella, salvataggio di messaggi, etc.).

La casella di posta elettronica aziendale dell'utente viene disabilita al momento della cessazione del rapporto; eventuali successivi accessi avvengono nel rispetto del GDPR e norme collegate. Si invitano i dipendenti a comunicare, all'U.O.C. Gestione Risorse Umane, un indirizzo di posta elettronica personale che possa essere utilizzato per comunicazioni postume al rapporto di lavoro (es. CUD dopo la cessazione).

7.1. Posta elettronica ordinaria

A ciascun dipendente è assegnato un indirizzo di posta elettronica aziendale nel formato *nome.cognome@aornmoscati.it*; parimenti, ad ogni U.O., Dipartimento o Direzione è assegnato un indirizzo nel formato *uo.descrizione@aornmoscati.it* ovvero *dipartimento.descrizione@aornmoscati.it* ovvero *direzione.descrizione@aomoscati.it*, la cui gestione è nella responsabilità del Direttore di competenza.

L'U.O.C. Sistemi Informativi provvede a verificare l'assegnazione della posta elettronica ordinaria secondo quanto innanzi è detto ed a disattivare le caselle e-mail difformi, fatte salve eventuali specificità, segnalate dal Direttore dell'U.O. di competenza ed autorizzate dal Direttore Sanitario o dal Direttore Amministrativo, secondo competenza.

La posta elettronica ordinaria aziendale, in quanto assegnata individualmente al dipendente e protetta da un sistema di identificazione ed autenticazione, individua univocamente il mittente ed il destinatario del messaggio all'interno dell'azienda e, pertanto, costituisce efficace ed esaustivo strumento di comunicazione intraziendale, attesi gli obblighi in capo al dipendente di cui è detto in premessa al presente paragrafo e fatta salva ogni ulteriore previsione di cui al presente regolamento ovvero sovraordinata disposizione.

Per le stesse motivazioni, non potranno essere prese in carico comunicazioni pervenute a mezzo mail personale.

È di fondamentale importanza che l'utente inserisca, nella propria area del portale del dipendente, il numero di telefono cellulare per l'operazione di recupero password in mancanza, in caso di necessità, non sarà possibile accedere né alla mail aziendale, né al pc con l'account individuale, né ai servizi intranet (es. visualizzazione cedolino).

7.2. PEC

Per ciascun servizio sono pubblicati nell'Indice PA (Indice delle Pubbliche Amministrazioni e delle Aree Organizzative Omogenee, istituito con DPCM del 31 ottobre 2000) gli indirizzi delle caselle di Posta Elettronica Certificata (PEC) che consentono l'interoperabilità tra le PP.AA. e l'Azienda.

L'indice PA costituisce, pertanto, il riferimento di individuazione e la porta d'accesso alle strutture organizzative ed ai servizi telematici offerti dall'Azienda.

Pertanto, le caselle di posta elettronica certificate non vengono assegnate nominalmente ai dipendenti ma alle UU.OO.; le relative credenziali, con password OTP, sono consegnate al Direttore o Dirigente Responsabile o suo collaboratore formalmente delegato, che ne assume la responsabilità.

La PEC è destinata ai fini esclusivi di opponibilità a terzi della comunicazione intrattenuta con soggetti esterni all'Azienda; non costituisce elemento di comunicazione ordinaria tra uffici né informale né formale, dovendosi utilizzare, all'uopo, la posta elettronica aziendale ordinaria e il protocollo informatico, ove necessario, nei termini dell'apposito regolamento di protocollo.

L'assegnazione e revoca delle caselle di PEC ai servizi individuati è attribuzione del Direttore Amministrativo o del Direttore Sanitario, per competenza, tramite l'U.O.C. Sistemi Informativi, secondo la macrostruttura organizzativa dell'Azienda, individuata gerarchicamente con atto del Direttore Generale.

Eventuali modifiche all'assetto organizzativo dell'Azienda potranno determinare modifiche nell'elenco delle strutture aventi caselle di PEC con eventuale revoca e/o nuova attribuzione.

Ogni Servizio abilitato avrà una casella di PEC che lo individua.

L'U.O.C. Sistemi Informativi provvede a verificare l'assegnazione della PEC secondo quanto innanzi è detto ed a disattivare le caselle PEC difformi, fatte salve eventuali specificità, segnalate dal Direttore dell'U.O. di competenza ed autorizzate dal Direttore Sanitario o dal Direttore Amministrativo, secondo competenza.

L'U.O.C. Sistemi Informativi, a seguito di comunicazione del Direttore Generale, o del Direttore Amministrativo o del Direttore Sanitario, provvede alla revoca della PEC qualora non sussistano più i presupposti di fatto e di diritto che ne hanno determinato la concessione.

L'U.O.C. Sistemi Informativi gestisce il registro delle PEC concesse e provvede al rinnovo di quelle in scadenza, ove ne sussistano le condizioni.

L'U.O.C. Sistemi Informativi normalizza la situazione esistente, in materia di PEC, secondo le prescrizioni del presente Regolamento, attestando, inoltre, le pec, sul dominio *pec.aornmoscati.it*

8. Firma digitale

È assegnato il sistema di firma digitale a:

- Direttore Generale, Sanitario e Amministrativo
- Direttori di Dipartimento
- Direttori UU.OO.
- Dirigenti
- personale non medico abilitato (ad es. in connessione alle funzionalità della cartella clinica)
- altro personale individuato dal Direttore Amministrativo o Sanitario nell'ambito delle rispettive competenze

L'U.O.C. Sistemi Informativi provvede a verificare l'assegnazione della firma digitale secondo quanto innanzi è detto ed a disattivare le firme digitali difformi, fatte salve eventuali specificità, segnalate dal Direttore dell'U.O. di appartenenza del dipendente ed autorizzate dal Direttore Sanitario o dal Direttore Amministrativo, secondo competenza.

Il titolare della firma digitale è tenuto ad informare immediatamente l'U.O.C. Sistemi Informativi di ogni circostanza che renda necessaria o comunque opportuna la revoca o la sospensione del certificato e dell'eventuale dispositivo di firma assegnati; deve altresì informare tempestivamente l'U.O.C. Sistemi Informativi di eventuali richieste di revoca o di sospensione che egli, per necessità o urgenza, abbia inoltrato direttamente al Certificatore.

La firma digitale è utilizzata per la sottoscrizione di documenti informatici esclusivamente nell'ambito delle attività istituzionali dei soggetti abilitati e nel rispetto dei poteri di firma derivanti dalla legge e/o dai regolamenti interni dell'Azienda.

L'U.O.C. Sistemi Informativi gestisce il registro delle firme digitali concesse e provvede al rinnovo di quelle in scadenza, ove ne sussistano le condizioni.

L'U.O.C. Sistemi Informativi, a seguito di comunicazione del Direttore Generale, o del Direttore Amministrativo o del Direttore Sanitario, provvede alla revoca della firma nei casi previsti dalla legge o qualora non sussistano più i presupposti di fatto e di diritto che ne hanno determinato la concessione.

La revoca di un certificato determina la cessazione anticipata della sua validità e può intervenire su iniziativa del Certificatore, del titolare oppure dell'Azienda.

La revoca deve essere richiesta dall'Azienda, quale terzo interessato, al Certificatore laddove ricorra almeno una delle seguenti cause:

a) cessazione del rapporto di lavoro del dipendente per qualunque causa;
b) venir meno, per qualunque causa, dei requisiti di ruolo, qualifica o funzioni istituzionali che ne motivavano l'assegnazione
c) sospetta falsificazione o abusi
d) richiesta di revoca da parte degli interessati motivata dalla possibile, ma non certa, compromissione della chiave privata
e) sospetta perdita di segretezza del codice di sblocco
f) qualunque causa che determini il temporaneo venir meno di uno o più requisiti che ne motivavano l'assegnazione, ivi compresa la sospensione dal servizio del dipendente che ne è titolare
g) perdita di possesso del dispositivo fisico di firma (token) o del dispositivo mobile su cui risiede l'app equivalente

le fattispecie sopra elencate e, in particolare, da *d)* a *g)* devono essere segnalate con immediatezza all'U.O.C. Sistemi Informativi da parte del titolare della firma elettronica.

Gli eventuali supporti fisici residualmente utilizzati per il sistema di firma devono essere restituiti all'U.O.C. Sistemi Informativi quando non più utilizzati.

La richiesta di firma digitale prevede la richiesta da effettuarsi sulla piattaforma aziendale di gestione dei flussi documentali (amministrazione.aornmoscati.it, link *"DgsWebOS"*)

9. Pubblicazione di contenuti web

L'U.O.C. Sistemi Informativi è responsabile dell'infrastruttura ICT/TLC sottesa al portale aziendale *www.aornmoscati.it* ed alla intranet *intranet.aornmoscati.it* e fornisce il relativo supporto tecnico, al fine di garantirne la continuità rispetto al livello di servizio atteso; interviene, inoltre, su disposizione della Direzione Strategica, allorquando è necessario:

- creare una nuova sezione
- modificare il layout o la struttura di una o più pagine
- profilare utenti per la pubblicazione
- erogare nuovi servizi
- pubblicare contenuti in urgenza

9.1. Pubblicazione ul portale (sito web) aziendale

La pubblicazione dei contenuti avviene, in autonomia (ovvero senza necessità di intervento dell'U.O.C. Sistemi Informativi), a cura dei seguenti uffici / strutture:

- U.O.C. Provveditorato – Economato (sezione *"bandi di gara"*)
- U.O.C. Gestione Risorse Umane (sezione *"bandi di concorso"*)
- Ufficio stampa (sezioni *"news"*, *"in primo piano"*, e tutti gli altri contenuti informativi a carattere pubblico sia di carattere estemporaneo – es. eventi – che di carattere strutturale – es. descrizione delle attività delle UU.OO., adeguamento dei contenuti informativi all'Atto Aziendale, nomina di responsabili, etc.)

L'U.O.C. Sistemi Informativi pubblica direttamente i soli contenuti relativi alle sezioni

- *"amministrazione trasparente"*: ogni richiesta di pubblicazione in quest'area deve pervenire, per conoscenza, anche al Responsabile Anticorruzione (RPCT)
- *"regolamenti"*: ogni richiesta deve essere completa della relativa delibera di approvazione

eventuali altri contenuti vengono pubblicati direttamente dall'U.O.C. Sistemi Informativi solo in caso di urgenza e su disposizione della Direzione Strategica.

Gli atti deliberativi e le determine vengono pubblicati automaticamente dal relativo sistema software gestionale.

Laddove un Dipartimento, una U.O. o un ufficio abbia necessità di aggiornare i contenuti informativi della propria pagina, dovrà prendere contatto con l'Ufficio Stampa che, in autonomia, provvederà alla pubblicazione, previa la valutazione e l'assenso della Direzione Strategica.

9.2. Pubblicazione sulla Intranet aziendale

La pubblicazione dei contenuti avviene, in autonomia (ovvero senza necessità di intervento dell'U.O.C. Sistemi Informativi), a cura dei seguenti uffici / strutture:

- Ufficio stampa: sezione "*rassegna stampa"*
- U.O. Rischio Clinico: sezione *"rischio clinico"*
- U.O.C. Sistemi Informativi: sezioni *"comunicazioni ai dipendenti"* (su richiesta del Direttore dell'U.O.C. di riferimento)*, "regolamenti"* (su richiesta del Direttore dell'U.O.C. di riferimento, con gli estremi della Delibera di approvazione)*, "modulistica"* (su richiesta del Direttore dell'U.O.C. di riferimento) ed ogni altro contenuto (su disposizione della Direzione Strategica).

Le richieste di pubblicazione nella sezione *"comunicazioni ai dipendenti"* incomplete di titolo, testo ed eventuali allegati non potranno essere prese in carico.

10.Fax

L'art.47 c.2 lett.c del D.Lgs. n.82 del 7/3/2005, come modificato dall'art. 14, comma 1-bis, D.L. 21 giugno 2013, n. 69, convertito, con modificazioni, dalla L. 9 agosto 2013, n. 98, statuisce, in materia di trasmissione di documenti nella P.A., che *"è in ogni caso esclusa la trasmissione di documenti a mezzo fax"*, limitandone l'utilizzo alla trasmissione, eventualmente da e verso privati.

A tal fine, l'U.O.C. Sistemi Informativi ha implementato un servizio di fax virtuale, attualmente in esercizio, in sostituzione dei numerosi fax fisici esistenti in Azienda, con conseguente risparmio di spesa circa consumabili, manutenzione, carta, etc.

L'uso del fax server è limitato alle fattispecie prescritte dalla normativa innanzi emarginata e, pertanto, non costituisce modalità di comunicazione intra-aziendale né verso altre PP.AA.: per queste ultime due tipologie si dovrà utilizzare la posta elettronica ordinaria e/o certificata.

L'U.O.C. Sistemi Informativi si occupa di normalizzare eventuali difformità pregresse.

Le credenziali per l'accesso al fax server sono assegnate individualmente al referente all'uopo individuato dal Direttore dell'U.O. assegnataria, che ne è responsabile.

Atteso che il fax virtuale non è una risorsa illimitata e che concorre alla produzione di traffico dati sulla rete aziendale, i numeri di fax virtuale non trafficati verso l'esterno per più di tre mesi vengono disattivati dandone informativa all'U.O. che li ha in carico.

L'U.O.C. Sistemi Informativi rileva i dati aggregati del traffico fax generato ai fini della verifica di conformità dell'utilizzo del fax rispetto alla normativa qui richiamata.

11.Telefonia fissa

L'U.O.C. Sistemi Informativi gestisce l'infrastruttura VoIP, attualmente in uso, dedicata alla telefonia aziendale; ogni richiesta di creazione, modifica o cancellazione di numeri di telefono deve pervenire, autorizzata dal Direttore dell'U.O. richiedente, con richiesta formulata per il tramite della piattaforma aziendale di gestione ei flussi documentali (amministrazione.aornmoscati.it, link *"DgsWebOS"*).

Atteso che la numerazione fonia non è una risorsa illimitata e che la fonia concorre alla produzione di traffico dati sulla rete aziendale, i numeri di telefono non trafficati per più di tre mesi vengono disattivati e riassegnati, dandone informativa all'U.O. che li ha in carico.

Le chiamate internazionali ed a pagamento sono inibite; l'abilitazione alle chiamate verso numeri cellulari è concessa su richiesta motivata del Direttore dell'U.O. di afferenza.

L'uso del dispositivo cordless, inteso come tradizionale radiotelefono su tecnologia DECT, non è possibile sull'infrastruttura digitale della rete di telefonia VoIP implementata in aziendale. L'analoga funzionalità è resa tramite la dotazione di un dispositivo mobile smartphone con apposita app *"Rainbow"*.

La richiesta dello smartphone *"Rainbow"* per funzionalità di cordless viene inoltrata formalmente dal Direttore dell'U.O.C. di appartenenza.

Le UU.OO. Sanitarie aventi titolo sono dotate di ulteriori smartphone collegati a specifici numeri di telefonia fissa destinati ai medici di turno per le consulenze e le emergenze/urgenze.

Considerato che l'infrastruttura VoIP è sensibile alle interruzioni di alimentazione elettrica, tutti i reparti e servizi sono stati dotati di più telefoni fissi cosiddetti *"di resilienza"* (opportunamente comunicati e segnalati a tutti gli interessati) che afferiscono ad una particolare infrastruttura TLC che ne consente il funzionamento anche in caso di interruzione elettrica.

12.Assistenza informatica

L'U.O.C. Sistemi Informativi garantisce l'assistenza tecnica informatica sui dispositivi forniti dall'U.O.C. medesima (comprensivi di hardware, software di base e software applicativo) e sull'infrastruttura di TLC aziendale.

Ferme le competenze di altri Uffici (ad esempio Ingegneria Clinica in tema di dispositivi medici e di sistemi software classificati come dispositivi medici), laddove dovessero pervenire richieste di assistenza per sistemi hardware e software non validati dall'U.O.C. Sistemi Informativi, questa sarà erogata, ove possibile, in modalità *"best effort"*, non potendo garantire certezza di tempi o di soluzione su eventuali piattaforme non conformi agli standard tecnici definiti dall'U.O.C. Sistemi Informativi.

L'attività di gestione dei consumabili (es. sostituzione toner) non rientra tra le attribuzioni dell'U.O.C. Sistemi Informativi.

L'attività di trasloco fisico delle apparecchiature non rientra tra le attribuzioni dell'U.O.C. Sistemi Informativi.

Le postazioni di lavoro su cui l'U.O.C. Sistemi Informativi eroga il servizio di assistenza sono individuate dall'apposizione di un'etichetta inventariale di colore **giallo**.

I dipendenti, in caso di problemi tecnici informatici (es. malfunzionamenti hardware, software o rete TLC) devono attivare il servizio di assistenza tecnica esclusivamente tramite chiamata telefonica al numero verde

800 40 50 90

raggiungibile da telefono fisso aziendale; l'operatore che prende in carico la chiamata provvede a fornire un numero di ticket che identifica univocamente l'apertura della segnalazione. Al fini della gestione e soluzione del problema, il chiamante dovrà fornire i seguenti dati:

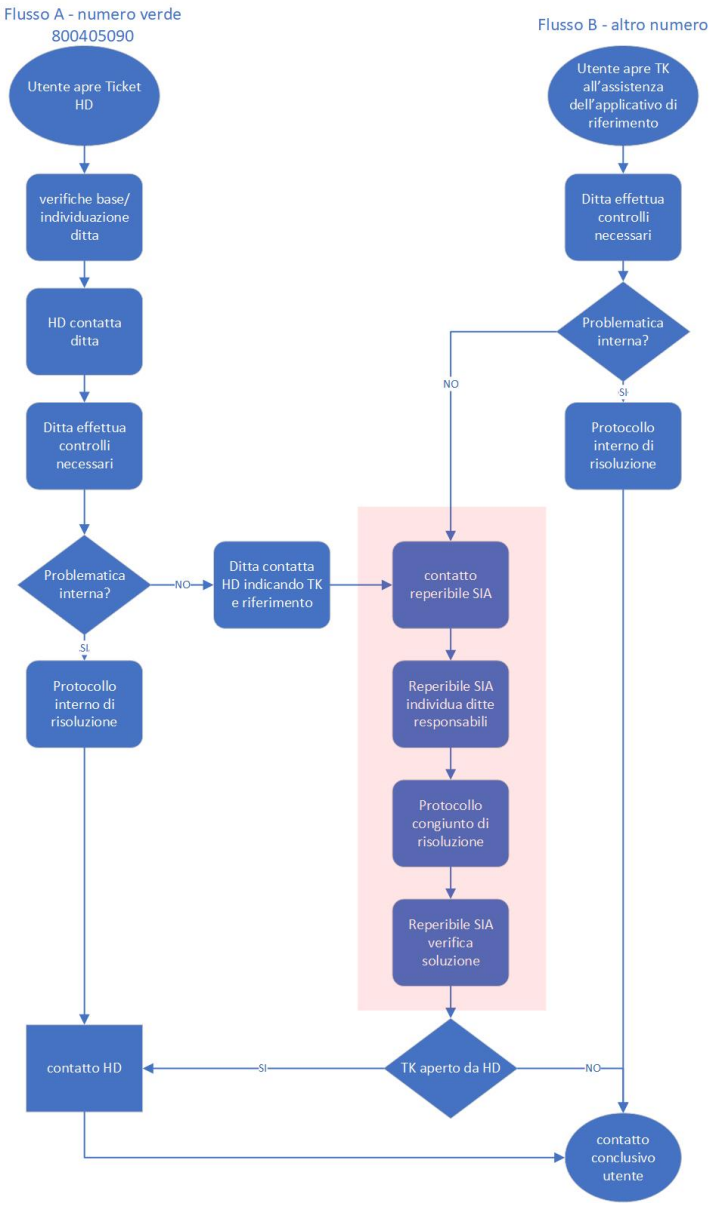
- dati identificativi del chiamante (almeno il numero di matricola)
- numero telefonico per il successivo contatto, qualora il problema risultasse non risolvibile in prima battuta
- descrizione del problema

Se l'utente risulta non raggiungibile, anche dopo reiterati tentativi, il ticket è chiuso d'ufficio, registrandone la motivazione; l'utente dovrà, in tal caso, aprire un nuovo ticket.

Le chiamate al numero verde potranno essere registrate, ai fini della valutazione del servizio, nei termini e nei limiti della vigente normativa in materia di privacy.

Se non è possibile l'immediata soluzione del problema, il ticket viene passato ad un secondo livello di assistenza che provvede alla soluzione tramite collegamento remoto o con intervento in loco.

Nel diagramma seguente si riporta il flusso operativo dell'assistenza informatica:



In aggiunta al numero verde, per il sistema informativo sanitario aziendale è possibile aprire ticket di assistenza tecnica anche utilizzando la piattaforma di ticketing interna al sistema medesimo.

Il personale incaricato dall' U.O.C. Sistemi Informativi ha facoltà di collegarsi da remoto alle singole postazioni di lavoro al fine di erogare il servizio di assistenza tecnica; il collegamento remoto è effettuato esclusivamente su chiamata del dipendente, sempre con il suo espresso consenso ed in modalità visibile e non nascosta, nel rispetto della vigente normativa in materia di privacy.

Il personale incaricato dall'U.O.C. Sistemi Informativi è autorizzato a compiere interventi sui sistemi informatici aziendali diretti a garantire la sicurezza e la salvaguardia dei sistemi stessi, nonché per ulteriori motivi tecnici e/o manutentivi inderogabili (ad esempio aggiornamento / sostituzione / implementazione di programmi, manutenzione hardware).

Il processo di risoluzione dei ticket di assistenza è determinato, in via prioritaria, non dalla consecutività cronologica delle richieste ma dalla loro natura (es. richieste che sottendono a degrado della performance generalizzato hanno la precedenza a richieste, anche bloccanti, per il singolo utente) e dal carico di lavoro del servizio.

La gestione delle richieste avviene nell'ambito e sotto le direttive dell'U.O.C. Sistemi Informativi, che riceve eventuali segnalazioni, al riguardo, in forma scritta e dettagliata all'indirizzo mail *sistemi.informativi@aornmoscati.it*, a firma del responsabile del servizio segnalante, con l'indicazione del numero di ticket.

Le richieste afferenti le apparecchiature elettromedicali non sono di competenza dell'U.O.C. Sistemi Informativi ma dell'Ingegneria Clinica; l'U.O.C. sistemi Informativi collabora con l'Ingegneria Clinica, se richiesto, in caso di necessità, secondo competenza.

Per le eventuali richieste attinenti alle modalità di lavoro in remoto (ad esempio: smartworking), si precisa che la competenza dell'U.O.C. Sistemi Informativi è meramente tecnica e, pertanto, non attiene né all'autorizzazione, né alla validazione dell'attività lavorativa, né all'approvvigionamento di risorse strumentali a domicilio, ma esclusivamente alla messa a disposizione delle risorse informatiche aziendali esistenti in modalità remota. L'U.O.C. Sistemi Informativi non eroga assistenza tecnica sui dispositivi personali che il lavoratore utilizza presso il proprio domicilio.

Riguardo lo smartworking (cd. "lavoro agile"), in particolare, l'U.O.C. Sistemi Informativi può prendere in carico esclusivamente le richieste a firma del Direttore / Dirigente dell'U.O. di competenza che indichino i dati del lavoratore collocato in tale modalità, completi di matricola, cognome, nome, riferimento telefonico e date di inizio e fine dello smartworking; ove fosse necessario l'accesso al pc aziendale la richiesta dovrà essere completa del numero di inventario del medesimo. Ulteriori informazioni in merito ai criteri per dispositivi mobili, telelavoro e lavoro da casa sono riscontrabili nella relativa politica (rif. PR05 Criteri per dispositivi mobili, telelavoro e lavoro da casa).

Gli utenti interni del sistema informativo aziendale sono tenuti a prendere visione della sezione FAQ del portale intranet che espone le soluzioni procedurali ai più comuni problemi di ambito informatico (es. come cambiare la password, etc.) e della manualistica operativa ivi scaricabile; tale manualistica è presente anche sul desktop di ciascun PC gestito dall'U.O.C. Sistemi Informativi.

Non è possibile prendere in carico richieste di assistenza inoltrate in difformità da quanto esposto al presente paragrafo e/o incomplete dei corretti dati di contatto.

Non è possibile prendere in carico richieste di assistenza o di supporto inoltrate da ditte terze per conto delle UU.OO. (es.: richieste di assistenza per videoconferenze collegate ad eventi inoltrate dalla ditta che gestisce l'evento per conto di una U.O.); la richiesta potrà essere presa in carico solo se proveniente dall'U.O.

13.Monitoraggio e controlli

L'Azienda si avvale di sistemi di controllo automatico delle risorse informatiche fisiche e logiche, ad esempio sistemi di:

- asset management, che consentono l'analisi e l'inventario in tempo reale delle postazioni di lavoro, che segnalano automaticamente le modifiche o i tentativi di modifica alla configurazione hardware e software originale
- end-point protection, che, oltre a prevenire e impedire attività malevole, segnalano anche i tentativi di attacco malware con cui la postazione di lavoro entra in contatto
- log di sistema, relativi agli accessi alle risorse ed alla navigazione in internet, che segnalano automaticamente anche tentativi di utilizzo difformi dalle regole implementate sugli apparati di protezione di frontiera
- network access control, che regolano l'accesso alle risorse informatiche ed i relativi livelli di autorizzazione
- monitoraggio della performance degli host che allertano lo staff dell'U.O.C. Sistemi Informativi in caso di superamento di valori soglia

Il trattamento dei dati contenuti nei log avviene in forma anonima e/o aggregata, in modo tale da precludere l'identificazione degli utenti e/o delle loro attività, fatta salva la possibilità di fornire informazioni puntuali su richiesta dell'autorità giudiziaria e, in ogni caso, secondo le prescrizioni di legge.

Tali informazioni vengono utilizzate dall'U.O.C. Sistemi Informativi per il tuning dei sistemi e delle policies di sicurezza.

14.Disposizioni finali

Il mancato rispetto o la violazione delle regole contenute nel presente regolamento sono perseguibili ai sensi dei regolamenti di disciplina di categoria nonché nelle sedi di giudizio, ove ne rilevi la circostanza, fatto salvo comunque il diritto dell'Azienda al risarcimento dei danni eventualmente patiti a causa della condotta del lavoratore.

L'U.O.C. Sistemi Informativi vigila, per quanto di competenza, sul rispetto del presente Regolamento e adotta tutte le opportune soluzioni tecniche disponibili per la sua corretta applicazione.

Per quanto non espressamente richiamato nel presente regolamento, si rinvia alle disposizioni di legge vigenti in materia.

L'U.O.C. Sistemi Informativi normalizza la situazione pregressa rispetto a qualunque difformità che venga riscontrata in ordine alle prescrizioni di cui al presente regolamento.

L'U.O.C. Sistemi Informativi verifica almeno trimestralmente che le risorse assegnate (pc, tablet, account, telefoni, cellulari, numeri di telefono, stampanti, etc.) vengano effettivamente utilizzate e, in caso negativo, provvede al ritiro ed alla riassegnazione, previa verifica con il Direttore dell'U.O. di afferenza, anche per silenzio / assenso.

SAN GIUSEPPE MOSCATI - AVELLINO
AZIENDA OSPEDALIERA DI RILIEVO NAZIONALE E DI ALTA SPECIALITÀ

PSI POLITICA PER LA SICUREZZA DELLE INFORMAZIONI Rev.0 13.05.2024

Dichiarazione generale di politica per la sicurezza

1. SCOPO E CAMPO DI APPLICAZIONE DEL DOCUMENTO

Lo scopo del presente documento è quello di descrivere i principi generali di sicurezza delle informazioni definiti dall' **U.O.C. Sistemi Informativi** al fine di sviluppare un efficiente e sicuro Sistema di Gestione della Sicurezza delle Informazioni.

2. RIFERIMENTI

- ISO/IEC 27001:2022 Information technology – Security techniques - Information security management systems – Requirements
- Decreto legislativo 30 giugno 2003, n. 196 – Provvedimenti del Garante
- Nuovo Regolamento Europeo DGPR 679/2016 in materia di protezione dei dati personali

3. RESPONSABILITÀ ED AGGIORMENTI

La politica della sicurezza delle informazioni viene costantemente aggiornata per assicurare il suo continuo miglioramento ed è condivisa con l'organizzazione, le terze parti ed i clienti, attraverso un sistema documentale interno e specifici canali di comunicazione.

La **U.O.C. Sistemi Informativi** dell'AORN S.G. Moscati è responsabile del sistema di gestione sicura delle informazioni, in coerenza con l'evoluzione del contesto aziendale, valutando eventuali azioni da intraprendere a fronte di eventi come:

- evoluzioni significative del business;
- nuove minacce rispetto a quelle considerate nell'attività di analisi del rischio;
- significativi incidenti di sicurezza;
- evoluzione del contesto normativo o legislativo in materia di trattamento sicuro delle informazioni;

4. SCOPO DELL'ORGANIZZAZIONE

L'**U.O.C. Sistemi Informativi** ha come missione strategica la gestione ed erogazione di servizi informatici con relativi servizi di assistenza e manutenzione nell'ambito Ospedaliero.

Il sistema di gestione, nella sua formulazione e attuazione, risponde a tutti i requisiti normativi che vanno dal 4 al 10.
Non ci sono esclusioni e quindi la stessa organizzazione dichiara la conformità del proprio sistema alla Norma internazionale. **La nostra organizzazione applica tutti i controlli di sicurezza previsti dall'appendice A della Norma ISO 27001:2022.**

5. FINALITÀ STRATEGICA

Per l'**U.O.C. Sistemi Informativi** la sicurezza delle informazioni ha come obiettivo primario la protezione dei dati e delle informazioni, della struttura tecnologica, fisica, logica ed organizzativa, e la loro gestione. Questo significa ottenere e mantenere un sistema di gestione sicura delle informazioni, attraverso il rispetto delle seguenti proprietà:

1. **Riservatezza:** assicurare che l'informazione sia accessibile solamente ai soggetti e/o ai processi debitamente autorizzati;
2. **Integrità:** salvaguardare la consistenza dell'informazione da modifiche non autorizzate;
3. **Disponibilità:** assicurare che gli utenti autorizzati abbiano accesso alle informazioni e agli elementi architetturali associati quando ne fanno richiesta;

la Politica è accessibile sul sito internet dell'organizzazione

4. **Controllo:** assicurare che la gestione dei dati avvenga sempre attraverso processi e strumenti sicuri e testati;
5. **Autenticità:** garantire una provenienza affidabile dell'informazione.
6. **Privacy:** garantire la protezione ed il controllo dei dati personali.

Consapevoli che i dati dell'utente, i risultati della loro analisi, gli indirizzi suggeriti e i metodi di indagine costituiscono informazioni il cui valore rappresenta il patrimonio dell'organizzazione e di quella dell'utente, abbiamo implementato un sistema di gestione per la sicurezza delle informazioni seguendo i requisiti specificati della Norma ISO 27001:2022 e delle leggi cogenti come mezzo per gestire la sicurezza delle informazioni e prevedendo la messa a punto di tutti i controlli di sicurezza applicabili al trattamento delle informazioni.

6. AMBITO DI APPLICAZIONE

La politica per la sicurezza delle informazioni dell'**U.O.C. Sistemi Informativi** si applica a tutto il personale interno ed alle terze parti che collaborano alla gestione delle informazioni ed a tutti i processi e risorse coinvolte nell'erogazione di servizi informatici con relativi servizi di assistenza e manutenzione nell'ambito Ospedaliero.

7. POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

La politica della sicurezza dell'**U.O.C. Sistemi Informativi** rappresenta l'impegno dell'organizzazione nei confronti degli utenti e terze parti a garantire la sicurezza delle informazioni, degli strumenti fisici, logici e organizzativi atti al trattamento delle informazioni in tutte le attività.

La politica della sicurezza delle informazioni dell'U.O.C. Sistemi Informativi si ispira ai seguenti principi:

1. Garantire all'organizzazione la piena conoscenza delle informazioni gestite e la valutazione della loro criticità, al fine di agevolare l'implementazione degli adeguati livelli di protezione.
2. Garantire l'accesso sicuro alle informazioni, in modo da prevenire trattamenti non autorizzati o realizzati senza i diritti necessari.
3. Garantire che l'organizzazione e le terze parti collaborino al trattamento delle informazioni adottando procedure volte al rispetto di adeguati livelli di sicurezza.
4. Garantire che le anomalie e gli incidenti aventi ripercussioni sul sistema informativo e sui livelli di sicurezza aziendale siano tempestivamente riconosciuti e correttamente gestiti attraverso efficienti sistemi di prevenzione, comunicazione e reazione al fine di minimizzare l'impatto sul business.
5. Garantire che l'accesso alle sedi ed ai singoli locali aziendali avvenga esclusivamente da personale autorizzato, a garanzia della sicurezza delle aree e degli asset presenti.
6. Garantire la conformità con i requisiti di legge ed il rispetto degli impegni di sicurezza stabiliti nei contratti con le terze parti.
7. Garantire la rilevazione di eventi anomali, incidenti e vulnerabilità dei sistemi informativi al fine di rispettare la sicurezza e la disponibilità dei servizi e delle informazioni.
8. Garantire la business continuity aziendale e il disaster recovery, attraverso l'applicazione di procedure di sicurezza stabilite.
9. Garantire risorse adeguate, aggiornate ed adeguatamente qualificate per la sicurezza delle informazioni

la Politica è accessibile sul sito internet dell'organizzazione

PSI POLITICA PER LA SICUREZZA DELLE INFORMAZIONI Rev.0 13.05.2024

La politica della sicurezza delle informazioni dell'U.O.C. Sistemi Informativi persegue i seguenti obiettivi:

1) **rispettare** le leggi e le disposizioni vigenti, i requisiti contrattuali e le procedure in essere, conformandosi ai principi e ai controlli stabiliti dalla ISO/IEC 27001:2022 o altre norme/regolamenti che disciplinano le attività in cui opera, tra i quali, in particolare le regolamentazioni inerenti i trattamenti dei dati personali e la loro sicurezza.

2) **dimostrare** agli stakeholders la propria capacità di fornire con regolarità la gestione ed erogazione di servizi informatici con relativi servizi di assistenza e manutenzione nell'ambito Ospedaliero, massimizzando gli obiettivi di sicurezza, anche promuovendo la collaborazione, comprensione e consapevolezza da parte dei fornitori strategici;

3) **minimizzare** il rischio di perdita e/o indisponibilità dei dati gestiti, pianificando e gestendo le attività a garanzia della continuità di servizio, svolgendo una continua ed adeguata analisi dei rischi che esamini costantemente le vulnerabilità e le minacce associate alle attività a cui si applica il sistema, controllando con continuità il corretto funzionamento degli asset aziendali al fine di rilevare eventi anomali, incidenti e vulnerabilità dei sistemi informativi per rispettare la sicurezza e la disponibilità dei servizi e delle informazioni;

4) **migliorare** con continuità il sistema di sicurezza delle informazioni al fine di rendere sempre più efficiente e sicuro il sistema informativo.

Politica per l'impegno per il miglioramento continuo del sistema di gestione

Il patrimonio informativo dell'utente e quello relativo al know-how dell'organizzazione costituiranno d'ora innanzi i punti focali dell'impegno di tutti. Un impegno assunto da tutti e da ciascuno.

Tale impegno sarà manifestato attraverso le "performance di sicurezza" che dovranno dare evidenza di quanto la nostra organizzazione ed il nostro sistema di gestione della sicurezza delle informazioni siano efficaci nel registrare un miglioramento continuo.

A.O.R.N. S. Giuseppe Moscati
U.O.C. Sistemi Informativi
Il Direttore
Dott. Giuseppe Versace

la Politica è accessibile sul sito internet dell'organizzazione

SAN GIUSEPPE MOSCATI - AVELLINO
AZIENDA OSPEDALIERA DI RILIEVO NAZIONALE E DI ALTA SPECIALITÀ

							Aggiornato al	13/09/2024
	Documenti descrittivi e prescrittivi		Classificazione Documento/Informazione			Revisione	Data Revisione	Tipo Documento
			P Pubblica	I Interna	C Confidenziale			
PSI	Politica per la Sicurezza delle Informazioni	(punto 5.2 controllo A.5.10)	P			0	13/05/2024	Policy
SOA	SOA		P			0	13/05/2024	Rapporto
DOC01	Clausole per le terze parti				C	0	13/05/2024	Documento
ORG	Funzionigramma U.O.C. Sistemi Informativi	(punto 5..3)		I		1	27/08/2024	Documento
MSGSI	Manuale Sicurezza Informatica			I		0	13/05/2024	Manuale
DOC02	Perimetro di certificazione	(punto 4.3)		I		1	10/09/2024	Documento
DOC03	Metodologia di Analisi del Rischio Cyber			I		1	10/09/2024	Documento
Mod01DOC03	Analisi e trattamento del rischio			I		1	10/09/2024	Documento
DOC04	Registro dei Trattamenti DSI			I		0	13/05/2024	Documento
PR01	Controllo dei documenti e delle registrazioni	(punto 7.5, controllo A.5.33)		I		0	13/05/2024	Procedura
Mod01PR01	Elenco dei documenti e delle norme	A.5.31	P			0	13/05/2024	Documento
PR02	Contesto, Swot e Gestione del rischio	(punto 4.2)		I		0	13/05/2024	Procedura
PR03	Gestione rischi e opportunità	(punto 6.1.2)		I		0	13/05/2024	Procedura
Mod01PR03	Identificazione e Valutazione del Rischio	(punto 6.1.3 e 6.2, 8.2 e 8.3)		I		0	13/05/2024	Documento
Mod02PR03	Scheda Obiettivo	(punto 6.2)		I		0	13/05/2024	Documento
PR04	Politica Gestione degli asset	(controllo A.5.9)		I		0	13/05/2024	Policy
Mod01PR04	Inventario degli asset			I		0	13/05/2024	Documento
PR05	Politica Criteri per dispositivi mobili, telelavoro e lavoro da casa	(controlli A.6.7, A.7.8, A.7.9 e A.8.1)		I		0	13/05/2024	Policy
PR06	Procedura smaltimento e distruzione dei dispositivi	(controlli A.7.10, A.7.14 e A.8.10)		I		0	13/05/2024	Procedura
PR07	Procedura di Gestione degli Amministratori di Sistema	(controllo A.7.7)		I		0	13/05/2024	Procedura
Mod01PR07	Elenco Amm.ri di Sistema			I		0	13/05/2024	Documento
Mod02PR07	Format Nomina			I		0	13/05/2024	Documento
Mod03PR07	Format Revoca			I		0	13/05/2024	Documento
PR08	Politica Criteri di backup	(controllo A.8.13)		I		0	13/05/2024	Policy
PR09	Politica Criteri di crittografia	(controllo A.8.24)		I		0	13/05/2024	Policy
PR10	Politica di gestione delle modifiche	(controllo A.8.32)		I		0	17/05/2024	Policy
PR11	Procedura per lo sviluppo delle competenze in materia di sicurezza delle informazioni	(punto 7.2)		I		0	17/05/2024	Procedura
Mod01PR11	Verbale di Formazione			I		0	17/05/2024	Documento
PR12	Procedura Comunicazione			I		0	17/05/2024	Procedura
PR13	Politica Classificazione delle informazioni (Comunicazione e trasferimento delle informazioni)	(controlli A.5.10, A.5.12 e A.5.13)		I		0	17/05/2024	Policy
PR14	Procedura Controllo degli accessi fisici e logici	(controllo A.5.15)		I		0	17/05/2024	Procedura
PR15	Politica Criteri password	(controlli A.5.16, A.5.17 e A.8.5)		I		0	17/05/2024	Policy
PR16	Politica Sicurezza fisica e ambientale delle informazioni			I		0	17/05/2024	Policy
PR17	Politica Data retention e cancellazione			I		0	17/05/2024	Policy
PR18	Politica Gestione dei Fornitori ICT	(controlli A.5.19, A.5.21, A.5.22 e A.5.23)		I		0	17/05/2024	Policy
PR19	Politica Security e privacy by design			I		0	17/05/2024	Policy
PR20	Politica Acquisizione e manutenzione dei sistemi			I		0	17/05/2024	Policy
PR21	Politica Business Continuity & Gestione della Crisi			I		0	17/05/2024	Policy
PR22	Politica di clear desk clean screen			I		0	17/05/2024	Policy
PR23	Procedura Change & Patch Management			I		0	29/05/2024	Procedura
PR24A	Runbook DDoS			I		0	29/05/2024	Documento
PR24B	Runbook Ransomware			I		0	29/05/2024	Documento
PR25	Procedura Security Event and Incident Management	(controllo A.5.7)		I		0	29/05/2024	Procedura
Mod01PR25	Registro Eventi ed Incidenti di Sicurezza			I		0	29/05/2024	Documento
PR26	Procedura Piano di continuità operativa			I		0	29/05/2024	Procedura
Mod01PR26	Lista contatti interni ed esterni			I		0	29/05/2024	Documento
Mod02PR26	Preliminary Business Impact Analysis			I		0	29/05/2024	Documento
PR27	Procedura Vulnerability Management			I		0	29/05/2024	Procedura
PR28	Procedura di Internal Audit	(punto 9.2)		I		0	29/05/2024	Procedura
Mod.01PR28	Piano di Audit	(punto 9.2)		I		0	29/05/2024	Documento
Mod.02PR28	Rapporto di Audit	(punto 9.2)		I		0	29/05/2024	Documento
Mod.03PR28	Registro Non Confomità	(punto 9.2)		I		0	29/05/2024	Documento
PR29	Procedura Riesame della Direzione	(punto 9.3)		I		0	29/05/2024	Procedura
Mod.01PR29	Verbale di Riesame della Direzione	(punto 9.3)		I		0	29/05/2024	Documento