REGOLAMENTO PER L'UTILIZZO DEGLI STRUMENTI E DEI SERVIZI INFORMATICI E TELEMATICI DELL'ENTE

Indice

Scopo e campo di applicazione del documento

L'obiettivo del presente documento è quello di illustrare le norme di sicurezza conformi alla normativa vigente in tema di trattamento dei dati personali, tutela del diritto d'autore, criminalità informatica e alle migliori prassi in uso, inoltre, ha lo scopo di dettare la procedura per una corretta e adeguata gestione dei sistemi informativi aziendali.

Premessa

Le Pubbliche Amministrazioni si caratterizzano per l'elevato uso della tecnologia informatica che da un lato ha consentito l'introduzione di innovative tecniche di gestione dell'Ente, dall'altro ha dato origine a numerose problematiche relative all'utilizzo degli strumenti informatici forniti al dipendente pubblico per lo svolgimento delle proprie mansioni. Premesso che l'utilizzo delle risorse informatiche e telematiche deve sempre ispirarsi al principio di diligenza e correttezza, nell'ambito di un rapporto di lavoro, l'azienda Sanitaria Locale di Taranto adotta il presente regolamento interno, così come previsto dal GDPR, General Data Protection Regulation – Regolamento UE 2016/679, rivolto ad evitare che comportamenti inconsapevoli possano provocare problemi o minacce per la sicurezza e nel trattamento dei dati.
Con l'entrata in vigore del presente Regolamento tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi abrogate e sostituite dalla presente.
Copia di questo Regolamento è presente e liberamente consultabile all'interno del portale della Intranet Aziendale al link: http://intranet.aslta.local/include/regolamenti.asp
Il presente documento è costituito da 11 capitoli. I primi tre riportano una breve premessa il campo di applicazione e le finalità, nel capitolo quattro un breve cenno alle normative, al capitolo 5 sono descritte le definizioni più usate all'interno del documento, nel capitolo 6 sono descritte tutte le norme di comportamento e le linee di condotta dell'utente illustrando i principi generali che hanno ispirato le policy, i capitoli 7 e 8 descrivono i principi di gestione monitoraggio e controllo da parte dell'Amministrazione mentre il capitolo 9 richiama le disposizioni in materia di privacy aziendale.

1 Finalità e ambito di applicazione del documento

Il presente Regolamento stabilisce le regole di comportamento da adottare nella gestione della sicurezza delle informazioni. Il presente Regolamento disciplina l'accesso e l'utilizzo delle risorse informatiche dell'Amministrazione con l'obiettivo di garantire la Riservatezza, l'Integrità e la Disponibilità delle informazioni

(RID) e descrive inoltre le procedure in essere presso l'Amministrazione. Si applica a tutti i dipendenti, senza distinzione di ruolo e/o livello, nonché a tutti i collaboratori dell'Azienda a prescindere dal rapporto contrattuale con la stessa intrattenuto (lavoratori somministrati, collaboratore a progetto, in stage, ecc.). Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche e telematiche, per **"utente"** deve intendersi ogni dipendente e collaboratore (collaboratore a progetto, in stage, personale convenzionato, ecc.) in possesso di specifiche credenziali di autenticazione.

Il presente Regolamento si applica ai contesti tecnologici attualmente utilizzati dall'Amministrazione così come a quelli futuri.

2 Riferimenti e normative di riferimento

- Legge 20.5.1970, n. 300, recante "Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro e norme sul collocamento"; in particolare l'art. 4, comma 1, della Legge 300/1970, secondo cui la regolamentazione dell'uso degli strumenti informatici non è finalizzata all'esercizio di un controllo a distanza dei lavoratori da parte del datore di lavoro ma solo a permettere a quest'ultimo di utilizzare sistemi informativi per fare fronte ad esigenze produttive od organizzative e di sicurezza nel trattamento dei dati personali;
- Regolamento Europeo 679/16 "General Data Protection Regulation"; in particolare viene garantito al singolo lavoratore il controllo sui propri dati personali secondo quanto previsto dagli articoli 15-16-17-18-20-21-77 del Reg. 2016/679;
- "Linee guida del Garante per posta elettronica e internet" in Gazzetta Ufficiale n. 58 del 10 marzo 2007;
- l'articolo 23 del D.lgs. n. 151/2015 (c.d. Jobs Act) che modifica e rimodula la fattispecie integrante il divieto dei controlli a distanza, nella consapevolezza di dover tener conto, nell'attuale contesto produttivo, oltre agli impianti audiovisivi, anche degli altri strumenti «dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori» e di quelli «utilizzati dal lavoratore per rendere la prestazione lavorativa».
- Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013, recante "Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44, 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005."
- Decreto del Presidente del Consiglio dei Ministri 13 novembre 2014, recante "Regole tecniche in materia di formazione, riproduzione e validazione temporale dei documenti informatici nonché di

formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23-bis, 23-ter, 40, comma 1, 41, e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005.

- "Linee guida sulla Formazione, gestione e conservazione dei documenti informatici", emanate dall'Agenzia per l'Italia Digitale il 09/09/2020.
- "Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico" emanate dal Garante italiano per la protezione dei dati personali il 14 giugno 2007.
- Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario - emanati dal Garante italiano per la protezione dei dati personali il 7 marzo 2019.
- Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche – emanate dal Garante italiano per la protezione dei dati personali il 2 luglio 2015.

3 Definizioni

- **Amministratore di Sistema**: Figura aziendale che preposta alla gestione e alla manutenzione di tutti i componenti che costituiscono il centro elaborazione dati dell'Asl di Taranto;
- **Dominio (active directory)**: Struttura organizzativa utilizzata per la gestione centralizzata delle risorse e utenti all'interno di un'organizzazione;
- **Utenti di Dominio**: Entità informatica con cui si definisce l'operatore che accede fisicamente alla postazione di lavoro attraverso l'utilizzo delle proprie credenziali personali;
- **PDL:** Postazione di lavoro più comunemente indicato come pc (Personal Computer);
- **Autorità di Controllo**: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 GDPR;
- **Consenso dell'Interessato**: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'Interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i Dati Personali che lo riguardano siano oggetto di Trattamento;
- **Dati Biometrici**: i Dati Personali ottenuti da un Trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

- **Categorie particolari di dati**: dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, dati genetici, dati personali biometrici, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.
- **Dati relativi alla salute**: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;
- **Destinatario/i**: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di Dati Personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di Dati Personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate Destinatari; il Trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del Trattamento;
- **DPO o Data Protection Officer**: è una persona fisica, nominata obbligatoriamente solo nei casi di cui all'art. 37.1 GDPR dal Titolare o dal Responsabile del Trattamento e deve possedere una conoscenza specialistica della normativa e delle pratiche in materia di protezione dei dati per assisterli nel rispetto a livello interno del GDPR;
- **GDPR o Regolamento**: Regolamento Generale sulla Protezione dei dati personali (UE) 2016/679;

4 Norme di comportamento

Tutti gli strumenti utilizzati dall'utente, quali PC, notebook, tablet, smartphone, e-mail ed altri strumenti (di seguito più semplicemente "strumenti informatici"), sono messi a disposizione dalla ASL di Taranto unicamente per svolgere la propria attività lavorativa.

Nell'utilizzare gli strumenti informatici messi a disposizione dall'Azienda, l'utente 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.

5 Dominio Aziendale

In informatica con il termine dominio di rete o Active Directory si intende un insieme di servizi di rete, meglio noti come directory services, adottati dai sistemi operativi Microsoft a partire da Windows 2000 Server e gestiti da un sistema centralizzato denominato “domain controller”.

Esso si fonda sui concetti di dominio e di directory e consente di catalogare e gestire in modo centralizzato risorse di vario genere come: utenti, gruppi di lavoro, stampanti, cartelle condivise, ecc. La struttura del database è di tipo gerarchico, con contenitori che contengono oggetti e altri contenitori.

Tutti i computer del dominio vengono amministrati come un'unità con regole e procedure comuni. Ogni dominio ha un nome univoco. Il nostro Dominio è denominato “ASLTA.LOCAL”.

Caratteristica importante di un PC in dominio è il “nomadismo”, l’accesso multiplo di più utenti su una qualsiasi postazione di lavoro. Tutti gli utenti (dipendenti, convenzionati, ditte esterne) censiti in Active directory potranno effettuare l’accesso ad un qualsiasi PC in dominio presente in tutta la rete Asl (ospedali, dipartimenti, distretti, ecc....) semplicemente utilizzando come nome utente il proprio codice fiscale ed una password temporanea assegnata al primo accesso e successivamente modificata dall’utilizzatore.

Può accadere che, per esigenze di servizio, esistano credenziali d’accesso non legate ad un singolo lavoratore e che possono essere condivise da tutto un gruppo di operatori, (ad esempio per i reparti e ambulatori) queste credenziali avranno un responsabile incaricato della gestione.

Tutti gli utenti avranno una scadenza della propria password di accesso ai PC pari a 90 giorni, secondo quanto prescritto dal Provvedimento “Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche”, superato questo periodo e avvisati già 15 gg prima dal sistema, gli utenti dovranno necessariamente cambiare la propria password.

I dati personali degli utenti dipendenti e non presenti su LDAP vengono aggiornati tramite estrazione mensile dagli archivi del modulo *Areas Gestione Personale*, tale procedura viene anche adottata per la cessazione del lavoratore. Gli utenti appartenenti ad aziende esterne e quindi non presenti nel modulo Areas verranno gestiti come di seguito riportato.

In caso di un utente non presente in Dominio per il quale occorre l’immediato accesso ai sistemi, il Dirigente del settore competente può richiedere l’inserimento attraverso l'apposita procedura di notifica al servizio di help desk che provvederà all'assegnazione della *userid* e della *password* provvisoria inserendo le credenziali nelle banche dati necessarie e comunica le credenziali all'utente in modo riservato; è a cura del lavoratore sostituire la password provvisoria con quella definitiva.

6 Utilizzo del Personal Computer

Il Personal Computer (PDL) affidato all'utente 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.
Il personale deve custodire la propria strumentazione in modo appropriato e diligente, segnalando tempestivamente ogni danneggiamento, furto o smarrimento al proprio responsabile di servizio.
L'accesso all'elaboratore è protetto da password che deve essere custodita dall'incaricato con la massima diligenza e non divulgata. Le password devono essere utilizzate per l'accesso alla rete, per l'accesso a qualsiasi applicazione che lo preveda e per lo screen saver. Non è consentita l'attivazione o la modificazione della password di accensione (bios).
Non è consentito installare autonomamente programmi provenienti dall'esterno salvo previa autorizzazione esplicita del Responsabile della Struttura Ingegneria Clinica e dei Sistemi Informativi ed una richiesta scritta da parte del dirigente responsabile dell'unità cui è assegnato la PDL. In caso di necessità di acquisto o dotazione di software applicativi e/o procedure pertinenti esclusivamente alcune aree ed ai relativi dirigenti, deve essere comunque richiesta per iscritto l'autorizzazione preventiva da parte del Responsabile della Struttura Richiedente al responsabile della Struttura Ingegneria Clinica e dei Sistemi Informativi, per garantire la compatibilità funzionale, tecnica ed il mantenimento dell'efficienza operativa dei sistemi e delle reti. Sussiste infatti il grave pericolo di introdurre involontariamente virus informatici o di alterare la stabilità delle applicazioni degli elaboratori e dei sistemi operativi.
Non è consentito l'uso di programmi diversi da quelli distribuiti ufficialmente dal Servizio Sistemi Informativi (Legge 22 aprile 1941 n. 633 e ss.mm.ii. "Protezione del diritto d'autore e di altri diritti connessi al suo esercizio"; Direttiva 2009/24/CE del Parlamento europeo e del Consiglio, del 23 aprile 2009, relativa alla tutela giuridica dei programmi per elaboratore).
Non è consentito all'utente di modificare le caratteristiche impostate sui PC assegnati, i punti rete di accesso, le configurazioni delle reti LAN/WAN presenti nelle sedi e la configurazione del Browser per la navigazione, salvo autorizzazione esplicita del Responsabile del Servizio Sistemi Informativi.
È responsabilità del dirigente verificare il coerente utilizzo delle risorse assegnate ed evitarne l'uso improprio o l'accesso alle risorse da parte di personale non autorizzato, compreso l'utilizzo da parte di terzi di punti rete in luoghi non presidiati.
La PDL deve essere spenta ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio. In ogni caso lasciare un elaboratore 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 sulla propria PDL o il collegamento sulla rete LAN Aziendale, di nessun dispositivo di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, pc portatili, telefoni cellulari, PDA ed apparati in genere), se non con l'autorizzazione espressa del Responsabile della Struttura Ingegneria Clinica e dei Sistemi Informativi, previa richiesta scritta da parte del dirigente responsabile dell'unità cui è assegnato la PDL o il segmento di rete LAN.

Agli utenti autorizzati al trattamento delle categorie particolari di dati è fatto obbligo di distruggere eventuali copie di sicurezza o supporti di tipo removibile (CDRom, Nastri) una volta non sia possibile rendere irrecuperabili i dati in essi contenuti.

Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il Responsabile della Struttura Ingegneria Clinica e dei Sistemi Informativi nel caso in cui siano rilevati virus ed adottando quanto previsto dal punto del presente Regolamento relativo alle procedure di protezione antivirus.

Non è consentita la memorizzazione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.

È vietato rimuovere, danneggiare deliberatamente o asportare componenti hardware.

È vietato accedere direttamente ad Internet con modem collegato alla propria PDL o Notebook se non espressamente autorizzati e per particolari motivi tecnici.

L'utente è tenuto ad osservare le direttive del responsabile dei Sistemi Informativi volte garantire il corretto funzionamento delle procedure di backup. I dati, documenti o file creati o modificati attraverso le applicazioni di produttività individuale –es. office o open-office- devono essere salvati solo sui supporti appositamente destinati

È vietato utilizzare gli strumenti informatici della ASL al fine di custodire, far circolare o promuovere materiale pubblicitario personale, codice malevolo (virus, trojan horses, programmi pirata o altre porzioni di codice malevolo) e/o altro materiale non autorizzato.

È vietato copiare o mettere a disposizione di altri materiale protetto dalla legge sul diritto d'autore (documenti, files musicali, immagini, filmati e simili) di cui l'ente non abbia acquisito i diritti.

L'utente che appartiene ad associazioni e/o organizzazioni, non utilizza il proprio tempo, lavoro, i beni o le attrezzature dell'azienda per promuovere l'attività di tali organismi.

L'utente utilizza i mezzi il materiale o le attrezzature di cui dispone per ragioni di ufficio e i servizi telematici e telefonici dell'ufficio nel rispetto dei vincoli posti dalla ASL avendo cura di non rendere noti a terzi eventuali credenziali per l'accesso a procedure informatiche aziendali.

7 Utilizzo della rete dell'ASL di Taranto

È presente una Intranet aziendale basata su tecnologia MPLS e piattaforma web interna. Ad essa possono avere accesso tutti i dipendenti abilitati e profilati in relazione al ruolo aziendale. L'accesso alla rete Internet, mediante Proxy Aziendale, è regolamentato con autenticazione integrata con Microsoft Active Directory.
Hanno diritto ad accedere alla rete Intranet della ASL di Taranto gli amministratori, le ditte fornitrici di software e/o servizi per motivi di manutenzione e limitatamente alle applicazioni di loro competenza, collaboratori esterni impegnati nelle attività istituzionali per il periodo di collaborazione.
Al fine di garantire la corretta gestione delle politiche di sicurezza delle informazioni è fatto divieto di replicare su dischi locali dei PC dati aziendali, banche dati e documenti sensibili senza esplicita autorizzazione del Responsabile della Struttura Ingegneria Clinica e dei Sistemi Informativi e senza l'adozione di adeguate politiche di sicurezza, quali la crittazione dei dati stessi e l'adozione di politiche di backup comprensive della dotazione di idonei archivi protetti.
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 nomi utente diversi dal proprio.
Il Responsabile della Struttura Ingegneria Clinica e dei Sistemi Informativi 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, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. È infatti assolutamente da evitare un'archiviazione ridondante.
Non è consentito all'utente di collegare reti di pc od altri dispositivi alla rete aziendale senza la preventiva autorizzazione scritta dell'Amministratore di Sistema ed una verifica della conformità agli standard tecnici presenti
È vietato agire deliberatamente con attività che influenzino negativamente la regolare operatività della rete e ne restringano l'utilizzabilità e le prestazioni per altri utenti.
È vietato agire deliberatamente con attività che distraggano risorse (persone, capacità, elaboratori).

È vietato fare o permettere ad altri trasferimenti non autorizzati di informazioni (software, basi dati, ecc.).
È vietato installare o eseguire deliberatamente o diffondere su qualunque computer e sulla rete, programmi destinati a danneggiare o sovraccaricare i sistemi o la rete (p.e. virus, cavalli di troia, worms, spamming della posta elettronica, programmi di file sharing - p2p.
È vietato monitorare o utilizzare qualunque tipo di sistema informatico o elettronico per controllare le attività degli utenti, leggere copiare o cancellare file e software di altri utenti, senza averne l'autorizzazione esplicita.
È vietato usare l'anonimato o servirsi di risorse che consentano di restare anonimi sulla rete.

8 Gestione delle password e degli accessi

All'atto della creazione delle credenziali di un nuovo utente, verrà assegnata una password provvisoria che dovrà essere cambiata al primo accesso alla postazione di lavoro assegnata.
Nella scelta della password personale di accesso alla postazione di lavoro si consiglia di non utilizzare riferimenti direttamente riconducibili all'assegnatario delle credenziali con l'obbligo di rispettare la regola di complessità delle password (Minimo 8 caratteri con almeno una lettera maiuscola, un numero e un carattere speciale)
Le password utilizzate dagli utilizzatori delle PDL hanno una durata massima di 3 mesi, trascorsi i quali le password devono essere sostituite.
Qualora l'utente venisse a conoscenza delle password di altro utente, è tenuto a darne immediata notizia alla Direzione o persona dalla stessa incaricata (Responsabile, Amministratore del Sistema, …), nonché al DPO.
È dato incarico ai dirigenti di comunicare tempestivamente al DPO eventuali cambi di mansione che comportino modifiche o revoche di autorizzazione all'accesso delle risorse informatiche, sia all'ufficio.

9 Utilizzo di unità di memorizzazione esterna

Tutti i supporti magnetici riutilizzabili (chiavette usb, hd portatili) contenentI categorie particolari di dati devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato. Una persona esperta potrebbe infatti recuperare i dati memorizzati anche dopo la loro cancellazione.
I supporti magnetici contenenti dati sensibili devono essere custoditi in archivi chiusi a chiave.
Non è consentito scaricare files contenuti in supporti magnetici/ottici non aventi alcuna attinenza con la propria prestazione lavorativa.

Tutti i files di provenienza incerta, ancorché potenzialmente attinenti all'attività lavorativa, non devono essere utilizzati/installati/testati. Nel caso di effettiva necessità di impiego devono essere sottoposti ad un preventivo controllo ed alla relativa autorizzazione all'utilizzo da parte del Responsabile della Struttura Ingegneria Clinica e dei Sistemi Informativi e/o del suo staff tecnico.

10 Gestione di unità di memorizzazione esterna, stampanti e documenti cartacei

Le stampe dimenticate o i dati memorizzati su supporti rimovibili possono spesso costituire involontaria fuga di notizie. Si raccomanda quindi la massima attenzione nell'utilizzo di stampe e dispositivi di memorizzazione con particolare riferimento alla corretta distruzione di documenti e o supporti non più utilizzati.

È cura dell'utente effettuare la stampa dei dati solo se strettamente necessaria e di ritirarla prontamente dai vassoi delle stampanti comuni.

È vietato portare fuori dall'azienda tabulati, stampe, supporti di memorizzazione sia magnetici che ottici salvo esplicita autorizzazione.

Qualsiasi CD, DVD prodotto all'interno dell'azienda deve obbligatoriamente essere realizzato mediante i supporti ufficiali. Non è assolutamente ammesso l'utilizzo di supporti (CD-R o CD-RW) diversi dai supporti ufficiali.

Tutti i supporti magnetici e/o ottici (cassette, CD-R, CD-RW, DVD-R, DVD-RD) contenenti dati sensibili devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato o cadere in mano a terzi non autorizzati. La semplice cancellazione dei supporti non garantisce l'eliminazione dei dati in essi memorizzati; una persona esperta potrebbe infatti recuperare i dati memorizzati anche dopo la loro cancellazione.

11 Utilizzo di PC portatili

L'utente è responsabile del PC portatile eventualmente assegnatogli dal Responsabile della Struttura Ingegneria Clinica e dei Sistemi Informativi e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

Ai PC portatili si applicano le regole di utilizzo previste per i Pc connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna.

I PC portatili utilizzati all'esterno (convegni etc.), in caso di allontanamento, devono essere custoditi in un luogo protetto.

Eventuali configurazioni di tipo Accesso Remoto, dirette verso la rete aziendale o attraverso internet, devono essere autorizzate esclusivamente a cura del Responsabile della Struttura Ingegneria Clinica e dei Sistemi Informativi.

Non è consentito l'utilizzo di dispositivi portatili personali privati se non preventivamente autorizzati dal Responsabile della Struttura Ingegneria Clinica e dei Sistemi Informativi.

12 Uso della posta elettronica

La casella di posta elettronica nome.cognome**@asl.taranto.it e/o nomestruttura@asl.taranto.it**, di tipo web-mail, ovvero accessibile collegandosi via web al sito che fornisce il servizio, assegnata all'ufficio e/o all'utente, è uno strumento di lavoro. Le persone/responsabili dei servizi assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse. Si rammenta che la tecnologia dei sistemi di posta elettronica non consente attualmente di garantire la riservatezza delle informazioni trasmesse, per cui si raccomandano gli utenti di non inoltrare dati ed informazioni classificabili "sensibili" o "riservate" con questo mezzo.

Per quanto sopra esposto, è fatto divieto di utilizzare il sistema di Posta Elettronica Aziendale per finalità differenti da quelle descritte in questo paragrafo (es. creazione di cartelle condivise, etc.).

È fatto divieto di utilizzare le caselle di posta elettronica aziendale per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail-list non attinenti la propria attività o funzione svolta per l'ente, salvo diversa ed esplicita autorizzazione.

È buona norma evitare messaggi completamente estranei al rapporto di lavoro o alle relazioni tra colleghi. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti. Secondo la convenzione in atto, è previsto un dimensionamento massimo per ciascuna casella, di questo spazio è buona norma non superare il 70-80%.

È possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario, ma di norma per la comunicazione ufficiale a privati è obbligatorio avvalersi degli strumenti tradizionali (posta certificata, posta etc. …).

È obbligatorio controllare con il Software antivirus i file attachment di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).

È vietato inviare catene telematiche (o di Sant'Antonio). Se si dovessero ricevere messaggi di tale tipo, lo si deve comunicare immediatamente all'Amministratore del Sistema. Non si deve in alcun caso attivare gli allegati di tali messaggi.

Nei messaggi inviati tramite posta elettronica aziendale (di servizio e/o nominative) dovrà essere accluso il seguente testo: "Si segnala che il presente messaggio e le risposte allo stesso potranno essere conosciute dall'organizzazione lavorativa di appartenenza del mittente secondo le modalità previste dal regolamento Aziendale adottato in materia. Se per un disguido avete ricevuto questa e-mail senza esserne i destinatari vogliate cortesemente distruggerla e darne informazione all'indirizzo mittente".

È obbligatorio controllare i file allegati di posta elettronica prima del loro utilizzo. In particolare, si deve evitare, secondo le regole di buona diligenza, l'apertura e la lettura di messaggi di posta elettronica in arrivo provenienti da mittenti di cui non si conosce con certezza l'identità o che contengano allegati del tipo .exe, .com, .vbs, .htm, .scr, .bat, .js, .pif.

Nel caso in cui fosse necessario inviare a destinatari esterni messaggi contenenti allegati con dati personali o dati personali particolari è obbligatorio che questi allegati vengano preventivamente resi illeggibili attraverso la criptografia con apposito software (archiviazione e compressione con password). La password di cifratura deve essere comunicata al destinatario attraverso un canale diverso dalla mail (ad esempio per lettera o per telefono) e mai assieme ai dati criptati. Tutte le informazioni, i dati personali e/o sensibili di competenza possono essere inviati soltanto a destinatari – persone o Enti – qualificati e competenti.

Non è consentito l'invio automatico di e-mail all'indirizzo e-mail privato (attivando per esempio un "inoltro" automatico delle e-mail entranti), anche durante i periodi di assenza (es. ferie, malattia, infortunio ecc.). In questa ultima ipotesi, occorrerà prevedere l'utilizzazione di un messaggio "Out of Office" facendo menzione di chi, all'interno dell'Ente, assumerà le mansioni durante l'assenza, oppure indicando un indirizzo di mail alternativo preferibilmente di tipo collettivo, tipo ufficio…@asl.taranto.it.

In caso di assenza improvvisa o prolungata di un dipendente e per improrogabili necessità legate all'attività lavorativa sarebbe auspicabile prevedere che il titolare della casella di posta designi un altro dipendente (fiduciario) per verificare il contenuto di messaggi e per inoltrare al titolare del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. Sarà compito del responsabile di struttura e/o area assicurarsi che sia redatto un verbale attestante quanto avvenuto e che si sia informato il lavoratore interessato alla prima occasione utile.

È bene, altresì, vietare l'invio di messaggi di posta elettronica in nome e per conto di un altro utente, salvo sua espressa autorizzazione scritta.

L'Azienda fa presente al personale dipendente che il servizio di posta elettronica fornito mediante l'attribuzione di un account aziendale è uno "strumento di lavoro", al pari degli altri servizi della rete aziendale, fra cui anche il collegamento a determinati siti internet. Costituiscono parte integrante di questi strumenti,

anche i sistemi e le misure – in uso presso l'Azienda - che ne consentono il fisiologico e sicuro funzionamento al fine di garantire un elevato livello di sicurezza della rete aziendale messa a disposizione del lavoratore (ad esempio: sistemi di logging per il corretto esercizio del servizio di posta elettronica, che conserva i soli dati esteriori, contenuti nella cosiddetta "envelope" del messaggio, per una durata non superiore a sette giorni; sistemi di filtraggio anti-virus che rilevano anomalie di sicurezza nelle postazioni di lavoro o sui server per l'erogazione dei servizi di rete; sistemi di inibizione automatica della consultazione di contenuti in rete inconferenti rispetto alle competenze istituzionali, senza registrazione dei tentativi di accesso).

Tutti i messaggi di posta elettronica (inviati e ricevuti), i cui contenuti possono avere una rilevanza giuridica e istituzionale per l'Azienda, costituiscono corrispondenza (disciplinata dalle norme del Codice Civile e, in particolare, in base al combinato disposto degli articoli 2214 e 2220) e pertanto vanno adeguatamente conservati. In ogni caso, il tempo di conservazione dei messaggi di posta elettronica, anche per le altre tipologie documentali, non sarà superiore a quello necessario agli scopi che si intendono perseguire (e, per tale motivo, può variare anche in base al ruolo a cui l'account era stato assegnato), nel rispetto dei principi di finalità, pertinenza e non eccedenza previsti dalla normativa in materia di protezione dei dati.

Ad ogni buon conto, il sistema di Posta Elettronica, non è un sistema di conservazione sostitutiva a norma, ai sensi dell'art. 3 del DPCM del 3 dicembre 2013 e, pertanto, non deve essere utilizzato come tale.

In caso di assenza improvvisa o prolungata del dipendente ovvero per imprescindibili esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio le ovvero per motivi di sicurezza del sistema informatico, l'azienda per il tramite dell'amministratore di sistema potrà, solo se previsto specificatamente nel regolamento e sulla base delle norme indicate, accedere all'account di posta elettronica, prendendo visione dei messaggi, salvando o cancellando file. Secondo quanto prescritto dal provvedimento "Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche", al termine della collaborazione lavorativa con l'Azienda Ospedaliera, l'eventuale account nominativo di posta elettronica aziendale del dipendente (di proprietà della Azienda) sarà disattivato entro 3 mesi e la stessa Azienda potrà disporre del suo utilizzo futuro, limitatamente alla corrispondenza intercorsa che ha un valore aziendale perché attinente all'attività lavorativa del dipendente cessato (che verrà conservata per un periodo di tempo congruo rispetto agli scopi che si intendono perseguire, che può variare anche in base al ruolo e alla figura a cui l'account era stato assegnato e fino a un massimo di 6 mesi); un messaggio automatico sull'account del dipendente cessato potrà segnalare al mittente il reindirizzamento dell'e-mail ad altro dipendente (su di un account alternativo). Inoltre, una volta consegnata la lettera di dimissioni o in caso di licenziamento o pensionamento non sarà possibile inviare mail verso l'esterno a meno di una deroga concessa dall'Azienda.

13 Uso della rete internet e dei relativi servizi

Per ragioni di sicurezza e per garantire l'integrità dei sistemi informatici, l'accesso ad Internet effettuato tramite elaboratori connessi alla rete ASL è scrupolosamente protetto da appositi dispositivi di sicurezza informatica (firewall, viruswall, antivirus, proxy server, etc.).

La PDL abilitata alla navigazione in Internet costituisce uno strumento aziendale necessario allo svolgimento della propria attività lavorativa. È proibita la navigazione in Internet per motivi diversi da quelli funzionali all'attività lavorativa stessa. È fatto divieto all'utente lo scarico di software gratuito (freeware) e shareware prelevato da siti Internet, se non espressamente autorizzato dal Responsabile della Struttura Ingegneria Clinica e dei del Servizio Sistemi Informativi.

È tassativamente vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili salvo i casi direttamente autorizzati dalla Direzione o attinenti i compiti e le mansioni assegnate e con il rispetto delle normali procedure di acquisto.

È da evitare ogni forma di registrazione a siti, mailing-list i cui contenuti non siano legati all'attività lavorativa.

È vietata la partecipazione a Forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames), se non attinenti l'attività lavorativa svolta.

La Struttura Ingegneria Clinica e dei Servizio Sistemi Informativi Aziendali si riserva di applicare politiche di navigazione concordate con la Direzione Aziendale, al fine di ottimizzare l'uso delle risorse, gli investimenti e le prestazioni delle connessioni esistenti.

Non è consentita la navigazione in siti ove sia possibile rivelare le opinioni politiche, religiose o sindacali dell'utilizzatore; non è consentito inoltre visitare siti e memorizzare documenti informatici dai contenuti di natura oltraggiosa e/o discriminatoria per sesso/etnia/religione/opinione e/o appartenenza sindacale e/o politica.

14 Aree di condivisione informazioni

Per ogni utente appartenente al dominio aziendale, sarà attivata a breve, un'area di storage remoto, fruibile da qualunque PC connesso alla rete Aziendale. Sono aree di memorizzazione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto qualunque file, che non

sia legato all'attività lavorativa, non può essere collocato, nemmeno per brevi periodi, in queste unità di storage.

Su queste unità vengono svolte regolari attività di verifica ed amministrazione da parte del personale preposto.

Gli utenti possono utilizzare le cartelle personali create nell'area di storage centralizzata il cui accesso in scrittura e lettura è concesso solo all'utente e agli operatori CED.

È assolutamente vietato la creazione 'uso di cartelle condivise su PC Aziendali.

A tal proposito, sono state messe a disposizione, degli utenti, aree condivise a livello di struttura/dipartimento ed altre a livello di ufficio in cui possono accedere in lettura e scrittura tutti gli utenti autenticati su richiesta del Responsabile della struttura e/o dipartimento. Per garantire maggiore flessibilità possono essere create, su richiesta del Responsabile di struttura, delle cartelle di lavoro condivise a seconda del gruppo di lavoro o del progetto.

Nelle suddette aree condivise, è assolutamente vietato copiare categorie particolari di dati.

È vietata la condivisione, attraverso le aree condivise, di categorie particolari di dati appartenenti a pazienti, personale dipendente, e persone fisiche in genere.

Le aree condivise non vanno usate per operazioni di archiviazione e scambio di files il cui contenuto non sia riferibile all'attività lavorativa; pertanto se nel caso di manutenzione delle cartelle condivise da parte del personale del SITA della Struttura Ingegneria Clinica e dei Sistemi Informativi Aziendali si dovessero manifestare usi non corretti della risorsa, il personale è autorizzato in prima istanza alla rimozione di tali files e qualora dovesse proseguire l'abuso si provvederà alla chiusura della risorsa fornita. Il personale della Struttura Ingegneria Clinica e dei Sistemi Informativi Aziendali del SITA, su richiesta del responsabile della Struttura servizio sistemi informativi, può in qualunque momento procedere alla rimozione di ogni file o applicazione che ritenga essere pericolosi per la sicurezza della rete aziendale sia sulla PDL degli incaricati sia sulle unità di rete.

Nel caso di cessazione del servizio e/o trasferimento per mobilità di un utente, deve esserne data, da parte del dirigente di struttura, comunicazione al la Struttura Ingegneria Clinica e dei Sistemi Informativi Aziendali Servizio Sistemi Informativi. È assolutamente vietato, in caso di cessazione del servizio e/o trasferimento per mobilità, la sottrazione di file e/o cartelle dal proprio computer, costituendo i file archiviati documentazione amministrativa/tecnica di proprietà della ASL di Taranto.

15 Protezione Antivirus

I personal Computer sono dotati di software Antivirus Centralizzato, ogni utente deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale mediante virus o mediante ogni altro software aggressivo.

Ogni utente è tenuto a controllare il regolare funzionamento e l'aggiornamento periodico del software installato, secondo le procedure previste.

Nel caso che il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente:

- sospendere ogni elaborazione in corso senza spegnere il computer
- segnalare l'accaduto al Responsabile del Servizio Sistemi Informativi.

Non è consentito l'utilizzo di pendrive, cd rom, cd riscrivibili, nastri magnetici di provenienza ignota.

Ogni dispositivo di memorizzazione, di provenienza esterna all'azienda, dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, dovrà essere informato l'amministratore di sistema.

16 Monitoraggio e controllo

Al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa, La ASL di Taranto, rende nota l'adozione di un sistema "Proxy" che consente di attivare determinati blocchi o filtri automatici che prevengano determinate operazioni quali l'upload o l'accesso a determinati siti inseriti in una black list o la consultazione di video in streaming ecc. Nell´effettuare controlli sull´uso degli strumenti elettronici, l'Ente assicura il rispetto dei principi di pertinenza e non eccedenza.

In caso di evento dannoso o di una situazione di pericolo, viene attivato un controllo preliminare su dati aggregati, riferiti all´intera struttura lavorativa o a sue aree. Il controllo anonimo, di regola, si conclude con un avviso generalizzato relativo ad un rilevato utilizzo anomalo degli strumenti aziendali e con l´invito ad attenersi scrupolosamente a compiti assegnati e istruzioni impartite. L´avviso può essere circoscritto a dipendenti afferenti all´area o settore in cui è stata rilevata l´anomalia.

Nel caso in cui l'anomalia non si risolva con i suddetti mezzi, l'ASL effettuerà verifiche più circoscritte, applicando il criterio della graduazione dei controlli.

Le eventuali verifiche possono avvenire mediante un sistema di verifica dei contenuti o mediante "file di log" della navigazione svolta. La consultazione dei file di log viene effettuata soltanto dietro richiesta scritta al Responsabile della Struttura Ingegneria Clinica e dei Sistemi Informativi Aziendali opportunamente motivata ed i file stessi sono conservati non oltre 7 giorni, ossia il tempo indispensabile per il corretto perseguimento delle finalità organizzative e di sicurezza dell'Ente.

Qualora il file di log venga utilizzato come prova in caso di provvedimenti disciplinari, è compito del personale del Servizio Sistemi Informativi, dietro autorizzazione scritta del Responsabile della struttura richiedente e del Responsabile del Servizio Sistemi Informativi, sentito il DPO, estrarre copia memorizzarla su un supporto non riscrivibile e consegnarla al Responsabile medesimo che provvederà alla

dello stesso. Tutte le informazioni eventualmente raccolte saranno utilizzate a tutti i fini connessi al rapporto di lavoro, compresa la verifica del rispetto del presente Regolamento, che costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli ai sensi del Regolamento Europeo 2016/679, nonché della L. n. 300/1970.

17 Accesso dall'esterno alla rete intranet

L'accesso alle risorse del sistema intranet dall'esterno è consentito tramite accesso VPN (Virtual Private Network) su richiesta scritta del responsabile di struttura e/o reparto, mediante apposito modulo precompilato, ed assunzione di responsabilità. Il Responsabile della Struttura Ingegneria Clinica e dei Sistemi Informativi Aziendali Servizio Sistemi Informativi può, verificati i requisiti di sicurezza, concedere le credenziali di accesso alla rete VPN.

Per accedere alla Intranet della Asl di Taranto, ogni Utente VPN dovrà ottenere le credenziali necessarie, dopo essersi impegnato ad osservare il presente Regolamento. La procedura di rilascio delle credenziali prevede l'accettazione delle stesse in forma scritta mediante la sottoscrizione di un modulo messo a disposizione dalla ASLTA.

L'Utente VPN:

- Dovrà accedere esclusivamente ai servizi per i quali è stato espressamente autorizzato e con le modalità consentite;
- È personalmente responsabile del mantenimento della necessaria riservatezza sulle proprie credenziali;
- È responsabile delle attività svolte all'interno della Intranet Aziendale attraverso le credenziali a lui assegnate.

Si impegna a comunicare immediatamente al Servizio Sistemi Informativi, o tramite il servizio HelpDesk, lo smarrimento, il furto o l'appropriazione da parte di terzi delle proprie credenziali;

È tenuto a segnalare immediatamente qualsiasi incidente o malfunzionamento tramite il servizio HelpDesk.

Resta inteso che possono accedere alla Intranet Aziendale ASLTA tramite VPN, gli utenti a cui sono state consegnate le credenziali di accesso deboli personali, esclusivamente per il periodo di tempo necessario all'espletamento dei propri compiti.La Struttura Ingegneria Clinica e dei Sistemi Informativi Aziendali Servizio

Sistemi Informativi della ASL può regolamentare e vietare temporaneamente l'accesso alla propria rete determinate categorie di utenti o singoli utenti, per l'accesso a sistemi in rete e servizi.

Non è in alcun modo consentito l'utilizzo di software di controllo remoto come:

- TeamviwerTeamViewer;
- SupRemo;
- Chrome Remote Desktop.

  Se non esplicitamente autorizzato e comunque per un periodo limitato di tempo sotto la supervisione del personale SITA della Struttura Ingegneria Clinica e dei Sistemi Informativi Aziendali.

18 Sistema di Videoconferenza

L'Amministrazione si è dotata di un sistema di videoconferenze. La gestione delle utenze di accesso al servizio rispecchia le norme che regolamentano le utenze interne dei Sistema Informativo. Per usufruire del servizio è necessario indirizzare una richiesta alla Struttura Ingegneria Clinica e dei Sistemi Informativi Aziendali S.S.D. SITA.

19 Osservanza delle disposizioni in materia di Privacy

È obbligatorio attenersi alle disposizioni in materia di Privacy e di misure minime di sicurezza. Tali indicazioni saranno fornite per iscritto a tutto il personale che operi in qualità di "designato al trattamento dei dati" o "autorizzato al trattamento dei dati", ovvero "delegato" a talune specifiche operazioni di trattamento.

20 Non osservanza della normativa aziendale

L'ASL di Taranto verificherà, nei limiti consentiti dalle norme legali e contrattuali, il rispetto delle regole e l'integrità del proprio sistema informatico. Il mancato rispetto o la violazione delle regole contenute nel presente regolamento è perseguibile con provvedimenti disciplinari nonché con le azioni civili e penali consentite.

21 Aggiornamento e revisione

L'ASL di Taranto verificherà, nei limiti consentiti dalle norme legali e contrattuali, il rispetto delle regole e l'integrità del proprio sistema informatico.