1.1

06.12.2024

ASP TRAPANI
AZIENDA SANITARIA PROVINCIALE

REGOLAMENTO
Regolamento aziendale per l'utilizzo dei sistemi e degli strumenti informatici e telematici in sicurezza

Struttura: Servizio Informatico Aziendale – ICT
Direttore: Dott. Maurizio Bruno

Revisione	Data	Autore	Approvato da
1.1	06.12.2024	DPO – Dott. Giampaolo Rachini	Direttore U.O.C. ICT Dott. Maurizio Bruno

Maurizio Bruno
08.01.2025
16:06:16
GMT+02:00

Sommario

VIA MAZZINI, 1 – 91100 TRAPANI
TEL.(0923) 805111 - FAX (0923) 873745
Codice Fiscale – P. IVA 02363280815

Art. 1 - PREMESSA E NORMATIVA DI RIFERIMENTO

Le risorse informatiche costituiscono uno strumento di lavoro ormai indispensabile che le amministrazioni pubbliche e private mettono a disposizione del proprio personale ed è necessario pertanto chiarire che, 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.

Per tutelarsi l'ASP di Trapani, al fine di ridurre il livello di rischio e la probabilità che questo si verifichi con conseguenti possibili danni patrimoniali, anche di immagine, adotta il presente regolamento interno che detta le condizioni di utilizzo delle risorse informatiche e dei dispositivi fissi e mobili (personal computer, smartphone, tablet, etc.), messi a disposizione del personale dipendente, al fine di evitare che i dipendenti abbiano comportamenti inconsapevoli che possano innescare problemi o minacce alla sicurezza informatica e al trattamento dei dati.

È un onere dell'Azienda assicurare la funzionalità degli strumenti messi a disposizione, definendone il corretto utilizzo ed adottando tutte le misure necessarie a garantire sicurezza, disponibilità ed integrità dei sistemi informativi, nel pieno rispetto delle normative di riferimento, ovvero:

- ✓ Normativa in materia di tutela dei dati personali Regolamento EU 2016/679 ed in particolare agli Artt. 29, 32 che prescrivono al Titolare del trattamento di istruire gli Addetti al trattamento e applicare le misure di sicurezza necessarie alla tutela dei dati personali;
- ✓ Decreto Legislativo 196/2003 (Codice in materia di protezione dei dati personali) e s.m.i. – Codice della privacy;
- ✓ Provvedimento del Garante per la Protezione dei Dati Personali del 01.03.2007 n. 58 (Linee guida per posta elettronica e internet);
- ✓ Provvedimenti del Garante per la protezione dei dati personali in materia di misure di sicurezza, in particolare con riguardo agli Amministratori di Sistema (Provvedimento generale del 27 novembre 2008 e s.m.i.);
- ✓ Direttiva n. 2 del 26 maggio 2009 della Presidenza del Consiglio dei Ministri – Dipartimento Funzione Pubblica, per l'Utilizzo di Internet e della casella di posta elettronica istituzionale sul luogo di lavoro;
- ✓ Agid - Regole tecniche del servizio di trasmissione di documenti informatici mediante posta elettronica certificata;
- ✓ Legge 20.05.1970 n. 300 (Statuto dei Lavoratori) e ss.mm.ii.;
- ✓ Legge del 22 maggio 2017, n.81, modificata dalla Direttiva della Presidenza del Consiglio dei Ministri del 29/12/2023 (lavoro agile);
- ✓ D. Lgs. 7.03.2005 n. 82 - Codice per l'Amministrazione Digitale – Gazzetta Ufficiale 16 maggio 2005 n. 112 S.O.
- ✓ Titolo IV del D.Lgs. 165/2001 e ss.mm.e ii.
- ✓ C.C.N.L. Personale Area Sanità 2019/2021 del 23/01/2024
- ✓ C.C.N.L. Personale Area Funzioni Locali 2019/2021 del 16/07/2024
- ✓ C.C.N.L. Personale Comparto Sanità 2016/2018 del 21/05/2018 e C.C.N.L. 2019/2021 del 02/11/2022

Il presente Regolamento sarà facilmente disponibile per la consultazione ai dipendenti sul sito web aziendale nella sezione regolamenti ed al seguente link: Ufficio Privacy - ASPTrapani.it - portale dei servizi on-line ASP 9 di Trapani

Art. 2 - CAMPO DI APPLICAZIONE

Il presente disciplinare interno si applica ad ogni dipendente assegnatario di beni e risorse informatiche ovvero utilizzatore di servizi e risorse informative di pertinenza della Azienza Sanitaria senza distinzione di ruolo e/o livello, che nel documento verrà indicato come "Utente".

Per Utente si intende, pertanto, a titolo esemplificativo e non esaustivo, ogni dipendente, collaboratore (interno o esterno), consulente, fornitore e/o terzo che in modo continuativo e non occasionale operi all'interno della struttura utilizzandone beni e servizi informatici.

Per Ente si intende, invece, l'organizzazione e/o comunque il Titolare dei beni e dei dati ivi disciplinate, il quale

VIA MAZZINI, 1 – 91100 TRAPANI
TEL.(0923) 805111 - FAX (0923) 873745
Codice Fiscale – P. IVA 02363280815

opererà per mezzo dei soggetti che ne possiedono la rappresentanza.

Art. 3 - TITOLARITÁ DEI DATI E DEGLI STRUMENTI INFORMATIVI

Gli strumenti informatici oggetto del presente Regolamento sono gli apparati ed i servizi di proprietà (o affidati in uso) dell'ASP di Trapani, messi a disposizione degli Utenti per svolgere quotidianamente il proprio lavoro: i PC, sia fissi sia portatili, gli smartphone, la connessione ad Internet e gli strumenti di scambio di comunicazioni e file, la posta elettronica e la posta elettronica certificata, i programmi e gli applicativi in uso a tutti i dipendenti-utenti, e qualunque altro strumento riconducibile ad attività informatica quali portali web, piattaforme e applicativi in atto disponibili.

Attenersi alle regole descritte in questo documento è un preciso obbligo dell'Utente che utilizza gli strumenti informatici che gli sono stati assegnati e dei Responsabili degli uffici e dei settori che devono verificare la corretta e puntuale messa in pratica delle disposizioni di cui al presente Regolamento, al fine di garantire la riservatezza, l'integrità e la disponibilità dei dati.

Le impostazioni dei dispositivi informatici sono predisposte dagli addetti informatici dell'ICT sulla base di criteri conformi al regolamento aziendale in funzione della qualifica dell'Utente, delle mansioni cui questi è adibito, nonché delle decisioni e della politica di utilizzo di tali strumenti stabiliti dall'Azienda stessa.

Art. 4 - RESPONSABILITÀ PERSONALE DELL' UTENTE

Ogni Utente è personalmente responsabile dell'utilizzo dei beni e delle risorse informatiche affidatigli dall'Azienda Sanitaria nonché dei relativi dati trattati per finalità istituzionali. A tal fine ogni Utente, nel rispetto dei principi di diligenza sottesi al rapporto instaurato con l'ASP di Trapani, è tenuto a tutelare (per quanto di propria competenza) il patrimonio da utilizzi impropri e non autorizzati, danni o abusi anche derivanti da negligenza, imprudenza o imperizia.

L'obiettivo è quello di preservare l'integrità e la riservatezza dei beni, delle informazioni e delle risorse.

Ogni Utente, pertanto, è tenuto, in relazioni al proprio ruolo e alle mansioni in concreto svolte, ad operare a tutela della sicurezza informatica, riportando al proprio responsabile e senza ritardo eventuali rischi di cui è a conoscenza ovvero violazioni del presente disciplinare interno.

Sono vietati comportamenti che possano creare un danno, anche di immagine, all'ASP di Trapani.

Art. 5 - I CONTROLLI

L'ASP di Trapani, in linea con quanto prescritto dall'ordinamento giuridico italiano (art. 4, Statuto dei Lavoratori), esclude la configurabilità di forme di controllo aventi direttamente ad oggetto l'attività lavorativa dell'Utente.

Tuttavia non si esclude che, per ragioni organizzative e produttive ovvero per esigenze dettate dalla sicurezza del lavoro, si utilizzino sistemi informatici, impianti o apparecchiature dai quali derivi la possibilità di controllo a distanza dell'attività dei lavoratori (per esempio videosorveglianza).

In tali casi, infatti, sarà onere dell'Azienda Sanitaria, sottoporre tali forme di controllo all'accordo con le rappresentanze sindacali.

In difetto di accordo, su istanza dell'ASP di Trapani, provvede l'Ispettorato del lavoro, dettando, ove occorra, le modalità per l'uso di tali impianti.

I controlli posti in essere, pertanto, saranno sempre tali da evitare ingiustificate interferenze con i diritti e le libertà fondamentali dei lavoratori e non saranno costanti, prolungati e indiscriminati.

Art. 6 - AMMINISTRATORI DI SISTEMA

L'ASP di Trapani può identificare, in base al perimetro tecnologico effettivamente ricoperto, diversi Amministratori di sistema ai quali conferire il compito di sovrintendere i beni e le risorse informatiche.

VIA MAZZINI, 1 – 91100 TRAPANI
TEL.(0923) 805111 - FAX (0923) 873745
Codice Fiscale – P. IVA 02363280815

Compiti degli Amministratori di sistema sono (a titolo esemplificativo e non esaustivo):

1) gestire l'hardware e il software di tutta la strumentazione informatica di appartenenza dell'Azienda;
2) gestire la creazione, l'attivazione, la disattivazione, e tutte le relative attività amministrative degli account di rete e dei relativi privilegi di accesso alle risorse, previamente assegnati agli utenti;
3) monitorare il corretto utilizzo delle risorse di rete, dei computer e degli applicativi affidati agli utenti, purché attività rientranti nelle normali attività di manutenzione, gestione della sicurezza, e della protezione dei dati;
4) creare, modificare, rimuovere o utilizzare qualunque account o privilegio purché attività rientranti nelle normali attività di manutenzione, gestione della sicurezza, e della protezione dei dati;
5) rimuovere software e/o componenti hardware dalle risorse informatiche assegnate agli utenti, purché attività rientranti nelle normali attività di manutenzione, gestione della sicurezza, e della protezione dei dati;
6) provvedere alla sicurezza informatica dei sistemi informativi, nel rispetto di quanto prescritto dall'art. 32 RGDP;
7) utilizzare le credenziali di accesso di amministratore del sistema per accedere, anche da remoto, ai dati o alle applicazioni presenti su una risorsa informatica assegnata ad un Utente in caso di prolungata assenza, non rintracciabilità o impedimento dello stesso. Tale attività, deve essere limitata al tempo strettamente necessario al compimento delle attività indifferibili per cui è stato richiesto.

Possono essere nominati Amministratori di sistema anche i fornitori di servizi che, per la natura del servizio stesso, possono essere identificati in questo ruolo. La loro designazione avverrà contestualmente alla designazione di responsabile del trattamento ai sensi dell'art. 28 del GDPR.

L'Amministratore di Sistema, sia interno che esterno, ha il compito di effettuare attività di monitoraggio e controllo, segnalare eventuali comportamenti non conformi, effettuare verifiche tecniche secondo le modalità che verranno di seguito indicate.

L'attività di monitoraggio e di controllo è finalizzata esclusivamente a prevenire i rischi descritti in precedenza e pertanto non ha alcuna finalità volta a controllare i lavoratori sul posto di lavoro.

Art. 7 - REGOLE GENERALI

Il sistema informativo aziendale è composto da un insieme di unità server centrali e macchine client connessi ad una rete locale (LAN), che utilizzano diversi sistemi operativi e applicativi. Il computer consegnato al collaboratore è uno strumento di lavoro e contiene tutti i software necessari a svolgere le attività affidate. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, rallentamenti del sistema, costi di manutenzione e, soprattutto, minacce alla sicurezza. L'accesso al PC è protetto da password che deve essere custodita dall'utente con la massima diligenza e non divulgata. Il computer che viene consegnato contiene tutti i software necessari a svolgere le attività affidate dall' Azienda.

Per necessità aziendali, l'amministratore di sistema, utilizzando le proprie credenziali di amministratore, può accedere, con le regole indicate nel presente documento, sia alle memorie di massa locali di rete (repository e backup) che ai server aziendali nonché al computer dell'Utente, anche in remoto.

Art. 8 - ISTRUZIONI SPECIFICHE PER TUTTI GLI AUTORIZZATI AL TRATTAMENTO DEI DATI PER IL CORRETTO USO E LA SICUREZZA DEGLI STRUMENTI AZIENDALI. UTILIZZO DEL PERSONAL COMPUTER IN DOTAZIONE

Il Personal Computer affidato al dipendente è uno **strumento di lavoro**. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.

Durante le missioni di lavoro, quando è necessario portare il notebook, questo deve essere portato come bagaglio a mano, evitando di trasportare in borsa i codici identificativi e le parole chiave di sicurezza per la privacy, nonché i supporti di memorizzazione con le copie di back-up.

Non è consentito l'uso di programmi diversi da quelli distribuiti ed installati ufficialmente dal *Responsabile dei sistemi informatici.* L'inosservanza di questa disposizione, infatti, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre l'azienda a gravi responsabilità civili ed anche penali in caso di

VIA MAZZINI, 1 – 91100 TRAPANI
TEL.(0923) 805111 - FAX (0923) 873745
Codice Fiscale – P. IVA 02363280815

violazione 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.

Non è consentito all'utente modificare le caratteristiche impostate sul proprio PC, salvo autorizzazione esplicita del *Responsabile dei sistemi informatici aziendali*.

Il Personal Computer deve essere spento prima di lasciare gli uffici o in caso di assenze prolungate. In ogni caso lasciare un PC incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso. In ogni caso deve essere attivato lo screen saver e la relativa password.

Non è consentita l'installazione sul proprio PC di alcun dispositivo di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, ecc.), se non con l'autorizzazione espressa del *Responsabile dei sistemi informatici aziendali.*

Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il *Responsabile dei sistemi informatici aziendali* nel caso in cui vengano rilevati virus.

Nel personal computer **non devono essere presenti file personali**, quali ad esempio fotografie, file musicali, file video, file di attività extra lavorative. Durante le operazioni di cambio / sostituzione del personal computer (ammodernamento del parco macchine), il tecnico addetto alla sostituzione rimuoverà, se presenti, tutti i file non inerenti all'attività lavorativa.

Il **personale incaricato, anche dei servizi esternalizzati**, che opera presso i Sistemi Informativi **è autorizzato a compiere interventi nel sistema informatico aziendale** diretti a garantire la sicurezza e la salvaguardia del sistema stesso, nonché per ulteriori motivi tecnici e/o manutentivi (quali aggiornamento, sostituzione, implementazione di programmi, manutenzione hardware). Detti interventi potranno comportare l'accesso in qualunque momento ai dati trattati da ciascun utente, ivi compresi gli archivi di posta elettronica, nonché alla verifica sui siti Internet visitati dagli utenti abilitati alla navigazione esterna. Analogamente, sempre ai fini di sicurezza del sistema e per garantire la corretta operatività delle attività istituzionali, si procede in caso di assenza prolungata od impedimento dell'utente.

Il personale incaricato del servizio di assistenza ai Sistemi Informativi e dei **servizi affidati in outsourcing è autorizzato a collegarsi e visualizzare in remoto** -previa autorizzazione da parte del personale che opera presso i sistemi informativi, e previa comunicazione all'utente – i client al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza contro virus, spyware, malware, e simili. L'intervento viene effettuato esclusivamente su chiamata dell'utente o, in caso di oggettiva necessità, a seguito della rilevazione tecnica di problemi nel sistema informatico e telematico. In quest'ultimo caso, fatta salva l'urgenza di procedere per non pregiudicare l'efficacia dell'intervento, verrà data comunicazione della necessità dell'intervento stesso.

È assolutamente vietato: effettuare in proprio attività manutentive, o permettere attività manutentive da parte dei soggetti non espressamente autorizzati dell'Azienda; utilizzare il personal computer non in dotazione; lasciare incustodito un notebook aziendale in ufficio o in viaggio (particolare attenzione deve essere riposta quando si viaggia sui mezzi pubblici).

Il Responsabile della sicurezza informatica qualora rilevi, nell'esercizio della sua funzione, l'utilizzo improprio da parte del dipendente del personal computer in dotazione (anche notebook), dovrà predisporre apposita relazione in merito e proporre al Direttore, ove presta servizio il predetto dipendente, che venga attivato il consequenziale provvedimento disciplinare.

Art. 9 - GESTIONE CREDENZIALI DI AUTENTICAZIONE E PASSWORD

L'utilizzo del computer e delle procedure informatiche è protetto da credenziali di accesso (username e password) che costituiscono l'Account istituzionale.

Il responsabile informatico, assegna a ciascun Autorizzato (Utente), uno username come chiave di accesso riconducibile ad una singola persona. Le chiavi di accesso possono coincidere per lo stesso utente su diversi sistemi. Le credenziali devono essere revocate alla chiusura del rapporto tra l'utente e l'Azienda Sanitaria.

Pertanto, qualunque **Utente, al momento in cui dovesse cessare il rapporto di lavoro con l'Azienda (collocamento in quiescenza, trasferimento, etc.) è obbligato a darne comunicazione all'ICT per la chiusura dei propri**

VIA MAZZINI, 1 – 91100 TRAPANI
TEL.(0923) 805111 - FAX (0923) 873745
Codice Fiscale – P. IVA 02363280815

account, attraverso email all'indirizzo maurizio.bruno@asptrapami.it
L'utente a cui viene assegnato per la prima volta uno username, riceve anche una password temporanea che dovrà modificare alla prima connessione. La password è il codice che rende "personale" la chiave, garantendone la riservatezza. La robustezza e segretezza delle password sono meccanismi fondamentali per la protezione di buona parte dei sistemi. Pertanto, la scelta della propria password deve rispondere ai seguenti **requisiti minimi**:
a) **Lunghezza**: dovrà avere una lunghezza minima di 8 caratteri alfanumerici (lettere e numeri) ed almeno due caratteri speciali e lettere maiuscole e minuscole;
b) **Complessità**: non deve contenere riferimenti agevolmente riconducibili al proprietario della stessa (es. data di nascita, nome dei figli, nome utente, etc.) e deve essere generata preferibilmente senza un significato compiuto;
c) **Ripetitività**: non potrà essere riutilizzata. Alla scadenza dovrà sempre essere impostata una password diversa da quelle impostate precedentemente;
d) **Scadenza**: la password assegnata deve essere prontamente sostituita al primo utilizzo e deve essere modificata con cadenza trimestrale.
Le password non utilizzate da almeno sei mesi verranno disattivate, come nel caso di perdita della qualità che consente all'Autorizzato (Utente) l'accesso (es. trasferimento, pensionamento, etc.).
La password individuale deve essere riservata. L'utente, al riguardo, deve mantenere i seguenti accorgimenti:

- non trascrivere la password su pezzi di carta o post-it lasciati in vista sulla scrivania, o attaccati al monitor;
- non comunicare a nessuno la propria password;
- non condividere con nessuno la propria password;
- assicurarsi che nessuno guardi la tastiera con l'intenzione di memorizzare la password, mentre la si digita;
- non inviare la password tramite e-mail e, se proprio è necessario comunicarla, farlo a voce, per telefono o a mano in una busta chiusa;
- non utilizzare la stessa password per più scopi o procedure informatiche;
- non utilizzare la funzione di memorizzazione automatica delle password inclusa nei vari browser;

Art. 10 - SUPPORTI DI MEMORIZZAZIONE

1) se possibile, archiviare sempre i dati e tutti i documenti elettronici (word, excel, access…) utilizzati per effettuare trattamenti di dati personali sul server centrale di rete ed eliminarli dall'hard disk del personal computer in dotazione. Questa misura di sicurezza per la privacy permette di proteggere con maggiore efficacia l'accesso ai dati da persone non autorizzate.
2) non salvare informazioni di natura particolare su supporti rimovibili (es. CD, DVD, pen drive, ecc.) salvo che non ne sia consentita la crittografia degli stessi. In ogni caso devono essere conservati in strutture chiuse a chiave e mai lasciati incustoditi;
2) se non più utilizzati, i supporti rimovibili contenenti dati particolari o giudiziari devono essere distrutti;
3) nel caso di utilizzo di pen drive, per la memorizzazione di dati, fare attenzione a disinserire le chiavi dalle porte USB seguendo la procedura di disconnessione sicura;
4) i supporti rimovibili non vanno mai ceduti a terzi; nel caso in cui sono consegnate a terzi per trasferire dati, assicurarsi che sui supporti di memorizzazione siano presenti solamente i dati necessari da trasferire, ovvero effettuare personalmente l'operazione di trasferimento, evitando di consegnare i supporti stessi a terzi, che potrebbero copiare le informazioni personali memorizzate;
5) eliminare documenti cartacei e dai supporti di memorizzazione in maniera sicura, evitando di gettarli nel cestino della spazzatura, senza averli previamente resi inutilizzabili utilizzando gli idonei distruggi documenti o averli distrutti in maniera appropriata dal supporto di memorizzazione informatico;
6) accertarsi che le informazioni non più utili vengano cancellate in modo sicuro dai supporti di dati e non conservare inutilmente messaggi di posta elettronica.

VIA MAZZINI, 1 – 91100 TRAPANI
TEL.(0923) 805111 - FAX (0923) 873745
Codice Fiscale – P. IVA 02363280815

Art. 11 - VIRUS

I virus possono alterare o addirittura distruggere i dati e i programmi; sono diffusi via internet sono spesso camuffati da programmi di utilità o di intrattenimento.
Pertanto ogni Utente deve tenere comportamenti tali da ridurre il rischio di attacchi al sistema informatico aziendale mediante virus, malware, phishing o altro, seguendo le seguenti best practice:
1) ogni computer è protetto da idonei strumenti per il rischio di attività di virus informatici;
2) lo strumento di protezione (di norma software antivirus) è abilitato;
3) è vietato disattivare, senza autorizzazione, il software antivirus;
4) la posta elettronica viene filtrata in entrata da un apposito prodotto antivirus che pulisce gli eventuali allegati contenenti virus. Evitare di aprire messaggi provenienti da mittenti sconosciuti o sospetti e cancellarli immediatamente;
5) nel caso di utilizzo di supporti di memorizzazione esterni, controllare sempre che i file memorizzati non siano infettati da virus attraverso la scansione del supporto;
6) controllare periodicamente la presenza di virus sul personal computer in dotazione mediante la scansione dell'intero sistema.
Qualsiasi malfunzionamento o segno sospetto dovranno essere segnalati prontamente all'ICT.

Art. 12 - SOFTWARE

Alle misure di sicurezza informatiche operate centralmente si richiede l'applicazione delle seguenti misure di sicurezza per le postazioni locali:
1) sul computer in dotazione può essere utilizzato solamente il software fornito dall'azienda;
2) non si possono installare software e applicazioni sul personal computer in dotazione senza una specifica autorizzazione da parte dell'Azienda ed il presidio di un tecnico del servizio informatico aziendale;
3) non creare e non utilizzare software senza licenza d'uso, è consentito unicamente l'utilizzo di software ufficialmente acquisiti ed inventariati dall'azienda.
4) provvedere al salvataggio (backup) degli archivi e documenti elettronici esistenti localmente sul personal computer con frequenza almeno settimanale;
5) adottare, relativamente all'accesso ai locali ove sono conservati i dati ed effettuati i trattamenti, misure di sicurezza per la privacy analoghe a quelle descritte per i trattamenti effettuati su supporto cartaceo (es. impedire l'accesso ai personal computer chiudendo a chiave le stanze negli intervalli di non utilizzo e/o assicurando la vigilanza del personale di reparto).

Art. 13 - USO DELLA POSTA ELETTRONICA DELLA RETE INTERNET E DEI RELATIVI SERVIZI

La casella di posta elettronica assegnata dall'Azienda all'utente ed il PC abilitato alla navigazione in Internet sono strumenti di lavoro, ogni utilizzo non inerente all'attività lavorativa può determinare un livello di sicurezza non adeguato oltre a disservizi e costi di manutenzione. Le persone assegnatarie delle caselle di posta elettronica e della rete Internet sono responsabili del corretto utilizzo delle stesse. L'utilizzo di caselle di posta elettronica personale è di norma evitato per attività o comunicazioni afferenti il servizio, salvi i casi di forza maggiore dovuti a circostanze in cui il dipendente, per qualsiasi ragione, non possa accedere all'account istituzionale.
La posta elettronica è uno strumento messo a disposizione esclusivamente per motivi di lavoro ai dipendenti (e collaboratori) individuati, nel rispetto degli obblighi derivanti dalle norme di legge e dalle clausole contrattuali che disciplinano il rapporto di lavoro.
Gli Utenti, assegnatari delle caselle di posta elettronica, sono responsabili del corretto utilizzo delle stesse e devono

VIA MAZZINI, 1 – 91100 TRAPANI
TEL.(0923) 805111 - FAX (0923) 873745
Codice Fiscale – P. IVA 02363280815

mantenerle in ordine, cancellando documenti inutili e soprattutto allegati ingombranti. Si raccomanda di cancellare periodicamente le mail ricevute e inviate non necessarie e svuotare il cestino con le mail eliminate.
Le comunicazioni via posta elettronica devono avere un contenuto che rispetti la normativa vigente. Le comunicazioni in uscita, devono essere firmate inserendo sempre il proprio nome e cognome, servizio di appartenenza, nome dell'Azienda, recapito telefonico e, se ritenuto utile, anche un indirizzo e-mail alternativo.
Quando si inviano email a più destinatari contemporaneamente ed è opportuno non rendere nota la loro identità agli altri utenti, gli indirizzi dei destinatari andranno inseriti nel campo CCN, ossia Copia per Conoscenza Nascosta.
L'Utente che si assenta per lunghi periodi (e.g. ferie) deve provvedere ad attivare l'opzione "Assente o Fuori sede" in cui indicare chi contattare in sua assenza.
Nei casi di assenza non programmata o impossibilità, temporanea o protratta nel tempo, se non è possibile attivare la procedura sopra citata, ove ritenuto necessario dal Responsabile della Struttura per garantire l'ordinaria operatività aziendale, l'utente deve delegare per iscritto, ad un collega il compito di verificare il contenuto di messaggi e di inoltrare al Responsabile quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa.
Qualora l'utente non abbia delegato un collega, il Responsabile della Struttura cui afferisce il dipendente, ove ritenuto necessario, può richiedere all'ICT di accedere alla casella di posta elettronica del dipendente-utente assente, in modo da prendere visione dei messaggi di posta. In questo caso il Responsabile della Struttura deve informare l'utente appena possibile, fornendo adeguata spiegazione e formalizzando quanto avvenuto.
La stessa procedura deve essere attuata qualora, per garantire l'ordinaria operatività aziendale, sia necessario accedere a informazioni o documenti di lavoro presenti sul PC dell'utente assente.
Nel caso in cui si debba inviare un documento in allegato alla mail è preferibile utilizzare un formato di scrittura accessibile (ad esempio il formato Acrobat *.pdf). Nel caso di invio di allegati "pesanti" (superiori a 25 MB) si possono utilizzare i formati compressi.
È onere del dipendente assegnatario della casella di posta dover effettuare un attento monitoraggio della stessa in quanto le comunicazioni via mail assumono formale carattere istituzionale. È vietato utilizzare indirizzi e-mail non istituzionali per trasmettere messaggi connessi alla propria attività istituzionale.
Nel caso di mittenti sconosciuti e sospetti o messaggi insoliti, per non correre il rischio di essere infettati da virus, occorrerà cancellare i messaggi senza aprirli o chiedere assistenza all'ICT. Analogamente, messaggi provenienti da mittenti conosciuti che contengono allegati sospetti (file con estensione .exe .scr .pif .bat .cmd) non devono essere aperti.
L'iscrizione a "mailing list" esterne è concessa solo per motivi professionali. Prima di iscriversi occorre accertarsi in anticipo se il sito sia affidabile. È invece vietato l'utilizzo dell'indirizzo mail aziendale per l'iscrizione a qualsiasi servizio on line (social network, gruppi di discussione, servizi telefonici, bancari, assicurativi di tipo personale etc.) che non sia correlato alla propria attività istituzionale.
Occorre prestare estrema attenzione alle mail di phishing ovvero quel genere di truffa telematica che ha l'obiettivo di sottrarre informazioni e dati personali in maniera fraudolenta. Il mittente del messaggio sembra di norma un'organizzazione attendibile, come la banca o la posta. Il testo ci avvisa che c'è un problema relativo al nostro account, in genere legato alla sicurezza o che è necessario un aggiornamento delle credenziali. Si invita solitamente a cliccare su un link che, però, riporta a un sito fittizio controllato dal cracker. Difficile accorgersi della differenza, dato che la pagina riproduce fedelmente il portale dell'istituto bancario o della posta. Così si è indotti a inserire i propri dati, che vengono in tal modo resi noti e il nostro dispositivo può al tempo stesso essere infettato da virus e malware. In questi casi occorre sempre rivolgersi all'ICT per qualsiasi dubbio o informazioni nel merito.
È possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario.
In ogni caso si chiede di verificare sempre il mittente di ogni email e in caso di email sospetta contattare l'ICT. Qualora anche per errore sia stata già aperta la email, evitare di aprire allegati con formati .exe.
I messaggi di posta elettronica aziendale devono contenere un avvertimento ai destinatari del seguente tenore letterale:

VIA MAZZINI, 1 – 91100 TRAPANI
TEL.(0923) 805111 - FAX (0923) 873745
Codice Fiscale – P. IVA 02363280815

RISERVATEZZA

Le informazioni trasmesse possono contenere documenti confidenziali e/o materiale riservato; sono quindi da intendersi esclusivamente ad uso della persona e/o società a cui sono indirizzate. Qualsiasi modifica, inoltro, diffusione o altro utilizzo, relativo alle informazioni trasmesse, da parte di persone e/o società diversi dai destinatari indicati, è proibito ai sensi del Regolamento Europeo n.2016/679 e della normativa nazionale di coordinamento. Qualora questa mail fosse stata ricevuta per errore, si prega di contattare il mittente e cancellarne il contenuto.

PRIVACY

The information transmitted may contain confidential document and/or private matter; they are therefore intended exclusively for the use of the person and/or company to which they are addressed. Any change, forwarding, diffusion or any other utilization related to the information provided by persons and/or companies different than the indicated recipients is forbidden according to the European Regulation n. 2016/679 and by the local law of privacy regulation. If this e-mail was received by mistake, please contact the sender and delete the content.

Art. 14 - PEC

La posta elettronica certificata (PEC) è un sistema di trasmissione sicuro e regolamentato dalla legge, per inviare documenti e messaggi di posta elettronica con valore legale. Viene istituita come versione digitale della raccomandata con ricevuta di ritorno e punta a rendere più agili, immediati ed economici, tutti gli scambi di informazioni tra i soggetti interessati, sfruttando le potenzialità del digitale.
La PEC è stata introdotta con il DPR 11 febbraio 2005, n. 68 "Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della legge 16 gennaio 2003, n. 3" (G.U. 28 marzo 2005, n. 97) in cui vengono emanate le regole per l'utilizzo della PEC e viene stabilito, tramite l'Art. 4 comma 1, che la PEC consente l'invio di messaggi la cui trasmissione è valida agli effetti di legge. Il suo utilizzo è regolamentato anche dal CAD (Codice dell'Amministrazione digitale) all'art. 6 e ss.mm.ii. Sempre nel CAD l'Art. 47 indica che le comunicazioni di documenti tra le pubbliche amministrazioni avvengono tramite l'utilizzo della posta elettronica e sono valide ai fini del procedimento amministrativo una volta che ne sia verificata la provenienza. A questo fine le comunicazioni sono valide se: sono sottoscritte con firma digitale o altra firma elettronica qualificata, sono dotate di segnatura di protocollo ovvero sono trasmesse attraverso sistemi di posta elettronica certificata. L'Art 48 del CAD indica che la trasmissione telematica di comunicazioni che necessitano di una ricevuta di invio e di una ricevuta di consegna avviene mediante la posta elettronica certificata.
La PEC ha dunque lo stesso valore legale di una raccomandata tradizionale con avviso di ricevimento. Per certificare l'invio e la ricezione di un messaggio di PEC, il gestore di posta invia al mittente una ricevuta che costituisce prova legale dell'avvenuta spedizione del messaggio e dell'eventuale documentazione allegata. Allo stesso modo, il gestore invia al mittente la ricevuta di avvenuta (o mancata) consegna del messaggio, con precisa indicazione temporale. Il personale che ha in uso tale tipo di posta elettronica, sia che si tratti di un indirizzo individuale o legato ad un determinato settore/ufficio/funzione, deve rispettare e attenersi alla riportata normativa.

Art. 15 - INVIO DOCUMENTAZIONE PER EMAIL, CONTENENTE DATI PERSONALI E/O PARTICOLARI

Qualsiasi comunicazione e/o documentazione contenente dati personali e/o particolari, deve essere inoltrata tramite email istituzionale personale o della U.O. di riferimento.
Non inviare email ai pazienti con destinatari multipli indicando gli indirizzi nel campo "A", ma inserire gli indirizzi email a cui inoltrare documenti e comunicazioni su "Ccn" (copia conoscenza nascosta), in questa maniera tutti gli

VIA MAZZINI, 1 – 91100 TRAPANI
TEL.(0923) 805111 - FAX (0923) 873745
Codice Fiscale – P. IVA 02363280815

indirizzi email inclusi nel campo CCN vengono mantenuti nascosti gli uni agli altri.

Art. 16 - INTERNET

La rete Internet è un servizio che viene messo a disposizione dei dipendenti a supporto delle loro attività istituzionali, favorendo la comunicazione verso l'esterno e per il reperimento e la divulgazione di informazioni utili per lo svolgimento della professione. Al dipendente è consentito l'utilizzo degli strumenti informatici forniti dall'amministrazione per poter assolvere all'incombenze personali senza doversi allontanare dalla sede di servizio, purchè l'attività sia contenuta in tempi ristretti e senza alcun pregiudizio per i compiti istituzionali.
È vietato accedere a siti web contenenti materiale pornografico, pedo-pornografico, materiale fraudolento illegale, materiale blasfemo/molesto/osceno.
È, altresì, vietato tentare di violare o aggirare i sistemi di controllo o di protezione dell'uso di Internet e della posta elettronica installati e utilizzati dall'azienda, nel rispetto del diritto alla riservatezza dei dipendenti;
È vietato il download di software gratuiti prelevati da siti Internet, se non espressamente autorizzato dall'ICT, in quanto potenzialmente responsabile di malfunzionamenti e di violazione delle procedure di sicurezza.
È vietato utilizzare l'accesso ad Internet in violazione delle norme in vigore nell'ordinamento giuridico italiano a tutela del diritto d'autore (es. legge 22 aprile 1941, n. 633 e successive modificazioni, d.lgs. 6 maggio 1999, n. 169 e legge 18 agosto 2000, n. 24S). In particolare, è vietato il download di materiale soggetto a copyright (software, testi, immagini, musica, filmati, file in genere).

Art. 17 - RETE DI COMUNICAZIONE

Le unità di rete sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità, vengono svolte regolari attività di controllo, amministrazione e backup.
Le password d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite. È assolutamente proibito entrare nella rete e nei programmi con altri nomi utente.
Il Responsabile dei sistemi informatici aziendali può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la Sicurezza sia sui PC degli incaricati sia sulle unità di rete.
Costituisce buona regola la periodica (almeno ogni sei mesi) pulizia degli archivi, ovviamente nel rispetto del regolamento di conservazione e scarto adottato dall'azienda, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. È infatti assolutamente da evitare un'archiviazione ridondante.
È cura dell'utente effettuare la stampa dei dati solo se strettamente necessaria e di ritirarla prontamente dai vassoi delle stampanti comuni.
È compito di ciascun utente, per quanto di propria competenza e secondo i canoni della diligenza, preservare i dati, le notizie e le informazioni aziendali che circolano nella rete informatica dalla conoscibilità di terzi soggetti non espressamente autorizzati ad averne notizia.
I sistemi di teleassistenza remota sono permessi solo tramite VPN, preventivamente autorizzata dai Sistemi Informativi. Altre modalità potranno essere valutate per i singoli casi

Art. 18 - UTILIZZO DELLA STAMPANTE

La stampa di documentazione contenente dati personali, particolari e giudiziari deve avvenire ad opera degli Autorizzati a trattare tali dati con obbligo di ritirare tempestivamente la documentazione dalla stampante utilizzata.
Il riutilizzo di fogli recanti una stampa su una sola facciata, per esigenze di risparmio e di sensibilità ambientale, deve riguardare esclusivamente supporti nella elusiva disponibilità dell'Autorizzato ed essere utilizzati nell'ambito delle proprie mansioni, evitando di far conoscere a terzi non autorizzati il contenuto dei documenti. Non possono mai essere riciclati fogli sottoscritti o che contengono dati sanitari o estremamente sensibili come per esempio: dati

VIA MAZZINI, 1 – 91100 TRAPANI
TEL.(0923) 805111 - FAX (0923) 873745
Codice Fiscale – P. IVA 02363280815

bancari, fiscali ecc…
I documenti contenenti dati personali e sensibili non più utilizzati e per i quali non è necessaria la conservazione, prima di essere conferiti nella raccolta differenziata, devono essere trattati in modo da rendere non intelligibili a terzi dati personali ivi contenuti, usando eventualmente un dispositivo distruggi documenti.

Art. 19 - UTILIZZO DEI DISPOSITIVI MOBILI

L'assegnazione e l'uso dei dispositivi di telefonia e connettività mobile (cellulari, smartphone, tablet, modem/router, etc.), come quelle dei personal computer, devono rispondere alle disposizioni e alle esigenze dell'Azienda, al fine di migliorare la qualità del lavoro e della produttività, in un quadro di economia, efficacia ed efficienza. I dispositivi possono essere utilizzati come strumento informatico, sia per la gestione della comunicazione, ad esempio a mezzo e-mail, che per la connettività Internet.
I dispositivi mobili saranno attribuiti alle figure aziendali che ne necessitano per l'esercizio della propria mansione.
Riguardo all'uso appropriato dei dispositivi mobili e delle relative utenze intestate all'Azienda dovranno essere rispettate le stesse regole applicate all'utilizzo dei PC, fissi o portatili.
Il dispositivo mobile aziendale può essere utilizzato solo per ragioni di servizio, ed è obbligo di ogni assegnatario farne un uso appropriato ed averne una diligente cura, custodia e conservazione. L'apparecchio affidato al dipendente-utente non può essere dato in uso a colleghi o a terzi.
La scheda SIM aziendale assegnata, come i dispositivi, dovrà essere utilizzata per ragioni di servizio. Pertanto, non è consentito attivare sulla stessa dei servizi in abbonamento o traffico dati per uso personale e/o non autorizzati dall'Azienda.
L'utente assegnatario dovrà inoltre custodire la scheda ove sono riportati i codici PIN e PUK.
Il dispositivo mobile aziendale è dato in uso all'assegnatario che, in analogia a quanto avviene per il personal computer e gli altri dispositivi informatici, ne diventa custode e responsabile del corretto utilizzo nel rispetto del presente regolamento. L'assegnazione dà luogo, in carico al titolare, delle medesime forme di responsabilità patrimoniale previste per i consegnatari di beni dell'amministrazione. Alla consegna del dispositivo mobile aziendale, della relativa SIM card e degli eventuali accessori forniti, l'assegnatario è tenuto, obbligatoriamente, a sottoscrivere le seguenti dichiarazioni:
- presa in consegna del telefono cellulare aziendale e degli eventuali accessori forniti;
- presa in consegna della SIM card aziendale;
- dichiarazione di conoscenza delle disposizioni previste nel presente regolamento.

I dispositivi mobili (telefono cellulare o smartphone) devono essere utilizzati esclusivamente per uso professionale e qualsiasi necessità di utilizzo promiscuo deve essere richiesta e autorizzata.
I dispositivi mobili utilizzati all'esterno (convegni, fiere, visite, ecc.), in caso di allontanamento, devono essere custoditi in un luogo protetto.
In particolare essi non devono mai essere lasciati incustoditi nell'autovettura o altrove.

Art. 20 - DISPOSITIVI DI FIRMA DIGITALE

Ai sensi dell'art. 32, comma 1, del Codice dell'Amministrazione Digitale (CAD) gli Utenti titolari di un dispositivo di firma digitale (smart card o token USB) sono tenuti a "… *assicurare la custodia del dispositivo di firma o degli strumenti di autenticazione informatica per l'utilizzo del dispositivo di firma da remoto, e ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri; è altresì tenuto ad utilizzare personalmente il dispositivo di firma*".
Pertanto, il dispositivo di firma digitale per motivi di sicurezza deve essere custodito con la massima diligenza esclusivamente dall'Utente titolare che è l'unico a poterlo utilizzare. Non deve essere mai lasciato in custodia a terzi.
Il PIN (Personal Identification Number), il codice numerico che consente all'Utente titolare di accedere alle funzioni del dispositivo di firma, è segreto e non deve essere svelato ad altri soggetti.

VIA MAZZINI, 1 – 91100 TRAPANI
TEL.(0923) 805111 - FAX (0923) 873745
Codice Fiscale – P. IVA 02363280815

Art. 21 - VERIFICHE AL TERMINE DEL RAPPORTO DI LAVORO

In caso di cessazione, a vario titolo, del rapporto di lavoro, l'Azienda e l'utente (dipendente, collaboratore ecc…) provvedono alle seguenti operazioni a garanzia del rispetto del principio di correttezza dei trattamenti tra le quali:

- ✓ verifica dei dispositivi informatici per valutare eventuale conservazione o cancellazione di file;
- ✓ restituzione all'Azienda di tutti i dispositivi informatici aziendali affidatigli durante l'attività lavorativa;
- ✓ disattivazione dell'account di posta elettronica dopo un periodo di 30 giorni prolungabili al bisogno, nei quali l'Azienda provvederà a segnalare ai destinatari l'indirizzo alternativo al quale inviare eventuali comunicazioni;
- ✓ archiviazione di eventuali file per i quali non si sia già provveduto alla loro conservazione;
- ✓ formattazione completa dei devices restituiti;
- ✓ conservazione dei dati del lavoratore per il tempo necessario a garantire il rispetto degli obblighi legislativi.

Art. 22 - SANZIONI

L'eventuale violazione di quanto previsto dal presente disciplinare interno, rilevante anche ai sensi degli artt. 2104 e 2105 c.c., potrà comportare l'applicazione di sanzioni disciplinari in base a quanto previsto dal Titolo IV del D.lgs. 165/2001 e ss.mm.e ii. e dai contratti collettivi richiamati all'art.1 del presente regolamento.
L'ASP di Trapani avrà cura di informare senza ritardo (e senza necessità di preventive contestazioni e/o addebiti formali) le autorità competenti, nel caso venga commesso un reato, o la cui commissione sia ritenuta probabile o solo sospettata, tramite l'utilizzo illecito o non conforme dei beni e degli strumenti informatici istituzionali.
Si precisa, infine, che in caso di violazione accertata da parte degli utenti delle regole e degli obblighi esposti in questo disciplinare, l'Azienda Sanitaria di Trapani si riserva la facoltà di sospendere, bloccare o limitare gli accessi di un account, quando appare ragionevolmente necessario per proteggere l'integrità, la sicurezza e/o la funzionalità dei propri beni e strumenti informatici.

Art. 23 - COMUNICAZIONI

Il presente Regolamento sarà facilmente disponibile per la consultazione ai dipendenti sul sito web aziendale nella sezione Regolamenti ed al seguente link: Ufficio Privacy - ASPTrapani.it - portale dei servizi on-line ASP 9 di Trapani.