Disciplinare dell'AO di Alessandria per l'uso di Internet, della Posta elettronica e della tenuta di file della rete interna

REGOLAMENTO PER L'UTILIZZO DEI SERVIZI ICT - Febbraio 2023

Azienda Ospedaliera di Alessandria

S.C. Area I.C.T.

Azienda Ospedaliera Nazionale

SS. Antonio e Biagio e Cesare Arrigo Alessandria

Febbraio 2023

Sommario

INTRODUZIONE ED AMBITO DI APPLICAZIONE

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

Premesso quindi che l'utilizzo delle risorse informatiche e telematiche deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito dei rapporti di lavoro, l'Azienda Ospedaliera "S.S. Antonio e Biagio e C. Arrigo", di seguito "ASO", con il presente Regolamento intende orientare i comportamenti degli operatori, in modo da evitare che azioni inconsapevoli possano innescare problemi o minacce alla sicurezza nel trattamento dei dati. A tale riguardo, si integra quanto disposto dal Regolamento (UE) 2016/679 del parlamento europeo e del Consiglio del 27 aprile 2016 (GDPR -General Data Protection Regulation).

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

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

Sono a

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

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

Ai fini del Regolamento si considerano le definizioni:

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

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

ASO: l'Azienda Ospedaliera S.S. Antonio e Biagio e Cesare Arrigo.

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

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

MFA: Multi Factor Authentication, autenticazione a più fattori

OTP: One Time Password

PdL: Postazione di Lavoro

Responsabili del Trattamento: sono tutti i Direttori e Responsabili di Struttura;

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

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

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

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

VPN: Virtual Private Network

SICUREZZA

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

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

PRINCIPI GENERALI

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

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

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

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

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

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

Il posto di lavoro, costituito da personal computer viene consegnato completo di quanto necessario per svolgere le proprie funzioni, software applicativo compreso, è pertanto vietato modificarne la configurazione.

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

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

L'uso delle risorse tecnologiche è limitato ai fini lavorativi ed istituzionali dell'ASO.

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

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

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

UTILIZZO DELLA PDL (POSTAZIONE DI LAVORO)

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

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

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

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

Al momento della consegna di un PdL sarà richiesta un'esplicita assunzione di responsabilità circa la regolare custodia e mantenimento della PdL, mediante firma di apposito modulo *(Allegato_4)*.

Eventuali, motivate, modifiche alla configurazione fisica possono essere effettuate solo dai tecnici della S.C. "Area I.C.T.". Eventuale e motivato spostamento della PdL può essere effettuato solo se autorizzati dai tecnici della S.C. "Area I.C.T.".

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

Il personale incaricato della S.C. "Area I.C.T." ha la facoltà di collegarsi e visualizzare in remoto il desktop delle singole postazioni PC, al fine di garantire l'assistenza tecnica e la normale attività operativa, nonché la massima sicurezza contro virus, spyware, malware, etc.

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

Non è consentito l'uso di programmi diversi da quelli ufficialmente installati dal personale della S.C. "Area I.C.T." per conto dell'ASO, né viene consentito agli utenti di installare autonomamente programmi provenienti dall'esterno, sussistendo infatti il grave pericolo di introdurre Virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti. L'inosservanza della presente disposizione espone la stessa A.O. a gravi responsabilità civili; si evidenzia inoltre che le violazioni della normativa a tutela dei diritti d'autore sul software, che impone la presenza nel sistema di software regolarmente licenziato, o comunque libero e quindi non protetto dal diritto d'autore, vengono sanzionate anche penalmente.

Salvo preventiva espressa autorizzazione del personale della S.C. "Area I.C.T.", non è consentito all'utente modificare le caratteristiche impostate sul proprio personal computer o sulla PdL in generale, né procedere ad installare dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, modem/router USB, dispositivi di memorizzazione USB ecc…).

Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il personale della S.C. "Area I.C.T." nel caso in cui siano rilevati virus.

RICHIESTA DI NUOVA PDL O SOSTITUZIONE DI PDL

Le Unità Operative potranno richiedere alla S.C. "Area I.C.T." la fornitura di una nuova PdL o la sostituzione della PdL in uso utilizzando esclusivamente gli appositi moduli (*Allegato_1 e Allegato_2*) compilabili sull'area Intranet e la relativa apertura di un ticket.

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

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

Laddove si renda necessario, formattare, cancellare o spostare dei dati tutti o in parte contenuti nell'hard disk della pdl l'utente dovrà compilare l'apposito modulo *(Allegato_3)* e la relativa apertura di un ticket.

MODALITÀ DI ACCESSO ALLA RETE ED AGLI APPLICATIVI

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

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

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

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

PRINCIPI GENERALI

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

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

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

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

SOGGETTI CHE POSSONO AVERE ACCESSO ALLA RETE

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

L'amministratore di sistema regolamenta l'accesso alla rete di determinate categorie di incaricati in base alla categoria di appartenenza secondo quanto indicato dal Responsabile del trattamento.

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

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

ACCESSO ALLA RETE INTERNA

Per essere autorizzati all'uso delle risorse informatiche, applicativi e posta elettronica è necessario che il Responsabile del Trattamento dei dati della Struttura invii l'apposito modulo *(Allegato_5)* e apra il ticket.

Tale modello deve essere compilato in ogni sua parte e quindi fatto pervenire agli amministratori di sistema.

Nel caso fosse evidenziata dal Responsabile la necessità per l'incaricato di accedere ai dati di competenza di una struttura diversa dalla propria, la richiesta di accesso dovrà essere approvata e sottoscritta anche dal responsabile del trattamento della struttura interessata.

Gli Amministratori di Sistema provvedono ad assegnare ad ogni incaricato un Account di rete secondo le modalità più avanti descritte.

ACCESSO ALLA RETE DALL'ESTERNO

Questa modalità di accesso prevede l'attivazione di una VPN (Virtual Private Network) ed è riferibile:

- al personale sanitario autorizzato dalla Direzione Medica di presidio, per funzioni di controllo da remoto di immagini diagnostiche e parametri vitali durante le reperibilità;
- al personale tecnico amministrativo in funzione della modalità di smart working autorizzato dal proprio Responsabile di Struttura;
- alle ditte che svolgono attività di manutenzione sui sistemi (hardware e software applicativi) come previsto nei contratti di Assistenza e Manutenzione stipulati tra la ditta e l'ASO.

La tipologia di accesso prevede la comunicazione di una mail personale a cui inviare un codice OTP per l'accesso in modalità MFA al collegamento privato.

Per essere autorizzati all'accesso tramite VPN, è necessario che il soggetto autorizzato al Trattamento dei dati della Struttura invii l'apposito modulo, lo stesso per la richiesta di accesso alla rete interna (*Allegato_5*), barrando l'apposita casella e indicando una mail personale, ed apra il ticket.

Ulteriori dettagli, nel paragrafo "Gestione delle VPN".

FORNITORI

Per essere autorizzati all'uso delle risorse informatiche e dei relativi servizi, è necessario inviare l'apposito modulo (*Allegato_6*) all'indirizzo **help_desk@ospedale.al.it** per ogni incaricato, che contenga i dati anagrafici degli incaricati, le risorse informatiche a cui accedere e gli estremi del contratto in essere con l'Azienda Ospedaliera.

CREDENZIALI DI ACCESSO ALLA RETE INFORMATICA

Le credenziali sono strettamente personali.

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

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

La disattivazione delle credenziali di autenticazione è immediata:

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

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

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

La password deve almeno

- avere una lunghezza minima di 8 caratteri, preferibilmente di 14 caratteri
- essere composte di caratteri alfanumerici con la presenza di caratteri maiuscoli e minuscoli
- contenere almeno un carattere speciale (!,?,$,&, ecc...)
- NON contenere nome/cognome proprio o informazioni come la data di nascita
- essere uniche per ciascun servizio o sito a cui si accede

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

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

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

ATTIVITÀ NON CONSENTITE NELL'USO DELLA RETE

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

Non sono inoltre consentite le seguenti attività:

- Utilizzare le Risorse Tecnologiche per usare, archiviare, detenere, duplicare o diffondere in qualunque forma materiali tutelati da diritti d'autore o diritti connessi o sui quali terzi vantino diritti morali e patrimoniali (D.lgs. n. 68/2003, Legge 22 Aprire 1941 n.633 e successive modificazioni);
- Usare la rete in modo difforme da quanto previsto dalle leggi penali, civili e amministrative e da quanto previsto dal presente regolamento;
- Utilizzare la Rete e in generale le risorse informatiche dell'ASO per scopi incompatibili con l'attività istituzionale dell'ASO stessa;
- Conseguire l'accesso non autorizzato a risorse di rete interne ed esterne alla Rete;
- Violare la riservatezza di altri incaricati o di terzi;
- Agire deliberatamente con attività che influenzino negativamente la regolare operatività della Rete e ne restringano l'utilizzabilità e le prestazioni per altri incaricati;
- Effettuare o permettere ad altri trasferimenti non autorizzati di informazioni (software, dati, etc.…);
- Installare qualsiasi programma da parte dell'incaricato o di altri operatori, se non previa autorizzazione degli amministratori di sistema;
- Installare applicativi non compatibili con l'attività istituzionale:
- Disinstallare, cancellare, copiare o asportare programmi software per scopi personali;
- Installare componenti hardware senza preventiva autorizzazione degli amministratori di sistema;
- Rimuovere, danneggiare o asportare componenti hardware e software fornite dall'amministratore di sistema;
- Utilizzare qualunque tipo di sistema informatico o elettronico per controllare le attività di altri incaricati, per leggere, copiare o cancellare files e software di altri incaricati;
- Utilizzare software visualizzatori di pacchetti TCP/IP, software di intercettazione di tastiera, software di decodifica password e più in generale software rivolti alla violazione della sicurezza del sistema e della privacy;
- Inserire password locali alle risorse informatiche assegnate (come, ad esempio, password che non rendano accessibile il computer agli amministratori di rete), se non prima comunicate agli amministratori di sistema e da questi espressamente autorizzate;
- Abbandonare il posto di lavoro lasciandolo senza protezione da accessi non autorizzati.

POSTA ELETTRONICA

Il servizio di posta elettronica è concesso esclusivamente ai dipendenti e agli operatori dei quali sia riconosciuta l'attività coerente con i fini lavorativi e istituzionali dell'Ente. Ogni responsabile del trattamento può richiedere l'assegnazione di una casella di posta elettronica per motivi di servizio per i propri collaboratori, compilando l'apposito modulo (*Allegato_5*) scaricabile dalla Intranet aziendale.

Sono attivati indirizzi di posta elettronica per le strutture aziendali, condivisi dagli operatori assegnati a ciascuna di esse (es.: tecnico@ospedale.al.it; medicina@ospedale.al.it).

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

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

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

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

ED IN INGLESE:

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

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

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

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

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

REGOLE DI GESTIONE DELLA CASELLA DI POSTA

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

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

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

ATTIVITÀ NON CONSENTITE NELLA GESTIONE DELLA POSTA ELETTRONICA

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

* L'utilizzo della posta elettronica per fini diversi da quelli istituzionali;
* Un uso che possa in qualche modo recare qualsiasi danno all'ASO o a terzi, come l'apertura di allegati in messaggi di posta elettronica senza il previo accertamento dell'identità del mittente;
* Inoltrare "catene" di posta elettronica, anche se afferenti a presunti problemi di sicurezza;

* La trasmissione a mezzo di posta elettronica di dati sensibili, confidenziali e personali di alcun genere, salvo i casi espressamente previsti dalla normativa vigente in materia di protezione dei dati personali (come da disposizioni del vigente GDPR).

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

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

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

La nomina del fiduciario deve essere redatta in forma scritta, riportare la sottoscrizione del fiduciante e del fiduciario e dovrà essere consegnata al responsabile del trattamento.

ACCESSO AD INTERNET ED USO RETE AZIENDALE

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

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

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

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

ATTIVITÀ NON CONSENTITE NELL'UTILIZZO DELL'ACCESSO A INTERNET

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

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

MEMORIZZAZIONE FILE DI LOG DELLA NAVIGAZIONE INTERNET

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

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

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

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

GESTIONE DI STRUMENTI ELETTRONICI / INFORMATICI INDIVIDUALI

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

1. sulle aree condivise del file server appositamente dedicate all'archiviazione documentale. La sicurezza dei documenti conservati sulle apposite aree del server è a cura della S.C. "Area I.C.T:";

2. mediante lo spazio su cloud aziendale compreso nella Suite Office 365, **One Drive** e **SharePoint**, che mette a disposizione, dai 50 Gb ai 100 Gb per ogni utente, a seconda della tipologia di licenza (rispettivamente E1 o E3). **Quest'ultima modalità è caldamente raccomandata, consentendo maggiore flessibilità, portabilità e possibilità di collaboration nel pieno rispetto della sicurezza e della tutela dei dati**.

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

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

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

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

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

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

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

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

GESTIONE DELL'AMBIENTE DI CARTELLE CONDIVISE

AI fine di rendere più efficienti e sicuri i sistemi di condivisione e salvataggio dei file correlati alle attività lavorative, a partire dal 01/04/2023 saranno disponibili le nuove cartelle condivise centralizzate (il cosiddetto "File Server") in sostituzione di quelle esistenti. Per ogni Centro di Responsabilità (CdR) aziendale sarà disponibile, previa richiesta alla S.C. Area ICT secondo le modalità descritte in seguito, **un'unica cartella avente per nome il codice CdR.**

Si raccomanda di salvare quanto strettamente necessario alla produttività individuale o alle esigenze di reparto prima della data sopra indicata. Dopo il 01/04/2023 il vecchio File Server sarà smantellato e sostituito dalla infrastruttura descritta.

MODALITÀ DI RICHIESTA DI UNA NUOVA CARTELLA CONDIVISA

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

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

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

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

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

La SC Area ICT fornirà ad ogni referente il supporto per gestirne i permessi di autorizzazione.

CAPIENZA DELLE CARTELLE CONDIVISE

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

CONTENUTI E FORMATO DEI DOCUMENTI

Le nuove cartelle condivise dovranno essere utilizzate esclusivamente per il salvataggio dei documenti statici di office automation inerenti all'attività istituzionale e non per applicativi multi-utenza, quali ad esempio MS Access, OO Base, etc., che richiedono specifici progetti e attrezzature informatiche.

Non potranno altresì contenere dati sensibili, men che meno dei pazienti e non saranno consentite scansioni di cartelle cliniche, copie di esami, richieste di prestazioni sanitarie, immagini diagnostiche e quant'altro possa compromettere il diritto alla riservatezza dei dati sanitari verso il paziente.

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

Potranno essere salvati solo documenti nei seguenti formati:

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

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

MODALITÀ ACCESSO UTENTE

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

RISERVATEZZA ED INTEGRITÀ DEI DATI

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

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

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

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

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

DISATTIVAZIONE VECCHIE CARTELLE CONDIVISE

Le vecchie aree share di presidio saranno utilizzabili fino al 31/03/2023 per dare la possibilità agli amministratori e agli utenti di rendere operative in modo graduale le nuove cartelle condivise.

A partire dal 01/04/2023 e fino al 31/08/2023, le vecchie aree share saranno consultabili in sola lettura, dopodiché verranno dismesse definitivamente.

A partire dal 01/04/2023 verranno interrotti i backup delle vecchie zone.

ASSISTENZA

Tutte le richieste di assistenza saranno accettate solamente se provenienti dai referenti delle cartelle condivise. Ogni quesito potrà essere esposto dal referente al servizio di 'HELP-DESK dell'Area ICT tramite mail help_desk@ospedale.al.it e telefono 0131 20 7800.

GESTIONE DELLE VPN

I dipendenti e/o i fornitori, per l'accesso in VPN (Virtual Private Network), possono accedere ad un collegamento tramite VPN delle PdL o delle infrastrutture informative aziendali, previa opportuna richiesta alla S.C. "Area I.C.T." e seguendo le indicazioni contenuto nella procedura aziendale relativa.

Che cosa è un accesso VPN

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

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

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

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

- accedere all'infrastruttura del Titolare per conseguire l'accesso non autorizzato a risorse di rete interne od esterne al Titolare;
- fornire il servizio di connettività di rete a soggetti non autorizzati all'accesso all'infrastruttura;
- violare gli obblighi contrattualmente assunti dal Titolare per la realizzazione e la gestione della propria infrastruttura, particolarmente in materia di diritto d'autore, licenze d'uso di software e regolamenti dei fornitori di connettività di rete;
- svolgere attività che causino malfunzionamento, diminuiscano la regolare operatività, danneggino o restringano l'utilizzabilità o le prestazioni dei sistemi del Titolare;
- violare la sicurezza di archivi e banche dati, compiere trasferimenti non autorizzati di informazioni (software, basi dati, ecc.), intercettare, tentare d'intercettare o accedere a dati in transito sull'infrastruttura del Titolare, dei quali non si è destinatari specifici;

- compiere azioni in violazione delle norme a tutela delle opere dell'ingegno, del diritto d'autore e del software;
- distruggere o tentare di distruggere, danneggiare o tentare di danneggiare, intercettare o tentare di intercettare, accedere o tentare di accedere senza autorizzazione alla posta elettronica o ai dati di altri Utenti o di terzi, usare, intercettare o diffondere o tentare di intercettare o diffondere password o codici d'accesso o chiavi crittografiche di altri Utenti o di terzi, e in generale commettere o tentare di commettere attività che violino la riservatezza di altri Utenti o di terzi, così come tutelata dalle norme civili, penali e amministrative applicabili.

Il servizio tecnico della S.C. "Area I.C.T." può disattivare, in qualsiasi momento, le credenziali o disconnettere un accesso VPN, senza necessità di preventivo avviso, qualora la disattivazione sia necessaria all'integrità o al funzionamento dei propri servizi ICT, oppure qualora vi sia fondato sospetto che l'utente VPN abbia violato il presente Regolamento. Il servizio tecnico della S.C. "Area I.C.T." utilizzerà sia sistemi di monitoraggio della rete che sistemi in grado di verificare che l'operato dell'Utente VPN risponda a quanto previsto dal presente Regolamento e nel rispetto delle normative vigenti.

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

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

ASSISTENZA DA REMOTO E SERVIZI DI REPERIBILITÀ

Il personale tecnico della S.C. "Area I.C.T." effettua attività di help desk e assistenza sia on-site che da remoto. Entrambe le tipologie di attività sono attivabili dagli utenti dell'ospedale mediante:

- chiamata al numero interno 0131 – 20 7800
- mail all'indirizzo: help_desk@ospedale.al.it
- compilazione dell'apposito form nella Intranet.

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

Le attività da remoto sono relative ai seguenti ambiti:

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

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

Gli operatori del servizio di help desk della S.C. "Area I.C.T.", a seguito della segnalazione telefonica o dell'apertura del ticket secondo le modalità su indicate (mail o compilazione del form sulla Intranet):

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

Il supporto di assistenza viene fornito nei seguenti orari:

- dal lunedì al venerdì: dalle 8,00 alle 17,00, con la presenza garantita di operatori in sede o da remoto se in smart working;
- dal lunedì al venerdì: dalle 20,00 alle 8,00 del giorno successivo, assistenza erogata da 1 unità di personale reperibile contattabile tramite il centralino dell'ASO;
- sabato e festivi: assistenza h24 erogata da personale reperibile contattabile tramite il centralino dell'ASO.

INDICAZIONI SUL SERVIZIO DI REPERIBILITÀ

Ai fini della copertura del servizio, è prevista la turnazione del personale tecnico afferente alla S.C. "Area I.C.T." durante la fascia oraria 17:00 – 08:00 dei giorni feriali, il sabato ed i festivi. In particolare, è previsto un reperibile per i periodi menzionati con lo specifico compito di prendere in carico le segnalazioni pervenute, aprire i ticket relativi ed eseguire le attività di I livello con particolare riferimento ai seguenti ambiti:

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

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

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

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

GRADUALITÀ DEI CONTROLLI

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

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

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

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

VIOLAZIONE AL PRESENTE REGOLAMENTO

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

PROVVEDIMENTI DISCIPLINARI

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

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

ALLEGATI AL REGOLAMENTO

- Allegato_1_Modulo_nuovo_hw
- Allegato_2_Modulo_spostamento_hw
- Allegato_3_Modulo_manutenzione_hw
- Allegato_4_Modulo_consegna_hw
- Allegato_5_ModuloChiaviAccesso_VPN
- Allegato_6_Modulo_accessoVPN_esterni

I presenti allegati al regolamento sono consultabili anche nel Sistema Qualità Aziendale per l'Area ICT.

REDAZIONE DOCUMENTO

	Cognome Nome	Ruolo	Data	Firma
Redazione	Gagandeep Singh Saini	Collaboratore tecnico professionale Cat. D	08/02/2023	GAGANDEEP SINGH SAINI AZIENDA OSPEDALIERA ALESSANDRIA 08.03.2023 08:25:28 UTC
	Michele Matteo Deserventi	Collaboratore tecnico professionale Cat. D	08/02/2023	MATTEO MICHELE DESERVENTI AZIENDA OSPEDALIERA ALESSANDRIA 13.03.2023 08:39:59 UTC
Revisori	Dario Ricci	Direttore f.f. SC Area ICT	06/03/2023	DARIO RICCI AZIENDA OSPEDALIERA ALESSANDRIA 13.03.2023 08:51:58 UTC
	Giulia Cunietti	Dirigente Analista	06/03/2023	GIULIA CUNIETTI AZIENDA OSPEDALIERA ALESSANDRIA 06.03.2023 14:19:19 UTC
Approvazione				

Data di rilascio	Nome documento	Versione
	Regolamento sull'uso degli strumenti informatici aziendali ASO AL	

Azienda Ospedaliera Nazionale
Santi Antonio e Biagio e Cesare Arrigo
Alessandria

RICHIESTA NUOVO HARDWARE

Giorno 28/02/2023

SERVIZIO:

RESPONSABILE:

UBUCAZIONE SERVIZIO:

UTENTE DI RIFERIMENTO:

TELEFONO:

INDICAZIONE DELLA COLLOCAZIONE DEL NUOVO HARDWARE

La collocazione deve essere provvista dei punti rete ed elettrici necessari

REPARTO/STRUTTURA:

PIANO:

STANZA:

PORTA DI RETE:

QUANTITA':

HARDWARE:

☑ PC ☐ MONITOR ☐ STAMPANTE ☐ CASSE ☐ WEBCAM ☐ TABLET ☐ LETTORE BARCODE

☐ PUNTO RETE ☐ TELEFONO ○ Altro

MOTIVAZIONE RICHIESTA:

◉ Nuovo Personale ○ Ampliamento Servizio ○ Sostituzione ○ Altro

DATA: **FIRMA del Richiedente:**

DATA: **FIRMA del Responsabile :**

STAMPA

Azienda Ospedaliera Nazionale
Santi Antonio e Biagio e Cesare Arrigo
Alessandria

RICHIESTA TRASFERIMENTO POSTAZIONE LAVORO

Giorno 28/02/2023

SERVIZIO:

RESPONSABILE:

UBUCAZIONE SERVIZIO:

UTENTE DI RIFERIMENTO:

TELEFONO:

POSTAZIONE DA TRASFERIRE

REPARTO/STRUTTURA:

PIANO:

STANZA:

INVENTARIO:PC

INVENTARIO:MONITOR

INVENTARIO:STAMPANTE

QUANTITA':

INDICAZIONE DELLA NUOVA COLLOCAZIONE

REPARTO/STRUTTURA:

PIANO:

STANZA:

PORTA DI RETE:

QUANTITA':

HARDWARE:

☑ PC ☐ MONITOR ☐ STAMPANTE ☐ TELEFONO

DATA: **FIRMA del Richiedente:**

DATA: **FIRMA del Responsabile :**

STAMPA

AO AL Azienda Ospedaliera di ALESSANDRIA Santi Antonio e Biagio e Cesare Arrigo

Via Venezia, 16 – 15121 ALESSANDRIA
Tel . 0131 206111 – www.ospedale.al.it
info@ospedale.al.it
asoalessandria@pec.ospedale.al.it (solo certificata)
C.F. – P.I. 01640560064

S.C. Area I.C.T.
Direttore f.f.: ing. Ricci Dario

Modulo Manutenzione HW

Indicazione reparto, ufficio, struttura _____

Dati referente del reparto, ufficio, struttura:

- Nome e cognome: _____
- Mail:_____ Tel:_____

Con la sottoscrizione del presente modulo si solleva il servizio Area ICT dalla responsabilità sui dati che risiedono sulla seguente macchina in caso di **formattazione o manutenzione, cambio pc per riparazione di guasti**:

Cespite/Inventario Ospedaliero: _____

Numero di serie: _____

Cognome e Nome del responsabile dei dati:

_____

Il presente modulo va necessariamente inviato via mail a help_desk@ospedale.al.it.
La firma può essere autografa oppure digitale[1].

Firma autografa del responsabile dei dati (da inserire solo nel caso in cui il modulo non venga firmato digitalmente)

_____

[1]Con validità a norma del Codice di Amministrazione Digitale (d.lgs 82/2005 e s.m.i.) e preferibilmente in formato PAdES (file .pdf) e non CAdES (file .p7m).

AO AL Azienda Ospedaliera di ALESSANDRIA Santi Antonio e Biagio e Cesare Arrigo

Via Venezia, 16 – 15121 ALESSANDRIA
Tel . 0131 206111 – www.ospedale.al.it
info@ospedale.al.it
asoalessandria@pec.ospedale.al.it (solo certificata)
C.F. – P.I. 01640560064

S.C. Area I.C.T.
Direttore f.f.: ing. Ricci Dario

Modulo Consegna HW

Descrizione reparto, ufficio, struttura:_____

Dati referente del reparto, ufficio, struttura:

- Nome e cognome: _____
- Mail:_____ Tel:_____

Con la sottoscrizione di questo modulo si dichiara l'avvenuta consegna da parte del Servizio ICT di

(indicare l'hw consegnato) _____

Cespite/Inventario Ospedaliero: _____

Si dichiara, inoltre, che non saranno violate le vigente norme sulla privacy o le regole Aziendali; si assume la responsabilità su eventuali danni, provocati dal personale che utilizzerà tale bene.

Il presente modulo va necessariamente inviato via mail a help_desk@ospedale.al.it.
La firma può essere autografa oppure digitale[1].

Firma autografa (da inserire solo nel caso in cui il modulo non venga firmato digitalmente)

_____

[1]Con validità a norma del Codice di Amministrazione Digitale (d.lgs 82/2005 e s.m.i.) e preferibilmente in formato PAdES (file .pdf) e non CAdES (file .p7m).

AO AL Azienda Ospedaliera di ALESSANDRIA Santi Antonio e Biagio e Cesare Arrigo

Via Venezia, 16 – 15121 ALESSANDRIA
Tel . 0131 206111 – www.ospedale.al.it
info@ospedale.al.it
asoalessandria@pec.ospedale.al.it (solo certificata)
C.F. – P.I. 01640560064

S.C. Area I.C.T.
Direttore f.f.: ing. Ricci Dario

GESTIONE CHIAVI DI ACCESSO

STRUTTURA RICHIEDENTE

DESCRIZIONE STRUTTURA	
RESPONSABILE DEL TRATTAMENTO (d. LGS 196/2003) – TELEFONO	

Autorizza e richiede ai sensi del D. Lgs 196/2003 e Regolamento (UE) 2016/679:

☐ Apertura
☐ Chiusura Dalla data,

Del profilo di autorizzazione al trattamento dei dati personali e sensibili per:

INCARICATO DELLA GESTIONE (Cognome / Nome / Matricola)

Cognome, Nome e Matricola	
Profilo Professionale & C.F.	

TRATTAMENTO

☐ Accesso alla rete Aziendale	☐ TRAK– Accettazione-Spedalità	☐ AREAS Contabilità
☐ Mail Aziendale	☐ TRAK– Gestione Reparto	☐ AREAS Magazzino
☐ Lapis Delibere/Determine	☐ TRAK– Ufficio Anagrafe	☐ AREAS Richieste
☐ Lapis Protocollo Centrale	☐ TRAK– Prenotazione	CENTRI DI COSTO
☐ Utente VPN	☐ TRAK– Pronto Soccorso	☐ AREAS Modulo File F
	☐ TRAK– Blocco Operatorio	
	MATRICOLA AZIENDALE	

Alessandria li,

Inviare dalla mail del Responsabile del Servizio

Invio Richiesta

AO AL Azienda Ospedaliera di ALESSANDRIA Santi Antonio e Biagio e Cesare Arrigo

Via Venezia, 16 – 15121 ALESSANDRIA
Tel . 0131 206111 – www.ospedale.al.it
info@ospedale.al.it
asoalessandria@pec.ospedale.al.it (solo certificata)
C.F. – P.I. 01640560064

S.C. Area I.C.T.

Direttore f.f.: ing. Ricci Dario

Richiesta accesso VPN

Il modulo compilato in tutte le sue parti permette di ottenere l'accesso VPN alla rete dell'AO AL e le credenziali per accedere ai server, pdl, vnc, ecc.

Verranno restituiti:

- istruzioni per download ed installazione client VPN;
- utente e password;
- OTP (uno ad ogni collegamento dopo aver inserito le credenziali, sarà inviato alla mail indicata nell'apposito elenco da allegare a questo modulo).

Il presente modulo va necessariamente inviato via mail ad help_desk@ospedale.al.it.
La firma può essere autografa oppure digitale[1].

Insieme al modulo vanno allegati anche i seguenti documenti:

- una fotocopia di un documento di identità del responsabile legale della ditta o suo delegato/rappresentante (vedi ad esempio il PM del progetto);
- l'elenco personale per cui è richiesto l'accesso comprensivo di nome, cognome, codice fiscale, indirizzo e-mail, eventuale richiesta utente active directory per accedere ai server e/o richiesta utente per accesso alle pdl;
- l'elenco indirizzi IP e porte a cui si deve accedere.

Numero determina/delibera di aggiudicazione della gara o del contratto di manutenzione:_____

Ragione sociale:_____

Dati referente del progetto/contratto:

- Nome e cognome: _____
- Mail:_____ Tel:_____

Sottoscrivendo questo modulo si dichiara che l'accesso sarà usato ai soli fini di manutenzione preventivamente accordata e che non saranno violate le vigenti normative sulla privacy o le regole Aziendali. Inoltre viene assunta la responsabilità su eventuali danni, provocati dal personale che utilizzerà tale accesso, ai sistemi dell'Azienda Ospedaliera di Alessandria.

Firma autografa e Timbro (da inserire solo nel caso in cui il modulo non venga firmato digitalmente)

_____

[1]Con validità a norma del Codice di Amministrazione Digitale (d.lgs 82/2005 e s.m.i.) e preferibilmente in formato PAdES (file .pdf) e non CAdES (file .p7m).