REGIONE DEL VENETO

ULSS6 EUGANEA

N. 51 **del** 21-01-2022

DELIBERAZIONE DEL DIRETTORE GENERALE

dott. Paolo FORTUNA

Coadiuvato dai Signori:

DIRETTORE AMMINISTRATIVO	dr.ssa Michela Barbiero
DIRETTORE SANITARIO	dr. Aldo Mariotto
DIRETTORE DEI SERVIZI SOCIO SANITARI	dr.ssa Maria Chiara Corti

Note Trasparenza: Con il presente provvedimento si adotta, nel rispetto della normativa vigente europea e nazionale, in materia di Protezione dei Dati Personali, il Regolamento per l'utilizzo degli Strumenti Informatici dell'ULSS 6 Euganea.

OGGETTO: Regolamento per l'utilizzo degli strumenti informatici dell'ULSS 6 Euganea.

Il Direttore della Struttura UOSD Sistemi informativi riferisce:
Lo sviluppo sempre più diffuso della digitalizzazione dei servizi, di strumenti informatici a supporto dei processi aziendali, di modalità di comunicazione celeri e disponibili su vari supporti digitali rendono fondamentale la condivisione di un percorso culturale aziendale che garantisca la sicurezza dei dati e modalità operative omogenee per assicurare il patrimonio informativo e la tutela dei diritti degli interessati.
La stringente normativa in materia e l'elevata attenzione a tutti i livelli decisionali (Regolamento UE 2016/679, Codice della Privacy D. Lgs. 196/2003 modificato dal D. Lgs. 101/2018, misure emanate da AGID sulla sicurezza ICT per le pubbliche amministrazioni) ha permesso l'avvio di un percorso di sensibilizzazione, condivisione delle modalità operative nonché di stringente attenzione alla definizione delle politiche aziendali sulla sicurezza informatica al fine di garantire l'integrità e la disponibilità dei dati trattati.
A questo contesto si aggiunge un processo aziendale di sburocratizzazione e di flessibilità delle modalità operative che incentiva l'utilizzo delle tecnologie informatiche e di strumenti digitali messi a disposizione dall'Azienda stessa (posta elettronica, accesso alla rete aziendale, condivisione di cartelle, internet, telefoni aziendali, computer portatili, tablet, etc.) che richiede necessariamente una regolamentazione uniforme nell'intero ambito aziendale e una capillare informazione e formazione dei professionisti coinvolti. Il ruolo, infatti, di ogni

dipendente nel corretto utilizzo della strumentazione è di fondamentale importanza oltre che nel rispetto del principio di diligenza anche per garantire la correttezza di gestione degli strumenti, dell'informazione e dei dati considerata l'accessibilità agli stessi che la digitalizzazione permette. Il dovere, d'altra parte, dell'azienda è quello di individuare il complesso delle misure tecniche, informatiche, organizzative e procedurali di sicurezza che configurano il livello minimo di protezione per il trattamento dei dati personale, nonché adottare tutte le modalità operative per prevenire utilizzi indebiti che possono essere fonte di responsbailità.
L'ULSS 6 Euganea è il frutto di un percorso di fusione aziendale che ha determinato per molti aspetti un'aggregazione di strutture e strumenti operativi nonché di disposizioni già presenti nelle precedenti ULSS.
Considerate le premesse, la Direzione Amministrativa ha ravvisato la necessità di completare il percorso di omogeneizzazione attraverso la revisione del sistema documentale con un approccio metodologico supportato dalla UOS Qualità e Percorsi di Accreditamento così da favorire, tramite un metodo maggiormente strutturato, un percorso uniforme di quanto elaborato nonché la massima condivisione e formalizzazione dei documenti prodotti.
A tal fine nel 2021, con Delibera del direttore Generale 776/2021, è stata approvata la nuova Procedura Trasversale "Elaborazione e gestione dei documenti aziendali" applicabile in tutto il contesto aziendale. Tale Procedura definisce le modalità di elaborazione, validazione, verifica, approvazione, attribuzione della codifica, diffusione, conservazione e revisione di alcune tipologie di documenti, tra i quali i Regolamenti, le Procedure trasversali, le Procedure operative e le Istruzioni operative.
L'ambito dei sistemi informativi rientra appieno nella necessità di ricondurre le diverse disposizioni già presenti nei territori che afferivano alle precedenti ULSS ad un'unica modalità operativa per le diverse aree di competenza.
In questo percorso la Direzione Amministrativa ha costituito un Gruppo di Lavoro composto da Sistemi Informativi, DPO, Ufficio Privacy, UOS Qualità e Percorsi di Accreditamento con l'obiettivo di produrre un regolamento che fornisca a livello aziendale specifiche ed uniformi disposizioni ad ogni utilizzatore di risorse informatiche e telematiche richiamando, al tempo stesso, alla responsabilità in caso di inosservanza delle stesse. E' stato inoltre affidato al medesimo gruppo di lavoro, nell'ambito dei Sistemi Informativi, il compito di continuare il percorso di revisione di tutte le istruzioni operative conseguenti al Regolamento elaborato e garantire la coerenza delle policy interne in materia.
Il Documento elaborato dal gruppo di lavoro è stato anche inviato a tutte le Organizzazioni Sindacali, per le osservazioni di competenza.
Attestata la conformità del presente provvedimento alla normativa nazionale e regionale, per quanto sopra si propone di approvare il regolamento allegato alla presente quale parte integrante.

IL DIRETTORE GENERALE

Dato atto che la UOSD Sistemi informativi ha attestato l'avvenuta regolare istruttoria della pratica anche in ordine alla compatibilità con la vigente legislazione statale e regionale;
Coadiuvato dai Direttori Amministrativo, Sanitario e dei Servizi Socio Sanitari, che ai sensi dell'art. 3 del D.Lgs. 502/92 e s.m.i. esprimono parere favorevole per quanto di rispettiva competenza;
In base ai poteri conferitogli dal D.P.G.R. n. 25 del 26.02.2021.

DELIBERA

Per le motivazioni di cui alle premesse, parti integranti e sostanziali del presente atto:

1. di adottare, per le motivazioni espresse in premessa, il Regolamento per l'utilizzo degli strumenti informatici;
2. di delegare il Direttore della UOSD Sistemi Informativi all'adozione di tutte le azioni necessarie a garantire la corretta applicazione del Regolamento nonché a proporre periodiche revisioni nel caso si rendano necessarie;
3. di delegare il Direttore della UOS Formazione all'attivazione dei percorsi formativi già previsti nel piano formativo e in linea con il presente regolamento;
4. di dichiarare, dalla data di adozione del presente provvedimento, l'inefficacia di precedenti provvedimenti, indicazioni o disposizioni fornite in materia di utilizzo degli strumenti informatici;
5. di disporre la massima pubblicità e diffusione del Regolamento mediante la pubblicazione sul sito internet aziendale, intranet aziendale e con eventuali ulteriori modalità che ne garantiscano la maggiore diffusione tra tutti i soggetti destinatari;
6. di confermare al Gruppo di Lavoro, istituito su input della Direzione Amministrativa, il mandato per rivedere tutte le istruzioni operative collegate al Regolamento e le policy connesse;
7. di prendere atto che il presente atto non comporta oneri per l'Azienda.

Il Direttore Generale
dr. Paolo Fortuna

Direttore Amministrativo	Direttore Sanitario	Direttore dei Servizi Socio Sanitari
dr.ssa Michela Barbiero	dr. Aldo Mariotto	dr.ssa Maria Chiara Corti

REGOLAMENTO PER L'UTILIZZO DEGLI STRUMENTI INFORMATICI

	Nome Cognome	Ruolo/Unità Operativa	Data	Firma
Redatto:	Antonio Sturaro	Coordinatore GdL Responsabile ff UOSD Sistemi informativi	19/01/22	
Validato:	Zampieri Tullio	Responsabile UOC Affari generali	19/01/22	
	Chiara Zambon	Data Protection Officer	19/01/22	
Verificato:	Carmelina Saraceno	Responsabile UOS Qualità e Percorsi di Accreditamento	19/01/22	
Approvato:	Michela Barbiero	Direttore Amministrativo	19/01/22	
	Aldo Mariotto	Direttore Sanitario	19/01/22	
	Maria Chiara Corti	Direttore Servizi Socio Sanitari	19/01/22	
	Paolo Fortuna	Direttore Generale	19/01/22	

INDICE

1.PREMESSA

L'Azienda ULSS 6 Euganea, nell'espletamento della sua attività istituzionale opera prestando la massima attenzione alla sicurezza delle informazioni, perseguendo elevati livelli di sicurezza fisica e logica del proprio sistema informativo e adottando idonee misure organizzative, tecnologiche ed operative volte sia a prevenire il rischio di utilizzi impropri delle strumentazioni sia a proteggere le informazioni gestite nelle banche dati del sistema informativo.

L'Azienda fornisce gli strumenti informatici e telematici agli utilizzatori confidando sul comune impegno affinché siano sempre garantiti sia il loro corretto ed equilibrato utilizzo, sia la sicurezza e l'integrità del sistema informatico/informativo; inoltre non vengano pregiudicate o ostacolate le attività dei singoli o della collettività a causa di un uso inappropriato delle risorse disponibili da parte del singolo e non vengano perseguiti interessi privati in contrasto con quelli pubblici.
Al fine di garantire la massima tutela alla protezione delle persone fisiche con riguardo al trattamento dei dati personali; alla dignità del paziente; al patrimonio informativo aziendale; all'utilizzatore dei sistemi e delle reti di comunicazione; ai sistemi informatici e delle reti di comunicazione nonché, al fine di promuovere la cultura della sicurezza, si rende necessario uniformare le regole e prassi aziendali presenti nelle tre ex aziende sanitarie 15-16 e 17 nel presente regolamento aziendale per l'utilizzo degli strumenti informatici.

Il presente documento definisce quindi le regole e le condizioni per l'utilizzo degli strumenti informatici dell'Azienda da parte dei dipendenti e di tutti coloro che, in virtù di un rapporto di lavoro a qualsiasi titolo (collaboratori, consulenti, frequentatori, stagisti, fornitori, etc.), utilizzano strumenti informatici dell'Azienda e le regole riportate si rifanno alla normativa in materia di protezione dei dati personali, alla normativa sul crimine informatico e più in generale al corpo normativo che disciplina i rapporti di lavoro. Quanto espresso in questo documento, pertanto, è di complemento al Codice di Comportamento Aziendale anche in merito alla possibile attivazione di procedimenti disciplinari.
Il presente regolamento deve considerarsi integrato da tutte le procedure trasversali/operative e dalle istruzioni operative adottate in Azienda.

2.SCOPO

Il presente regolamento contiene tutte le regole e le disposizioni che ogni utilizzatore di risorse informatiche e telematiche dell'Azienda deve conoscere e richiama alle responsabilità in caso di inosservanza delle stesse.

3.CAMPO DI APPLICAZIONE E DESTINATARI

Il documento opera nei confronti di ogni dipendente dell'Azienda e di tutti coloro che a vario titolo si trovino a utilizzare il sistema informativo aziendale.

4. GRUPPO DI LAVORO

Nome e Cognome	Ruolo	Figura professionale	U.O Afferenza
Antonio Sturaro	Coordinatore GdL	Dirigente analista Responsabile	UOSD Sistemi informativi
Claudio Voci	Componente GdL	Dirigente statistico	Collaborazione esterna
Fabio Piovanello	Componente GdL	Collaboratore tecnico	UOSD Sistemi informativi
Massimo Gola	Componente GdL	Dirigente analista	UOSD Sistemi informativi
Tullio Zampieri	Componente GdL	Dirigente amministrativo	Ufficio Affari Genrali/Privacy
Chiara Zambon	Componente GdL	Collaboratore Amministartivo esperto	Data Protection Officer Aziendale
Marzia Serafini	Componente GdL	Infermiere	UOS Qualità e Percorsi di Accreditamento

5. GLOSSARIO E ACRONIMI

Glossario	Definizione
Risorse Informatiche	Qualsiasi mezzo di comunicazione e elaborazione elettronica, hardware, software, rete, servizio e informazione in formato elettronico di proprietà dell'Azienda o in disponibilità o a essa concesso in licenza d'uso. Le risorse informatiche includono a titolo di esempio: -sistemi informatici a uso sanitario, amministrativo o tecnico (es. posta elettronica, accesso a Internet, applicativi aziendali quali Gestione di Reparto/cartella SIO, eRis, Galileo, Eusis, WebRainbow ecc.); -ogni sistema di elaborazione elettronica delle informazioni: server, personal computer fissi o portatili, tablet e similari (inclusi smartphone); -software di base e di ambiente: sistemi operativi, software di rete, sistemi per il controllo degli accessi, package, utility e similari; -software di produttività individuale (MS Office, LibreOffice, OpenOffice, Project, Visio ecc.); -ogni informazione elettronica registrata o conservata in file e banche dati (es. CD, nastri, dischi esterni ecc.); -ogni periferica: stampanti, scanner, plotter, apparecchiature per l'archiviazione elettronica dei dati, supporti di memorizzazione, video terminali; -ogni dispositivo di rete: concentratori, ripetitori, modem, switch, router, gateway, firewall, apparati VoIP e similari, access point, chiavette Internet; -ogni mezzo trasmissivo di cablaggio strutturato per reti locali, metropolitane e geografiche: cavi in fibra e in rame per dorsali e cablaggio orizzontale, permutazioni, attestazioni, patch e similari.

Utente	E' un individuo (dipendente, collaboratore a vario titolo o personale di ditte esterne) che ha accesso, mediante consegna di credenziali di abilitazione, a strumenti informatici o telematici collegati alla rete o ai sistemi dell'Azienda ed è espressamente autorizzato a effettuare trattamenti di dati attraverso applicazioni software.
Autorizzazioni	Le autorizzazioni sono concesse dal Responsabile del Sistema informativo o di Struttura che individua ambito e profilo di autorizzazione con comunicazione al SI, che provvede alle necessarie impostazioni a livello di sistema o di applicativo.
Trattamento	Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.
Interessato	La persona fisica cui si riferiscono i dati personali.
Dato personale	Qualsiasi informazione riguardante una persona fisica identificata o identificabile; si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale. Sono dati personali: nome e cognome, indirizzo, codice fiscale, foto, l'indirizzo IP o qualsiasi altra ripresa audiovisiva.
Dati particolari	Dati personali che, per la propria delicatezza, richiedono particolari cautele; sono quei dati idonei a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, i dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, nonché i dati relativi alla salute o all'orientamento sessuale della persona.
Dati relativi a condanne penali e reati	Dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza (quali dati personali idonei a rilevare provvedimenti emessi dalle Autorità Giudiziarie e contenuti nel casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reati e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli artt. 60 e 61 c.p.p.)
Comunicazione	Il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dell'Unione europea, dal responsabile o dal suo rappresentante nel territorio dell'Unione europea, dalle persone autorizzate, ai sensi

	dell'articolo 2-quaterdecies, al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione.
Diffusione	Dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione. Per soggetti indeterminati si intendono soggetti non identificabili a priori.
Archivio	Qualsiasi insieme strutturato analogico o digitale di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico.
Misure di sicurezza	Le misure tecniche e organizzative definite dal titolare del trattamento e adeguate al rischio insito nel trattamento effettuato.
Credenziali di autenticazione	Le credenziali di autenticazione sono le chiavi di accesso a strumenti informatici, procedure e dispositivi.
Password	E' la componente di una credenziale di autenticazione associata a una persona e solo a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica, da mantenere riservata.
Postazione di lavoro	Si considera "Postazione di Lavoro" un qualsiasi sistema collegato alla rete di comunicazione aziendale, dal quale sia possibile utilizzare applicazioni software, accedere ai dati conservati nei server aziendali o in cloud e navigare in Internet. Sono Postazione di Lavoro i personal computer, i tablet, gli smartphone, i thin client, i terminali e i dispositivi elettromedicali.
Prodotti e Servizi gestiti dal SI	Prodotti informatici realizzati ed implementati autonomamente e quelli per i quali la UOC/SI ha in gestione l'esecuzione di un contratto per l'approvvigionamento di beni e prestazione di servizi, nell'ambito del quale sono definite la manutenzione ordinaria, correttiva, adeguativa ed evolutiva dei sistemi.
Backup	Creazione di copie di sicurezza dei dati.
Acronimi	**Termini**
SI	UOSD Sistemi informativi
U.O.	Unità Operativa
DIR	Direttore di UOC/UOSD/UOS/Servizi
PdL	Postazioni di lavoro
QA	UOS Qualità e Percorsi di Accreditamento Istituzionale

6.DESCRIZIONE DELL'AMBITO DI ATTIVITÀ OGGETTO DELLA REGOLAMENTAZIONE E RESPONSABILITÀ

ART.1 PRINCIPI GENERALI

Gli strumenti informatici sono assegnati agli utenti/utilizzatori per lo svolgimento dell'attività lavorativa e devono essere utilizzati con modalità e mediante comportamenti adeguati ai compiti assegnati e alle responsabilità connesse, nel rispetto del presente regolamento, del Codice di comportamento aziendale e delle altre procedure e istruzioni operative interne.

Le risorse informatiche sono parte integrante del patrimonio dell'Azienda e rispettano i principi di:

- ✓ accessibilità: devono essere rese accessibili e utilizzate per gestire le attività aziendali, secondo le finalità autorizzate e definite dalla struttura aziendale di afferenza e inerenti alla propria mansione, nel rispetto dei principi di integrità e riservatezza, minimizzazione, esattezza, limitazione della conservazione;
- ✓ responsabilità: devono essere rese disponibili solo alle persone autorizzate e nei limiti di quanto necessario allo svolgimento dell'attività;
- ✓ sicurezza: devono essere protette mediante misure tecniche e organizzative adeguate, in modo da garantire la sicurezza dei dati personali dal rischio di trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali;
- ✓ gestione dati: i dati personali e gestionali, gestiti con risorse informatiche, sono trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»); sono raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo compatibile con tali finalità («limitazione della finalità»); sono adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»); sono esatti e aggiornati («esattezza»); sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati («limitazione della conservazione»); sono trattati in maniera da garantire una loro adeguata sicurezza, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).

ART.2 POSTAZIONI DI LAVORO

Le Postazioni di Lavoro (PdL) sono gestite da SI che le assegna agli utenti.

La PdL è provvista di software di sicurezza (software antivirus, personal firewall, software per aggiornamento automatico delle patch di sistema etc.).

L'assegnatario della PdL è profilato come utente senza diritti amministrativi.

La PdL è provvista del software base approvato dall'Azienda nonché, in relazione della propria attività lavorativa, dei software necessari per lo svolgimento della stessa.

Ulteriori necessità lavorative potranno essere presentate a SI, che valuterà l'ammissibilità delle richieste.

L'utente assegnatario della PdL è responsabile del suo corretto utilizzo nel rispetto delle seguenti regole comportamentali:

a) la PdL è assegnata all'utente per lo svolgimento della propria attività lavorativa ed è consentito l'uso ad altri utenti autorizzati con identificazione personale;
b) la PdL non deve essere accessibile a soggetti non autorizzati;
c) l'utente non deve apportare modifiche alle configurazioni della PdL che non siano state preventivamente richieste e autorizzate da SI;
d) tutto il personale ha l'obbligo di salvare la documentazione relativa alla propria attività lavorativa solo sugli spazi di condivisione aziendali;
e) durante l'allontanamento dalla PdL, l'utente deve bloccare la propria postazione per consentirne l'accesso unicamente mediante l'immissione della password;
f) al termine della giornata lavorativa, soprattutto per motivi di sicurezza, deve essere effettuato lo spegnimento delle PdL.

Le regole sopra citate valgono per tutte le tipologie di PdL. Si evidenzia che le PdL portatili, utilizzate al di fuori dell'Azienda, sono maggiormente esposte a rischi di sicurezza, quali danneggiamenti conseguenti agli spostamenti, furti, violazione della riservatezza delle informazioni contenute. Tutti gli utenti, pertanto, devono custodire con cura e diligenza la PdL assegnata. Le PdL devono essere verificate dal SI per l'installazione di eventuali aggiornamenti e/o patch di sicurezza. La verifica avviene mediante appuntamento concordato con il Servizio stesso. In caso di significativo rischio di compromissione o/e sicurezza, SI può richiedere all'utente lo spegnimento della PdL fino a verifica ovvero bloccare il dispositivo da remoto.

ART.3 NORME GENERALI PER L'UTILIZZO DEGLI STRUMENTI INFORMATICI

L'uso di tutti gli strumenti informatici aziendali è autorizzato per le sole finalità lavorative e professionali, nell'ambito della mansione e del profilo di autorizzazione previsto per l'utente.
Tutte le informazioni relative alle modalità di abilitazione agli applicativi aziendali sono disponibili sull'Intranet aziendale o tramite il servizio Help Desk (Telefono numero 0497300300).
Nell'esecuzione della propria attività lavorativa, gli utenti sono tenuti ad attenersi alle seguenti istruzioni generali:
a) effettuare la propria attività uniformandosi alle disposizioni dell'Azienda e alle istruzioni ricevute;
b) custodire con diligenza gli strumenti informatici loro affidati, segnalando tempestivamente alle strutture preposte, secondo le modalità previste, ogni danneggiamento, smarrimento o furto;
c) mantenere la riservatezza sulle informazioni e sui dati personali di cui siano venuti a conoscenza durante lo svolgimento della propria attività;
d) in caso di cessazione dal servizio o dalla prestazione svolta per l'Azienda, astenersi dalla diffusione di informazioni, dati e documenti acquisiti durante lo svolgimento della propria attività;
e) adottare ogni misura di sicurezza idonea a scongiurare rischi di perdita o distruzione (anche accidentale) dei dati.

ART.4 DIVIETI

Qualsiasi utilizzo degli strumenti informatici messi a disposizione dell'Azienda, che non sia relativo a finalità lavorative e professionali è vietato.
In particolare è fatto divieto di:

- ✓ introdursi abusivamente nei sistemi informatici aziendali;
- ✓ introdurre, installare, utilizzare programmi che non siano stati regolarmente acquistati, distribuiti e installati dalle preposte funzioni aziendali ai sensi del D.Lgs. n. 518/1992 sulla tutela giuridica del software e Legge n. 248/2000 nuove norme di tutela del diritto d'autore;
- ✓ rivelare la propria password di accesso alla rete aziendale, ad uno degli applicativi o servizi disponibili (inclusi i siti regionali o ministeriali);
- ✓ procurare a sé, o ad altri, profitto, o arrecare danni all'Azienda, procurandosi, riproducendo, diffondendo, o consegnando codici, parole chiave o altri mezzi idonei all'accesso ai sistemi informatici;
- ✓ riprodurre, duplicare e/o asportare, comunicare a terzi, diffondere i dati di cui l'Azienda è titolare del trattamento;
- ✓ riprodurre e asportare documentazione di qualsiasi tipo classificata riservata, compresi progetti, schede, prospetti, se non, per fini particolari, dietro esplicita autorizzazione del titolare dei relativi diritti (o di persona delegata);
- ✓ intercettare, impedire, interrompere le comunicazioni inerenti ai sistemi informatici.
- ✓ distruggere, deteriorare, rendere inservibili, del tutto o in parte, i sistemi informatici ovvero i programmi e le informazioni o i dati esistenti nei sistemi;
- ✓ riprodurre, duplicare e/o asportare programmi installati di cui l'Azienda è licenziataria o proprietaria;
- ✓ navigare nei siti internet non legati a finalità di lavoro/professionali e conservare nei sistemi e unità di memorizzazione assegnati, file, documenti, mail, immagini, video non legati alle finalità lavorative e professionali, in particolar modo di contenuto osceno, violento, offensivo alla morale o alla pubblica decenza, oltraggioso e/o discriminatorio;
- ✓ utilizzare *i* social media, forum, chat-line, instant messaging, Voice over IP *o* video chat per finalità diverse da quelle professionali o di formazione;
- ✓ utilizzare gli account di posta elettronica forniti dall'ULSS6, sia condivisi, sia personali, per l'iscrizione a siti di qualunque tipologia o natura non correlati a fini aziendali.
- ✓ fornire l'indirizzo email di ULSS6 come secondo indirizzo di conferma per l'iscrizione a siti di qualsiasi natura per scopi non aziendali.;
- ✓ adottare comportamenti che mettano a rischio la sicurezza del sistema informatico/informativo, inclusi i dati contenuti, o che pregiudichino o ostacolino le attività della collettività degli utilizzatori;
- ✓ archiviare file con riferimenti personali (es. nome e cognome) delle persone siano essi dipendenti oppure pazienti a cui si riferiscono i file stessi.

ART.5 ATTORI E RESPONSABILITA'

Vengono di seguito identificati gli attori interni ed esterni coinvolti nella gestione delle risorse informatiche e vengono definiti i relativi compiti e responsabilità:

A) DIR SI:

- ✓ è responsabile della progettazione del sistema e delle reti e stabilisce il livello di autorizzazioni e di controlli:
- ✓ provvede alle necessarie impostazioni a livello di sistema o di applicativo;
- ✓ è responsabile delle tecnologie dell'informazione e della comunicazione;

- ✓ verifica periodicamente l'attività degli Amministratori di Sistema attraverso audit interni, al fine di accertarne la conformità alle mansioni attribuite e la rispondenza alle misure organizzative, tecniche e di sicurezza previste dalle norme vigenti;
- ✓ redige annualmente la "Relazione sull'attività svolta dagli Amministratori di Sistema", i risultati degli audit interni, la conformità alle misure organizzative, tecniche e di sicurezza previste dalle norme vigenti, riportando in evidenza tutti gli interventi volti a migliorare il livello complessivo di sicurezza;
- ✓ è responsabile del governo del sistema informativo ovvero l'insieme delle attività promosse e gestite dal management e dai sistemi informativi, al fine di trovare la migliore integrazione possibile tra sistema, mission e politica aziendali, in un'ottica di riduzione dei rischi.

B) Amministratori di Sistema:
rappresentano il personale sistemistico e di networking e hanno accesso alle informazioni secondo le regole indicate nei documenti aziendali.
La nomina e il controllo degli amministratori di sistema è di responsabilità del Direttore SI. Sarà cura del RUP/DEC dei contratti, non gestiti direttamente dal SI, formalizzare la richiesta di nomina direttamente alla SI.

C) DIR Struttura (UOC/UOSD/UOS/servizio):
in forza della nomina a Delegato al trattamento dei dati personali è responsabile dell'applicazione del sistema a livello locale e individua uno o più utenti nell'ambito e profilo di autorizzazione e lo comunica al SI.
Con periodicità almeno annuale provvede alla verifica dell'ambito e del profilo di autorizzazione degli utenti assegnati alla propria struttura, comunicando al SI le eventuali variazioni.
Il Dir Struttura ha l'obbligo:

- ✓ di segnalare immediatamente al Direttore del SI eventuali situazioni di rischio della sicurezza dei sistemi e delle reti di comunicazione, al fine di tutelare il patrimonio informativo aziendale e garantire la necessaria continuità operativa;
- ✓ di vigilanza sugli operatori della propria struttura al fine di verificare l'effettivo adempimento della prestazione lavorativa e il corretto utilizzo degli strumenti di lavoro.

D) Utente
E' espressamente autorizzato a effettuare trattamenti di dati attraverso applicazioni software. Le autorizzazioni possono essere nominali o per funzione ovvero per appartenenza a uno specifico gruppo di lavoro. E' responsabile, civilmente e penalmente, del corretto uso delle risorse Informatiche, dell'utilizzo dei servizi e programmi ai quali ha accesso e dei dati personali che tratta.
Deve attenersi scrupolosamente alle istruzioni e raccomandazioni impartite dal delegato al trattamento, alle procedure operative indicate nei manuali d'uso, nelle istruzioni operative, negli aiuti in linea.
E' responsabile della protezione delle risorse a lui affidate ed ha il dovere di segnalare tempestivamente al proprio responsabile qualsiasi evento o situazione di rischio della sicurezza

dei sistemi e delle reti di comunicazione, al fine di tutelare il patrimonio informativo aziendale e garantire la necessaria continuità operativa.

E) Fornitori di prodotti e servizi

Sono coloro che provvedono all'approvvigionamento di beni o alla prestazione di servizi all'organizzazione.

In fase di aggiudicazione dell'appalto, il Direttore Generale, quale Titolare del trattamento dei dati, nomina Responsabile del trattamento dei dati nell'ambito del contratto/convenzione, la persona fisica che ha il potere di rappresentare il fornitore acquisendo la dichiarazione circa il possesso delle garanzie sufficienti per mettere in atto le misure tecniche ed organizzative adeguate in modo tale da soddisfare i requisiti di cui al Regolamento UE 679/2016 e garantire la tutela dei diritti dell'interessato. Il Responsabile è tenuto a dichiarare di accettare le regole e le procedure del presente regolamento. In caso di outsourcing di un servizio relativo a un sistema oppure a un applicativo, il Responsabile nomina il personale tecnico Amministratore di Sistema. Il Responsabile è tenuto a comunicare al Responsabile SI l'elenco degli Amministratori di Sistema nominati e autorizzati a effettuare il servizio relativo all'appalto.

ART.6 SISTEMI DI AUTENTICAZIONE E DI AUTORIZZAZIONE

Tutti coloro che per ragioni di lavoro devono avere accesso al sistema informatico aziendale devono essere intestatari di un nome utente all'interno del dominio di sicurezza aziendale, l'user ID di accesso corrisponde al Codice Fiscale dell'utente interessato.

L'Azienda si è dotata di un dominio unico e specifico AULSS 6. In alcuni casi, occorrono credenziali specifiche, per l'accesso ad alcune procedure aziendali o extra-aziendali (es. messe a disposizione da Azienda Zero).

Il trattamento di dati personali, con strumenti elettronici, è consentito ai soli utenti/utilizzatori autorizzati come sopra e dotati di credenziali di autenticazione. I requisiti di definizione della password sono conformi alle normative vigenti e alla tecnologia disponibile.

ART.7 COLLEGAMENTO DI APPARECCHIATURE ALLA RETE DATI

La rete dati aziendale su cavo o wireless (wi-fi) è gestita da SI.

L'accesso di computer o altre attrezzature alla rete aziendale deve essere autorizzato da SI, che definisce la connettività da assegnare in base alle caratteristiche dell'attrezzatura e alle esigenze dell'utilizzatore.

ART.8 UTILIZZO DELLA RETE INTERNET, INTRANET ED EXTRANET AZIENDALE

A ogni punto della rete Internet è visibile un numero identificativo (denominato indirizzo IP pubblico) che può anche essere utilizzato direttamente per l'accesso. La navigazione in internet è messa a disposizione del personale come fonte di informazione per le finalità di documentazione, ricerca e studio, utili per lo svolgimento della prestazione lavorativa. Qualsiasi operazione effettuata sulla rete esterna (accesso a siti web per necessità non inerenti all'attività lavorativa, salvataggio di file, partecipazione a forum, etc.) è posta sotto la responsabilità dell'utente, che deve mantenere un comportamento lecito e tale da non compromettere le attività e il buon nome dell'Azienda. Ogni utente è tenuto a osservare le seguenti regole comportamentali: utilizzare internet per fini leciti, astenendosi da qualsiasi comportamento che

possa avere natura oltraggiosa e/o discriminatoria verso terzi; trasferire sul proprio computer (download) solo file da siti web verificati e affidabili, tenendo presente che quando si trasferisce materiale da internet occorre prestare la massima attenzione al fine di non incorrere in violazioni di diritti di proprietà intellettuale; non utilizzare social network, forum, chat e simili per scambiare informazioni riservate o lesive dell'immagine dell'Azienda e dei colleghi; la navigazione in internet avviene in modalità trasparente e non anonima, soprattutto se attraverso intranet o strumenti aziendali; in ogni caso è vietato accedere a siti i cui contenuti non siano adeguati all'immagine e al buon nome dell'Azienda. Al fine di prevenire l'accesso a siti web e risorse internet potenzialmente nocivi, per la navigazione dalla rete aziendale l'Azienda adotta soluzioni di sicurezza basate su filtri e decriptazione delle informazioni della navigazione Internet attraverso i quali l'accesso a specifiche e determinate categorie di siti è bloccato a priori. Al fine di prevenire il download di file o pagine web contenenti codici malevoli, l'Azienda adotta soluzioni di sicurezza basate su tecnologie antimalware che effettuano la scansione dei contenuti della navigazione Internet e bloccano il download del contenuto in caso di rilevazione di codice malevolo.

L'Intranet è il sito interno aziendale che è costituito dal complesso sistema di informazioni e di servizi di utilità generale accessibili solo dalla rete interna. Tale sito può essere reso disponibile anche all'esterno della rete aziendale, in questo caso si parla di Extranet. Tutti i dipendenti e collaboratori aziendali hanno accesso alla rete Intranet o Extranet e devono costantemente prendere visione dei contenuti informativi.

ART.9 POSTA ELETTRONICA

L'utilizzo della casella di posta elettronica, gestita su dominio Google, costituisce un diritto e un dovere per ogni dipendente, pertanto, se non sussistono giustificati impedimenti, essa gli viene assegnata d'ufficio.
L'intestatario della casella è responsabile della costante lettura e dell'invio dei messaggi, ed è responsabile della custodia e dell'aggiornamento della password di accesso esclusiva a doppio fattore di autenticazione.
La casella di posta aziendale (nome.cognome@aulss6.veneto.it), sia essa individuale o di gruppo (condivisa), è uno strumento di lavoro che ha lo scopo di inviare/ricevere comunicazioni attinenti alla propria attività lavorativa quanto quello di ricevere comunicazioni/informazioni riguardanti l'Azienda e/o il proprio rapporto di lavoro; ciascun titolare di casella e-mail è, pertanto, direttamente responsabile del corretto utilizzo della stessa.
Non è quindi consentito l'utilizzo della posta elettronica aziendale, anche se l'account è individuale, per svolgere attività che non rientrino tra i compiti istituzionali. Sono vietati invii di messaggi ingiuriosi, minatori, lesivi dell'immagine dell'Azienda o che utilizzino linguaggi o immagini oscene, ingannevoli o diffamatorie nonchè l'utilizzo dell'indirizzo e-mail per l'iscrizione e/o la partecipazione a social network, mailing list, servizi di instant messaging, forum o altri servizi pubblici su internet di interesse personale e non lavorativo. Non è altresì consentito l'utilizzo dell'account aziendale su social.
Non è altresì ammesso l'utilizzo di caselle di posta private (es: @virgilio.it, @libero.it, @gmail.it ecc.).

Al termine della collaborazione lavorativa con l'Azienda per qualsiasi motivo (es. pensionamento, licenziamento, trasferimento presso altro datore di lavoro etc.), l'eventuale account nominativo di posta elettronica aziendale dell'Utente (di proprietà di ULSS6) sarà disattivato alla data di cessazione del rapporto di lavoro e di collaborazione. Alla disattivazione dell'account seguirà la cancellazione dell'indirizzo di posta elettronica aziendale. Le e-mail saranno conservate solo ai fini di tutela dei diritti in sede giudiziaria, nei limiti di cui all'art. 160-bis, c. 1 del D.Lgs. 196/2003.

ART.10 SERVIZI CLOUD E SPAZI DI CONDIVISIONE DI RETE AZIENDALE

Gli spazi di condivisione file server o cloud, devono essere utilizzati per la memorizzazione di file ad uso strettamente lavorativo. I file e i documenti di lavoro devono essere obbligatoriamente memorizzati nello spazio di condivisione apposito al fine di impedire la perdita di dati aziendali. In caso di comprovato pericolo per la sicurezza dei sistemi, SI potrà procedere, anche senza preavviso, alla rimozione di file e/o applicazioni presenti negli spazi di condivisione degli utenti, dandone successiva e tempestiva comunicazione agli interessati.

ART.11 UTILIZZO SISTEMI DI VIDEOCONFERENZA

L'Azienda mette a disposizione un completo sistema di videoconferenza all'interno della piattaforma GSuite denominato Meet. Tale sistema deve essere utilizzato necessariamente per le videocomunicazioni tra dipendenti, collaboratori e soggetti terzi invitati in riunioni o incontri in remoto organizzate da personale dell'Azienda. È ammesso l'utilizzo di altri sistemi diversi da Meet esclusivamente se si è invitati a eventi o videochiamate gestite da organizzatori esterni all'Azienda e solo attivando connessioni web e non installando programmi dedicati. In questo caso la verifica del rispetto delle norme di sicurezza è in carico al partecipante. Ogni eccezione a quanto qui indicato deve essere autorizzata.

ART.12 UTILIZZO DELLO SMARTPHONE AZIENDALE

Al fine di assicurare il servizio di pronta reperibilità e lo svolgimento dell'attività istituzionale, l'Azienda fornisce smartphone aziendali ai propri dipendenti, previa valutazione da parte del relativo del DIR di Dipartimento o di macrostruttura. Il telefono e gli eventuali cellulari aziendali devono essere utilizzati per scopi puramente lavorativi.

ART.13 UTILIZZO IN AZIENDA DI DISPOSITIVI DI TELECOMUNICAZIONE, RADIOMOBILI O WIRELESS

A causa della concreta possibilità che le attrezzature informatiche ed elettromedicali aziendali siano soggette a malfunzionamenti legati alla presenza di sorgenti di campi elettromagnetici (es. dispositivi mobili con connessione di tipo wireless),l'Azienda mette a disposizione di tutti gli operatori aziendali delle raccomandazioni nel documento "Raccomandazioni per l'utilizzo in azienda di dispositivi di telecomunicazione radiomobili o wireless" presente nella Intranet.

ART.14 SALVATAGGIO DEI DATI

La SI provvede al salvataggio dei dati registrati tramite i sistemi informativi aziendali centralizzati. La politica di backup definisce la frequenza di salvataggio e il tempo di tenuta dei backup e viene adottata da SI in linea con indicazioni normative, raccomandazioni e best practice.

ART.15 ACCESSIBILITA'

L'Azienda promuove e favorisce la diffusione dell'accessibilità degli strumenti informatici all'interno dell'azienda nel pieno rispetto delle disposizioni della normativa e delle indicazioni di AgID.

ART.16 ASSISTENZA E INTERVENTI MANUTENTIVI

In caso di assistenza è attivo un servizio di HELP DESK contattabile preferibilmente via mail help.desk@aulss6.veneto.it o al numero di telefono 0497300300.

Per poter fornire assistenza e supporto tempestivi nel caso di guasti e malfunzionamenti, su ciascun computer fisso o portatile è installata un'applicazione che consente ai tecnici del UOSI di collegarsi da remoto, senza bisogno di intervenire sul luogo. Solo nel caso di mancata soluzione del problema in modalità remota, viene effettuato un intervento in loco.

La SI si impegna a fornire continuità ai servizi erogati, riservandosi la possibilità di interromperli esclusivamente per le manutenzioni ordinarie e cercando di arrecare il minor disagio possibile agli utenti. Salvo impedimenti, le interruzioni saranno comunicate agli utenti. L'Azienda si riserva la possibilità di interrompere i servizi informatici per le manutenzioni ordinarie e straordinarie e per la gestione dei guasti, impegnandosi tuttavia, nel limite del possibile, ad avvertire preventivamente gli utenti di dette interruzioni.

ART.17 PROCEDURE TRASVERSALI/OPERATIVE, ISTRUZIONI OPERATIVE SPECIFICHE E MODULISTICA

Le procedure sono sviluppate, raccolte e diffuse a cura del SI. Nella piattaforma Intranet ed Extranet aziendale sono contenute le ultime versioni aggiornate. Al fine di evitare disallineamenti nella distribuzione delle procedure è sconsigliata la stampa: è necessario fare riferimento sempre all'ultima versione digitale pubblicata nella piattaforma Intranet ed Extranet. Ogni documento è redatto secondo la Procedura Trasversale aziendale "Elaborazione e gestione dei documenti aziendali". La modulistica di riferimento aggiornata all'ultima revisione è reperibile nella Intranet aziendale.

ART.18 CONTROLLI DI SISTEMA

Le attività di controllo e vigilanza sono fondate sul principio della "proporzionalità" che si concretizza nella pertinenza e non eccedenza del controllo; pertanto, i mezzi e l'ampiezza del controllo sono proporzionati agli scopi che, nello specifico, sono quelli di garantire la massima sicurezza del sistema informatico e l'appropriato utilizzo delle risorse.

L'Azienda si riserva il diritto di effettuare controlli specifici tesi ad accertare lo stato dei fatti relativamente all'uso delle attrezzature aziendali nel caso in cui accerti manomissioni alle configurazioni del sistema informatico, telematico, telefonico aziendale e/o accessi indebiti allo stesso, ovvero riscontri diffusioni indebite di informazioni atte a pregiudicare la sicurezza del sistema stesso o il suo buon funzionamento e/o a garantire ad altri accessi o altri privilegi non dovuti, o ancora abbia concrete ragioni che portino a pensare che la sicurezza del sistema tecnologico aziendale possa essere minacciata.

Vengono effettuati ulteriori controlli periodici ed a campione, come descritto nella procedura disponibile nella intranet aziendale, sia nelle email che negli accessi nei limiti imposti dalla

finalità' del trattamento su motivi specifici tra i quali in particolare verifiche anche ex post dirette ad accertare comportamenti del dipendente illeciti e lesivi del patrimonio o all'immagine dell'Azienda.
In caso di anomalie l'Azienda può disabilitare le autorizzazioni all'accesso e all'uso delle apparecchiature aziendali, segnalare al responsabile organizzativo situazioni e comportamenti anomali degli operatori, presentare denuncia all'autorità giudiziaria, in caso di reati perseguibili d'ufficio.
In caso di problemi inerenti alla sicurezza della infrastruttura tecnologica l'Azienda si riserva il diritto di adottare tutte le misure tecniche che garantiscano la gestione della contingenza, ad esempio isolando dalla rete stazioni che siano state infettate da virus che ne pregiudichino il buon funzionamento, aggiornando configurazioni software e/o hardware ecc. Tutte le azioni messe in atto sono valutate in una logica di costo/beneficio e sono improntate a un criterio di minimizzazione del disservizio. L'Azienda si riserva la facoltà di sospendere l'accesso ai servizi qualora, anche a seguito di segnalazioni del DIR di struttura, sussistano nel tempo reiterate evidenze delle inadempienze da parte dell'operatore.

ART.19 FORMAZIONE

L'Azienda prevede sessioni formative e aree dedicate alla formazione. In tali aree si potranno reperire varie risorse per accrescere le proprie competenze e migliorare la gestione delle informazioni aziendali. La formazione viene programmata al momento dell'ingresso in servizio, in occasione di cambiamenti di mansioni o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali. I corsi di formazione previsti non sono facoltativi e la mancata ed ingiustificata assenza può portare a provvedimenti di natura disciplinare.

ART.20 SANZIONI

Le operazioni effettuate in palese non conformità al presente Regolamento e al codice di comportamento aziendale, esporranno i trasgressori alle sanzioni disciplinari, civili e penali previste dalla normativa vigente. Ogni DIR, qualora rilevi Il mancato rispetto o la violazione di quanto previsto dal presente Regolamento, è tenuto ad attivare le procedure per l'avvio del procedimento disciplinare o a dare tempestiva comunicazione dell'illecito al Direttore Generale per le eventuali segnalazioni alle autorità competenti.
Resta ferma la responsabilità civile, penale e contabile di ogni utente per fatti illeciti e/o danni derivanti da usi non consentiti della rete o degli strumenti informatici messi a disposizione dall'Azienda.

ART.21 FINALITA' E TRATTAMENTO DEI DATI

L'Azienda si impegna a trattare i dati relativi all'utilizzo dei servizi informatici unicamente per motivi volti a garantire la sicurezza e il corretto funzionamento dei servizi informatici e per finalità direttamente pertinenti all'attività lavorativa del dipendente.
Le operazioni effettuate servendosi delle credenziali di autenticazione potranno essere memorizzate per finalità di sicurezza del sistema.
L'attività di registrazione avviene attraverso i file "log" di sistema a cura del SI o dell'articolazione aziendale che detiene la responsabilità organizzativa dei sistemi o servizi.

Per quanto riguarda l'utilizzo dei sistemi informativi aziendali, le operazioni effettuate servendosi delle credenziali di autenticazione potranno essere memorizzate al fine di garantire la tracciabilità del trattamento dei singoli dati.
Le informazioni relative alla tracciabilità del dato (inserimento, modifica, cancellazione) vengono gestite con le stesse modalità del dato a cui si riferiscono. Le registrazioni potranno essere utilizzate per finalità statistiche e di valutazione della qualità in riferimento a taluni servizi erogati, esclusivamente da parte di personale dell'Azienda appartenente a SI ed esclusivamente in formato anonimo e/o aggregato.
L'Azienda garantisce che i dati informatizzati da essa gestiti, nonché i sistemi di elaborazione dati e gli strumenti di telecomunicazioni, non saranno utilizzati per il controllo a distanza dei lavoratori (artt. 113, 114, 171 Codice Privacy; artt. 4 e 8, L. 20 maggio 1970, n.300 - Statuto dei Lavoratori), se non nei limiti consentiti dallo Statuto dei Lavoratori, così come modificato dal D. Lgs. 151/2015 [Jobs Act] e s.m.i. e comunque previa informativa ai dipendenti interessati.
I dati relativi all'utilizzo degli strumenti informatici sono trattati esclusivamente dagli operatori del SI, per le finalità indicate al punto precedente. In applicazione delle procedure e delle disposizioni aziendali, in particolare in materia disciplinare, i log potranno essere oggetto di comunicazione ai soggetti aventi funzioni ispettive e di controllo all'interno dell'Azienda e, laddove ne ricorrano i presupposti di legge, all'Autorità giudiziaria.

7.DIFFUSIONE, CONSERVAZIONE E ARCHIVIAZIONE

La diffusione del presente documento viene effettuata dalla QA/U.O attraverso:

- News aziendale;
- Intranet al link https://intranet.aulss6.veneto.it/pages/docbrowser sezione "Documenti"
- Via mail ai DIR e coordinatori di UUOO

Il documento originale è conservato presso la QA (una copia nella U.O redattrice) e archiviato secondo le indicazioni fornite dal Documento Massimario di scarto aziendale. La QA garantisce l'eliminazione dal sito intranet dei documenti "superati".

8.RIFERIMENTI BIBLIOGRAFICI, NORMATIVI E SITOGRAFIA

✓ Raccomandazione del Consiglio dell'OCSE nella sua 1037ª sessione del 25 luglio 2002;
✓ Provvedimento del Garante per la Protezione dei Dati personali del 13 ottobre 2008 "Rifiuti di apparecchiature elettriche ed elettroniche (Raee) e misure di sicurezza dei dati personali";
✓ Legge 23 dicembre 1993 n. 547- "Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica";
✓ Direttiva n. 2/2009 della Presidenza del Consiglio dei Ministri-Dipartimento della funzione pubblica: "Utilizzo di Internet e della casella di posta elettronica istituzionale sul luogo di lavoro";
✓ Deliberazione 13 del 1 Marzo 2007 "Lavoro: le linee guida del Garante per posta elettronica e internet";
✓ Legge n° 300 del 20/05/1970 e s.m.i cd "Statuto dei lavoratori";
✓ Direttiva 27 novembre 2003 del Dipartimento per le innovazioni e la tecnologia "Impiego della posta elettronica nelle pubbliche amministrazioni";
✓ 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";

- ✓ Decreto Legislativo 7 marzo 2005 n. 82 "Codice dell'amministrazione digitale" e s.m.i.;
- ✓ Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE("Regolamento Generale sulla Protezione dei Dati personali");
- ✓ D. Lgs. 196/2003 come modificato dal D.Lgs.101/2018 "Codice in materia di protezione dei dati personali";
- ✓ Direttiva del 18 novembre 2005 "Linee guida per la Pubblica amministrazione digitale";
- ✓ Circolari AgID n° 1 e 2/2017[1];
- ✓ Piano triennale AgID;
- ✓ CCNL delle tre aree contrattuali: Comparto sanità- Dirigenza Enti locali e Dirigenza sanità;
- ✓ Codice di comportamento aziendale;
- ✓ Principali riferimenti aziendali;
- ✓ Delibera n° 520 del 22/07/2020 Adozione Piano Operativo per l'applicazione di alcuni adempimenti previsti dal Regolamento Europeo (UE) 2016/679 in materia di trattamento dati personali;
- ✓ POLA aziendale.

9.TEMPI DI ENTRATA IN VIGORE

Il Regolamento entra in vigore dal mese di Gennaio 2022.

[1] http://www.gazzettaufficiale.it/eli/id/2017/05/05/17A03060/sg

REGIONE DEL VENETO

ULSS6 EUGANEA

ATTESTAZIONE DI PUBBLICAZIONE

La presente deliberazione è stata pubblicata all'Albo On-line di questa ULSS 6 per 15 giorni consecutivi dal 24-01-2022

Il Direttore
U.O.C. Affari Generali
(Dott. Tullio Zampieri)

CERTIFICAZIONE DI ESECUTIVITA'

La presente deliberazione è divenuta esecutiva il 24-01-2022

Il Direttore
U.O.C. Affari Generali
(Dott. Tullio Zampieri)

Copia composta di n. 0022 fogli (incluso il presente) della delibera n. 51 del 21-01-2022 firmata digitalmente e conservata secondo la normativa vigente presso Infocert S.p.a.

Padova, li 24-01-2022

Il Direttore
U.O.C. Affari Generali
(Dott. Tullio Zampieri)
