AZIENDA SANITARIA PROVINCIALE

Regolamento aziendale per l'uso degli strumenti informatici, Internet, posta elettronica e per la tutela dei sistemi informativi. Istruzioni operative per Delegati e Autorizzati in materia di trattamento di dati personali

Approvato con delibera n.°_____ del_____	**Data versione _____**	**Versione**	**1.0**

INDICE

1. Premessa

L'Azienda Sanitaria Provinciale di Ragusa (più avanti Azienda) con il presente Regolamento si propone l'obiettivo di salvaguardare il proprio patrimonio informativo aziendale, inteso quale complesso di risorse informatiche e di informazioni di cui dispone, dettando le procedure e le istruzioni per una sua corretta e adeguata gestione.

Tale Regolamento si inquadra nell'ambito delle misure tecniche ed organizzative adottate dall'Azienda per fare fronte ad esigenze di sicurezza nel trattamento dei dati personali e per minimizzare il rischio di violazioni dei dati (*data breach),* nel rispetto del Regolamento Europeo 2016/679.

In tale ottica, il presente documento si inquadra nei principi contenuti nell'art. 32 del Regolamento UE n.679/2016 (più avanti GDPR), recante *"Sicurezza del trattamento"*, ai sensi e per effetto del quale, il trattamento dei dati personali in Azienda deve essere assistito da adeguate misure di sicurezza **al fine di attuare efficacemente i principi di protezione dei dati, secondo l'art. 5 GDPR:**

- liceità, correttezza e trasparenza del trattamento, nei confronti dell'interessato;
- limitazione della finalità del trattamento, cioè i dati vanno raccolti e trattati per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non siano incompatibili con tali finalità;
- minimizzazione, vale a dire i dati devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
- esattezza, per il quale i dati devono essere esatti e, se necessario, aggiornati, adottando tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;
- limitazione della conservazione, ossia è necessario che i dati vengano conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore a quello necessario rispetto agli scopi per i quali viene effettuato il trattamento;
- integrità e riservatezza, ossia occorre garantire un'adeguata sicurezza e protezione dei dati, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali;
- principio di necessità, secondo cui i sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi in relazione alle finalità perseguite, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante dati anonimi od opportune modalità che permettano di indentificare l'interessato solo in caso di necessità;
- principio di pertinenza e non eccedenza, vale a dire che i trattamenti vanno effettuati per finalità determinate, esplicite e legittime, nella "misura meno invasiva possibile".
- principio di trasparenza il quale impone che le informazioni e comunicazioni relative al trattamento di tali dati personali siano facilmente accessibili e comprensibili e che sia utilizzato un linguaggio semplice e chiaro.

Ai fini di questo regolamento si specifica che con il termine **"dati"** deve intendersi l'insieme più ampio di informazioni di cui un dipendente o un collaboratore (a prescindere dal rapporto contrattuale con l'Azienda) può venire a conoscenza e delle quali deve garantire la riservatezza e la segretezza e non solo i dati personali intesi a norma di legge.

E' responsabilità di tutti i soggetti che utilizzano il personal computer ed altri dispositivi elettronici, la posta elettronica e internet, messi a disposizione dell'Azienda, applicare e rispettare puntualmente le disposizioni del presente Regolamento.

In linea generale, ogni dato, nell'accezione più ampia prima detta, del quale si viene a conoscenza, nell'ambito dell'attività lavorativa, è da considerarsi riservato e non deve essere comunicato o diffuso a nessuno, salvo specifica ed esplicita autorizzazione dell'Azienda.

Anche fra colleghi oppure fra dipendenti e collaboratori esterni è necessario adottare la più ampia riservatezza nella comunicazione dei dati conosciuti, limitandosi solo a quei casi che si rendono necessari per espletare al meglio l'attività lavorativa richiesta.

Copia del presente Regolamento viene pubblicata sul sito internet aziendale al link "Protezione dati personali" e consegnata a ciascun dipendente all'atto dell'assunzione ed a ciascun collaboratore ad inizio attività.

Il Regolamento potrà essere aggiornato ogniqualvolta se ne presenti l'opportunità e di tali revisioni sarà data tempestiva comunicazione.

2. Riferimenti normativi

Le presenti regole di sicurezza hanno valenza per l'Azienda e si pongono l'obiettivo di fornire agli utenti idonee misure di sicurezza e linee di comportamento adeguate per utilizzare in modo conforme e non rischioso i dispositivi informatici aziendali, la posta elettronica aziendale e la navigazione in internet.

Il presente Regolamento è adottato in conformità:

- al Regolamento Generale sulla Protezione dei Dati (GDPR) UE n.679/2016;

- al D.Lgs 30 giugno 2003 n.196 "Codice in materia di protezione dei dati personali" come modificato e integrato dal D.Lgs n. 101/2018;

- Provvedimento del Garante per la protezione dei dati personali "Linee guida per posta elettronica e Internet" del 1° marzo 2007;

- Provvedimento del Garante "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema- del 27 novembre 2008;

- Provvedimento del Garante "Modifiche del provvedimento del 27 novembre 2008 recante prescrizioni ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni di amministratore di sistema e proroga dei termini per il loro adempimento" del 25 giugno 2009;

- Provvedimento del garante "Rifiuti di apparecchiature elettriche ed elettroniche (Raee) e misure di sicurezza dei dati personali" del 13 ottobre 2008;

-Direttiva n. 2/2009 del Dipartimento della Funzione Pubblica recante "Utilizzo di Internet e della casella di posta elettronica istituzionale sul luogo di lavoro";

- Legge 20 maggio 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";

- D.Lgs n.151/2015 (c.d. Jobs Act), art. 23 che modifica la fattispecie integrante il divieto dei controlli a distanza

Campo di applicazione

Il presente regolamento si applica ad ogni *Utente* a vario titolo (dipendente, borsista, tirocinante, collaboratore, libero professionista, stagista, ecc..) autorizzato al trattamento dei dati.
In particolare, con riferimento alle istruzioni relative all'utilizzo di strumenti informatici, internet e posta elettronica, si applica ad ogni *Utente* autorizzato all'uso di beni aziendali informatici, quali PC, tablet, smartphone, internet, posta elettronica, ecc.

Nel caso di autorizzazione da parte della Azienda all'utilizzo per motivi di lavoro di dispositivi di proprietà dell'*Utente* (ad es. *smart-working*), la presente policy aziendale di sicurezza è estesa anche a tali dispositivi personali, per quanto compatibile.

L'Utente è tenuto ad un comportamento consapevole, ispirato ai principi di diligenza, fedeltà, correttezza ed idoneo a preservare l'integrità delle risorse aziendali e la riservatezza delle informazioni, nel rispetto degli obblighi di cui agli articoli 2104 e 2105 del codice civile e della normativa vigente in materia di protezione dei dati personali.

La mancata osservanza delle disposizioni contenute presente Regolamento può comportare gravi danni all'Azienda e in quanto tale, pertanto, costituisce, per tutti i soggetti sopra richiamati, un grave inadempimento dei compiti assegnati e potrebbe avere gravi conseguenze sia sotto il profilo disciplinare, sia sotto il profilo civilistico, sia sotto il profilo penale, con conseguente risarcimento di eventuali danni causati all'Azienda stessa ed a terzi (art. 20 del presente regolamento).

3. Oggetto e Finalità

Il presente Regolamento ha per oggetto le politiche di sicurezza dettate per un utilizzo corretto del sistema informativo dell'Azienda da parte dell'*Utente* ed è pertanto finalizzato a:

a) garantire la sicurezza, l'integrità, la disponibilità e la riservatezza del sistema informativo;

b) tutelare i beni ~~aziendali~~ (beni e risorse informatiche, servizi ICT e reti informatiche, informazioni cartacee) dell'Azienda;

c) assicurare la mitigazione del rischio di *data breach* (*violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati),* per prevenire ed evitare condotte inconsapevoli, scorrette o illecite da parte degli Utenti che potrebbero esporre l'Azienda a sanzioni amministrative, danni patrimoniali e di immagine.

4. Gestione degli strumenti Informatici

4.1. Prescrizioni di carattere generale

Gli strumenti informatici sono il complesso di **dispositivi fisici** (PC, stampanti, lettori portatili, smartphone, ed altri devices) messi a disposizione dell'*Utente* per il perseguimento degli obiettivi aziendali. Sono strumenti di lavoro, in quanto utilizzati dal *lavoratore per rendere la prestazione lavorativa.* **Ogni *Utente,* pertanto, è tenuto ad usarli esclusivamente per ragioni di servizio ed è responsabile dell'integrità e della custodia dei dispositivi fisici e delle informazioni/dati allo stesso affidati dall'Azienda.**

Ad ogni dispositivo è associato un numero di inventario, la collocazione fisica e l'Utente, allo scopo di curare il parco dispositivi aziendale e definire le responsabilità in caso di furto, smarrimento o guasto volontario.
Qualsiasi spostamento permanente del dispositivo (es. trasloco, assegnazione ad altro reparto, assegnazione ad altro professionista) deve essere concordata con il Responsabile del Servizio Patrimonio e con il Referente Informatico e/o con l'Amministratore di sistema allo scopo di consentirne la tracciabilità.

Qualora occorra, i dispositivi possono anche essere utilizzati in condivisione con qualsiasi operatore dell'Azienda, con la previsione della sessione individuale di lavoro per ogni utente e specifiche credenziali di identificazione ed autenticazione.

L'installazione di sistemi operativi e programmi applicativi sui personal computer avviene ad opera dei tecnici informatici incaricati; il Personal Computer è, quindi, fornito all'Utente con una **configurazione software predefinita che non può essere dallo stesso modificata autonomamente.**
L'uso di tali programmi deve avvenire nel rispetto dei contratti di licenza che li disciplinano e delle specifiche prescrizioni di volta in volta indicate.

La configurazione dei profili abilitativi di tutti gli utenti aziendali è eseguita con privilegi che non consentono l'installazione o l'esecuzione di programmi non autorizzati sulle macchine client e sui server.

Tutti i software caricati sul sistema operativo ed in particolare i software necessari per la protezione dello stesso o della rete internet (quali antivirus o firewall) non possono essere disinstallati o in nessun modo manomessi dagli Utenti (salvo quando questo sia richiesto dall'amministratore di sistema per compiere attività di manutenzione o aggiornamento).

Nell'uso dei dispositivi informatici, quali strumenti di lavoro, l'*Utente* è tenuto alle seguenti prescrizioni di carattere generale:

- utilizzare i dispositivi fisici con consapevolezza, appropriatezza e professionalità unicamente per finalità compatibili con le attività aziendali;
- custodire con cura e diligenza i dispositivi fisici per evitare la sottrazione, la distruzione o il danneggiamento;
- in caso di furto, smarrimento, malfunzionamento o guasto, effettuare la immediata segnalazione (al massimo entro 24 ore dalla conoscenza dell'evento) al Titolare, al Delegato del trattamento ed al *Data Protection Officer*, seguendo la procedura aziendale per il *Data Breach* pubblicata sul sito aziendale nel Link "Protezione dati personali". Tale adempimento è necessario sia per ripristinare il dispositivo, sia per ottemperare agli obblighi imposti dal Regolamento Europeo 2016/679 (eventuale notifica al Garante entro 72 ore ed agli interessati), sia per effettuare le eventuali denunce agli Enti competenti (Autorità giudiziaria, ecc.);
- è fatto assoluto divieto di cedere in uso, anche temporaneo, le attrezzature e i beni informatici aziendali a soggetti terzi, di rimuovere, danneggiare o asportare componenti hardware, ovvero di modificare la configurazione hardware e software del proprio dispositivo;
- non è consentito utilizzare strumenti potenzialmente in grado di consentire accessi non autorizzati alle risorse informatiche.

4.2 Prescrizioni sull'utilizzo di Personal Computer, PC Portatili e Tablet

- E' vietato collegare alla rete aziendale Personal Computer, PC portatili ed altri dispositivi hardware che non appartengano all'Azienda, senza l'autorizzazione dell'Azienda stessa, del Referente Informatico e/o dell'Amministratore di sistema;
- è vietato l'uso di programmi diversi da quelli distribuiti ed installati ufficialmente dall'Amministratore di sistema o dal Referente Informatico; l'inosservanza di questa disposizione, infatti, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre a gravi responsabilità civili, oltre che penali in caso di violazione della normativa a tutela dei diritti d'autore sul software; eventuali abusi o utilizzi illeciti saranno puniti conformemente alle disposizioni che disciplinano il rapporto di lavoro. In ogni caso, l'Utente sarà tenuto a manlevare e tenere indenne l'Azienda da qualsiasi danno o richiesta di risarcimento che venga avanzata da soggetti terzi.
- non lasciare incustodita la postazione di lavoro con la sessione utente attiva;
- in caso di allontanamento dalla propria postazione di lavoro, spegnere il PC o bloccare tastiera e schermo con un programma salvaschermo (screensaver) protetto da password, ovvero disconnettersi, effettuando il log-out dalla sessione;
- al termine del lavoro spegnere il proprio dispositivo;
- eseguire il backup periodico (almeno settimanale) dei dati secondo le indicazioni dell'Amministratore di sistema; nel caso di salvataggio su supporto magnetico rimovibile l'Utente deve sostituire periodicamente tali supporti e provvedere alla loro conservazione in un luogo sicuro;
- non caricare o inserire all'interno del dispositivo fisso o portatile dati personali non attinenti con l'attività lavorativa svolta; in ogni caso, prima della riconsegna di tali dispositivi per restituzione o riparazione, gli Utenti sono obbligati a cancellare tutti i dati personali eventualmente presenti;
- utilizzare sistemi di cifratura dei dati personali, al fine di evitare l'accesso di soggetti non autorizzati in caso di furto o smarrimento; l'Utente dovrà dare tempestiva comunicazione nel caso in cui, per qualsiasi motivo, abbia fondati motivi di ritenere che possa essere compromessa la riservatezza della password, o comunque ne sia stato fatto un utilizzo indebito.
- Nell'ipotesi di assenza o impossibilità, temporanea o protratta nel tempo, qualora per ragioni di sicurezza o comunque per garantire l'ordinaria operatività aziendale sia necessario accedere a informazioni o documenti di lavoro presenti sul personal computer assegnato, inclusi i messaggi di posta elettronica in entrata e in uscita, l'Utente può delegare a un suo fiduciario il compito di verificare il contenuto di messaggi e inoltrare al responsabile dell'area in cui lavora quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa (così come indicato nelle "Linee guida del Garante su posta elettronica e internet" del 01/03/2007). Di tale attività deve essere redatto apposito verbale e informato il dipendente interessato alla prima occasione utile.

  Nel caso in cui l'Utente non abbia delegato un suo fiduciario, il responsabile della struttura a cui è assegnato, può richiedere con apposita e motivata richiesta all'amministratore del sistema di accedere alla postazione e/o alla casella di posta elettronica dell'Utente assente, in modo che si possa prendere visione delle informazioni e dei documenti necessari. Contestualmente il Responsabile della struttura, appena possibile, deve informare l'Utente dell'avvenuto accesso fornendo adeguata spiegazione e redigendo apposito verbale.
- Per finalità di assistenza, manutenzione e aggiornamento e previo consenso esplicito del dipendente stesso, l'amministratore di sistema o soggetti appositamente incaricato allo svolgimento di tale attività, potranno accedere da remoto al personal computer del dipendente attraverso un apposito programma software.

4.3. Prescrizioni sull'utilizzo di stampanti e fotocopiatori

- Stampare documenti solo se strettamente necessari per lo svolgimento dell'attività lavorativa;
- utilizzare le stampanti di rete in luogo di quelle locali per ridurre i materiali di consumo;
- spegnere le stampanti in caso di inutilizzo ed a fine giornata lavorativa;
- in caso di stampante condivisa, qualora possibile, attivare la funzione che genera un PIN da digitare sulla stampante per sbloccare la stampa al momento del ritiro. In ogni caso, evitare di lasciare le stampe incustodite e ritirare immediatamente le copie non appena stampate, in modo che non possano venirne a conoscenza persone non autorizzate.

4.4. Prescrizioni sull'utilizzo di supporti rimovibili

I supporti rimovibili sono quei dispositivi che consentono di copiare o archiviare dati, files o documenti esternamente al computer (CD-ROM, DVD, penne o chiavette USB, hard disk portatili, ecc.). L'uso di supporti di memorizzazione rimovibili è in via generale sconsigliabile.
Qualora il loro utilizzo si renda assolutamente necessario, l'Utente è tenuto ad adottare le seguenti cautele:

- utilizzare i dispositivi rimovibili aziendali esclusivamente su computer aziendali;
- prima dell'uso, sottoporre sempre tutti i supporti di origine esterna a scansione antivirus/antimalware con un programma antivirale aggiornato ed avvertire immediatamente l'Amministratore di sistema del rilevamento di virus o malware di qualsiasi natura;
- qualora vi sia la assoluta necessità di memorizzare su dispositivi rimovibili dati particolari, l'Utente è tenuto ad adottare sistemi di crittografia, avendo cura di permettere la lettura solo agli aventi diritto, ovvero, in mancanza, utilizzare sistemi di pseudonimizzazione (ad esempio, contrassegnando i documenti semplicemente con un codice) o sistemi di anonimizzazione;
- custodire con cura i supporti rimovibili su cui sono memorizzati dati personali in armadi chiusi a chiave, al fine di evitare che il contenuto possa essere trafugato, o alterato, e/o distrutto, ovvero conosciuto da terzi non autorizzati ad accedervi;
- procedere alla cancellazione "sicura" dei dati personali presenti sui supporti magnetici od ottici, prima del loro riutilizzo;
- consegnare i supporti magnetici obsoleti (dischetti, nastri, chiavi USB, CD riscrivibili ed altro) all'Amministratore di sistema per l'opportuna distruzione, onde evitare che il loro contenuto possa essere recuperato successivamente alla cancellazione.

4.5. Prescrizioni in materia di sicurezza privacy per lo *smart working* /lavoro agile

L'Azienda può mettere a disposizione degli Utenti la possibilità di accedere alle proprie risorse informatiche anche dall'esterno mediante rete VPN (Virtual Private Network), un canale privato e criptato verso la rete interna.
Anche in tal caso l'Utente (ad es. *smart-worker*) è tenuto a conformarsi a tutte le prescrizioni di sicurezza dettate nel presente Regolamento, per quanto compatibili.

Inoltre, l'Utente abilitato ad accedere alle risorse informatiche aziendali dall'esterno è tenuto a:

- individuare uno spazio idoneo per predisporre la propria postazione lavorativa da utilizzare in modo esclusivo, ponendo ogni cura per evitare che ai dati possano accedere persone non autorizzate;
- assicurarsi della conformità delle prese elettriche prima di utilizzarle per alimentare il dispositivo o i dispositivi aziendali;

- assicurarsi che la postazione scelta non possa essere investita da acqua, fuoco, vento, calore eccessivo;
- non lasciare incustodita la postazione di lavoro e riporre gli strumenti di lavoro in armadietti chiusi a chiave al termine di ogni sessione lavorativa; usare meccanismi (cifratura dei dati, pasword di sicurezza, ecc.) che consentano di inibire la possibilità di accesso ai dati a chi dovesse entrarne in possesso;
- bloccare l'elaboratore in dotazione in caso di allontanamento dalla propria postazione di lavoro, anche per un intervallo molto limitato;
- adoperare "misure di sicurezza" nell'utilizzo di pc o tablet come para schermi (privacy-screen) che impediscano la visuale laterale al vicino;
- non condividere con i colleghi documenti aziendali o attività lavorative su piattaforme come Google document, ovvero altre simili e/o comunque piattaforme diverse da quella aziendale o da quella indicata dal datore di lavoro;
- utilizzare il dispositivo aziendale solo ed esclusivamente per le attività lavorative;
- a conclusione della prestazione lavorativa giornaliera conservare e tutelare i documenti eventualmente stampati, provvedendo alla loro eventuale distruzione con particolare accuratezza, utilizzando appositi apparecchi "distruggi documenti" o, in mancanza, sminuzzandoli in modo da non renderli più ricomponibili.

Qualora l'Utente (*smart-worker*) sia anche autorizzato all'uso di un dispositivo client remoto proprio, è altresì tenuto ad osservare le seguenti disposizioni per assicurare lo stesso livello di sicurezza dei dispositivi client aziendali:

- utilizzare sui dispositivi client solo sistemi operativi per i quali è garantito l'aggiornamento;
- effettuare costantemente gli aggiornamenti di sicurezza del sistema operativo del dispositivo client utilizzato;
- installare un adeguato sistema antivirus/antimalware da tenere costantemente aggiornato;
- collegarsi a dispositivi mobili (ad es.pen-drive) solo se si conosce la provenienza (ad es. nuovi, forniti dall'Amministrazione) ed, in ogni caso, effettuare una scansione preventiva di tutti i supporti rimovibili utilizzati;
- evitare di utilizzare il dispositivo adoperato per lo *smart-working* per l'uso di social network o altre applicazioni social facilmente hackerabili;
- verificare che gli accessi al sistema operativo siano protetti da password sicura, conforme alle disposizioni del presente Regolamento;
- non installare sul dispositivo utilizzato software proveniente da fonti/repository non ufficiali;
- utilizzare l'accesso a reti adeguatamente protette;
- non utilizzare pc pubblici o comunque di terzi
- né reti Wi-Fi pubbliche, le quali possono essere un veicolo che consente più facilmente di condurre attacchi ai dispositivi
- effettuare sempre il log-out dai servizi/portali utilizzati dopo che si è conclusa la sessione lavorativa;
- non cliccare su link o allegati contenuti in e-mail sospette;
- utilizzare strumenti di crittografia in caso di condivisione di dati particolari per posta elettronica.

Si precisa che le forme di accesso consentite tra il dispositivo dell'Utente ed il server aziendale sono solo le connessioni sicure (ad es. VPN –Virtual Private Network).
Esse comportano la registrazione degli accessi in file *Log (*ad es. nome utente, indirizzo IP di provenienza, orari in cui tali operazioni vengono effettuate) per finalità di tutela della sicurezza, riservatezza ed integrità dei dati aziendali trattati.

L'Amministratore di Sistema è tenuto al controllo della sicurezza delle postazioni esterne remote, negando o interrompendo l'accesso alla rete agli Utenti che utilizzino dispositivi non adeguatamente protetti e/o aggiornati che possano costituire una concreta minaccia per la sicurezza informatica dell'Azienda.

Il presente Regolamento Aziendale costituisce adeguata informazione sul trattamento dei dati personali, sulle modalità d'uso delle risorse informatiche e sull'effettuazione dei controlli ai sensi del Regolamento Europeo 2016/679 e dell'art.4 della Legge 20.5.1970, n. 300.

5. Gestione della rete informatica interna e della rete internet

Ciascun Utente abilitato alla rete interna aziendale ed alla navigazione in internet deve usare la rete in modo appropriato ed unicamente per esigenze aziendali, in quanto la stessa costituisce uno strumento di lavoro.
Per l'utilizzo della rete l'utente deve osservare i principi di prudenza nella trasmissione di dati personali, come prescritto dal Regolamento Europeo 2016/679, avendo cura di non tenere comportamenti che possono comportare rischi per l'integrità, la riservatezza e la disponibilità delle informazioni aziendali.
E' assolutamente vietato:

- accedere alla rete con un codice d'identificazione di un altro operatore;
- condividere cartelle in rete sprovviste di password, fatte salve situazioni particolari da autorizzare caso per caso;
- alterare la configurazione di rete di stazioni di lavoro e di altri dispositivi in rete (stampanti condivise, ecc...);
- aggiungere protocolli di rete o servizi in rete (per es. condivisione di stampanti in rete, *browsing* di risorse di rete, ecc.);
- scaricare, copiare, distribuire documenti, o altro, in violazione delle leggi sul diritto di autore;
- effettuare installazioni non autorizzate di modem per linee analogiche o digitali che sfruttino il sistema di comunicazione in fonia per l'accesso a banche dati esterne o interne all'Azienda;
- effettuare installazioni di hardware o software di qualsiasi tipo che consenta o faciliti il superamento delle misure di sicurezza adottate;
- nel caso in cui il software antimalware rilevi la presenza di un virus/malware, sospendere ogni elaborazione in corso e segnalare prontamente l'accaduto all'Amministratore di sistema ed al Referente Informatico

Al fine di evitare all'Utente la navigazione in siti non pertinenti l'attività lavorativa, si rende noto che è previsto l'uso di un sistema di blocco o filtro automatico che prevenga determinate operazioni, quali l'upload e l'accesso a determinati siti inseriti in una black list.

L'efficacia del sistema di filtraggio è controllata dall'Amministratore di sistema o dal Referente Informatico.

Dato che le apparecchiature, i servizi e le tecnologie utilizzati per accedere a internet sono beni aziendali, si rappresenta che potranno essere eseguiti eventuali controlli sul traffico internet, mediante *"file di log"* della navigazione svolta.

Tali log sono indispensabili all'Azienda per il perseguimento di finalità organizzative e di sicurezza e saranno trattati in maniera tale da fornire informazioni in maniera aggregata, precludendo l'immediata identificazione degli utenti, a meno che non vi siano specifiche ragioni per accedere alle informazioni di tipo nominativo.

Il presente Regolamento Aziendale costituisce adeguata informazione sul trattamento dei dati personali, sulle modalità d'uso delle risorse informatiche e sull'effettuazione dei controlli ai sensi del Regolamento Europeo 2016/679 e dell'art.4 della Legge 20.5.1970, n. 300.

6. Assegnazione degli account e gestione e controllo degli accessi logici

Obiettivo fondamentale della sicurezza delle informazioni è quello di limitare l'accesso dei dati alle effettive e legittime necessità operative dell'Utente.
Tutti i sistemi informatizzati di nuova acquisizione dovranno essere dotati della possibilità di definire profili di abilitazione mediante i quali dettagliare i privilegi dei diversi ruoli professionali in termini di funzionalità eseguibili e di dati accessibili nell'ambito dello specifico sistema, in linea con le prescrizioni dettate dal Regolamento Europeo 2016/679 e dal Garante per la protezione dei dati personali.
Ad ogni Utente è, pertanto, assegnata una identità digitale aziendale (c.d. "credenziali di accesso"), con l'attribuzione di permessi di accesso ai dati in base al ruolo ed il reparto/servizio di appartenenza ed alle attività eseguibili.
Tali credenziali, generate con modalità che assicurino la segretezza, sono composte da un identificativo univoco dell'utenza (user-id) e da una password (inizialmente impostata provvisoriamente e da cambiare obbligatoriamente al primo accesso ed al massimo ogni sei mesi, ovvero ogni tre mesi se i dati trattati sono particolari e/o giudiziari).
L'account Utente consente l'autenticazione dell'operatore nel sistema informatico e di conseguenza ne disciplina l'accesso alle risorse informatiche aziendali.
Gli Utenti, dunque, devono accedere alle risorse informatiche ed alla rete solo ed esclusivamente con le proprie credenziali di identificazione ed autenticazione, le quali sono strettamente personali e non cedibili. Le medesime, pertanto, devono rimanere strettamente riservate e vanno custodite con cura e diligenza.
A tal fine, gli Utenti sono tenuti a rispettare le seguenti prescrizioni:

- non condividere le proprie password con nessun altro Utente (colleghi, utenti Amministratori, assistenti tecnici), né rivelare la password al telefono, o inviarla via E-mail;
- evitare di trascrivere le proprie password su qualsiasi tipo di supporto, digitale o cartaceo;
- evitare la digitazione in presenza di terzi e la conservazione in luogo accessibile ad altri;
- cambiare la password obbligatoriamente al primo accesso ed ogni volta che viene richiesto dal sistema (al massimo 6 mesi o 3 mesi se i dati trattati sono particolari e/o giudiziari), ovvero in caso vi sia il dubbio che ne sia stata violata la segretezza;
- in tutti i casi di allontanamento, anche temporaneo, è necessario chiudere la propria sessione di lavoro; tale accorgimento deve essere adottato soprattutto in caso di utilizzazione, da parte di più soggetti, della medesima stazione di lavoro;
- adottare uno screensaver protetto da password;
- aver cura di evitare di cadere vittima di truffe online mirate al furto di credenziali di accesso o altri dati personali (Phishing);
- non tentare di acquisire i privilegi di Amministratore di sistema;
- in caso di smarrimento e/o furto della password o se si rilevino accessi non autorizzati a sistemi che trattano dati personali, occorre darne immediata notizia al Titolare, al Delegato del trattamento e al *Data Protection Officer* ed attivare la procedura *Data Breach* aziendale.

La definizione della propria password deve avere come obiettivo primario l'impossibilità da parte di terze parti di indovinarla o ricostruirla.
Pertanto, nella scelta della password l'Utente deve osservare le seguenti istruzioni:

- le password devono avere una lunghezza minima di 8 caratteri e devono essere formate dalla combinazione di caratteri alfabetici (almeno un carattere minuscolo ed uno minuscolo), numerici (almeno un carattere) e di simboli come ad es. @, $£! (almeno un carattere);

- non utilizzare più di due caratteri consecutivi identici (es: aaaaa…);
- non utilizzare sequenze di cifre consecutive (es: 12345…);
- non utilizzare elementi o notizie facilmente riconducibili all'utilizzatore: ad esempio, la password non deve essere legata al nome dell'Utente, oppure alla sua User-id, o in generale a parole allo stesso riconducibili (nome della moglie o dei figli, luogo e data di nascita, numero di matricola, nome di familiari, numero di telefono di casa o dell'ufficio, soprannomi noti, ecc.);
- non deve essere basata su parole di uso comune (nomi di luoghi, personaggi, mesi, giorni della settimana, ecc.);
- non deve essere uguale ad una delle ultime 5 già utilizzate;
- non utilizzare per il proprio account lavorativo una password già utilizzata per un account personale;
- modificare immediatamente la password ogniqualvolta vi sia il sospetto che possa essere stata compromessa

Il mancato rispetto delle istruzioni relative alla riservatezza delle credenziali di autenticazione danneggia l'intero sistema di gestione dei profili utente ed ha evidenti ricadute sul complessivo sistema di sicurezza.
In caso di interruzione a qualsiasi titolo del rapporto di lavoro con l'Azienda, è vietato all'Utente di utilizzare il proprio Account e sarà disposta la disabilitazione delle sue credenziali di autenticazione

Le credenziali di autenticazione sono, altresì, revocate quando non sussiste più la necessità di disporre delle risorse e/o delle informazioni aziendali concesse (ad es. in caso di modifica delle mansioni o spostamento in altro servizio/ufficio).

Il sistema informativo aziendale mantiene traccia di tutte le operazioni svolte dall'utente identificato con le sue credenziali di accesso, ivi compresi gli accessi da dispositivi remoti tramite ad es. VPN, registrando su di un apposito *file log* ogni azione svolta dallo stesso (accesso ai dati, modifica dei dati, uso di risorse informatiche aziendali locali o remote, ecc.).

I Log possono essere oggetto di controllo attraverso l'Amministratore di sistema, in quanto consentono di ricostruire l'attività di un sistema informatico e di individuare eventuali responsabilità in caso di errore o violazioni di legge.

Il presente Regolamento Aziendale costituisce adeguata informazione sul trattamento dei dati personali, sulle modalità d'uso delle risorse informatiche e sull'effettuazione dei controlli, ai sensi del Regolamento Europeo 2016/679 e dell'art.4 della Legge 20.5.1970, n. 300.

7 Gestione della Posta Elettronica

Il servizio di Posta elettronica è fornito dall'Azienda in funzione della comunicazione e delle altre attività strumentali correlate ai fini istituzionali.
Nell'ambito **dell'attività di proselitismo Sindacale**, è consentito l'utilizzo della mail aziendale **per comunicazioni sindacali** dei lavoratori in **regolare permesso o in pausa**, esclusivamente nella misura in cui questo non turbi il normale svolgimento dell'attività aziendale e non costituisca mezzo per la diffusione di messaggi aventi contenuti diffamatori o istigatori nei confronti dell'Azienda.
l servizio è subordinato all'osservanza integrale delle condizioni di seguito indicate.
L'utilizzo del servizio da parte dell'Utente costituisce implicita accettazione delle citate condizioni.
La casella di posta assegnata all'*Utente* è uno strumento di lavoro messo a disposizione per lo svolgimento della prestazione lavorativa.

In considerazione di ciò, è fatto divieto di utilizzare le caselle di posta elettronica aziendale per l'invio di catene telematiche e comunque di messaggi personali o per la partecipazione a dibattiti, forum o mail-list salvo diversa, preventiva ed esplicita autorizzazione della Direzione Aziendale.
E' fatto inoltre divieto di fornire a terzi, che non siano in rapporto di attività di lavoro, l'indirizzo e-mail dell'Azienda.
Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

7.1 Utenti del servizio di Posta elettronica, Account e Indirizzi

L'account di posta elettronica (username, password ed indirizzo di posta) è fornito, insieme ad un limitato spazio disco, alle seguenti categorie di Utenti:

1) Organi, Strutture ed articolazioni aziendali centrali e periferiche (PP.OO. DD.SS.SS.) Aree di gestione, Uffici di Staff; in questo caso il formato dell'indirizzo di posta sarà: **nomeservizio@asp.rg.it**

2) Personale dipendente in servizio attivo; in questo caso il formato dell'indirizzo di posta sarà: **nome.cognome@asp.rg.it, con eccezioni previste per i casi di omonimia**

L'attivazione dell'account avverrà, a cura dell'Amministratore del sistema, su richiesta scritta autorizzata dal Dirigente responsabile del Settore e/o Ufficio, dopo la verifica dei requisiti richiesti.
L'Utente si impegna ad adoperarsi attivamente per salvaguardare la riservatezza della sua password ed a segnalare qualunque situazione che possa inficiarla.
L'Utente sarà responsabile dell'attività espletata tramite il suo account.
La "personalizzazione" dell'indirizzo non comporta il suo carattere "privato", in quanto trattasi di strumenti di esclusiva proprietà aziendale messi a disposizione dell'Utente al solo fine dello svolgimento delle proprie mansioni lavorative.

7.2 Obblighi e diritti dell'Azienda

L'Azienda si impegna ad utilizzare i dati forniti dall'Utente ai fini dell'erogazione e gestione del servizio e di attuare quanto in suo potere per proteggere la privacy dell'Utente medesimo.
L'Azienda si impegna a fornire il servizio in modo continuativo, fatte salve eventuali sospensioni dovute all'ordinaria o straordinaria manutenzione, a malfunzionamenti e ad altre eventualità.
Inoltre, l'Azienda si impegna ad effettuare regolari backup generali sui server gestiti direttamente; non sono previsti backup e ripristini individuali.
Tutte le informazioni eventualmente raccolte saranno utilizzate a tutti i fini connessi al rapporto di lavoro, compresa la verifica del rispetto del presente Regolamento Aziendale, che costituisce adeguata informazione sul trattamento dei dati, sulle modalità d'uso degli strumenti e sull'effettuazione dei controlli ai sensi del Regolamento Europeo 2016/679 e dell'art.4 della Legge 20.5.1970, n. 300.

7.3 Limiti di responsabilità dell'Azienda

L'Azienda attuerà tutte le misure ritenute necessarie e sufficienti a minimizzare il rischio di perdita d'informazioni; ciò nonostante l'Utente solleva l'Azienda da ogni responsabilità ed obbligazione in relazione alla cancellazione, al danneggiamento, al mancato invio/ricezione o all'omessa conservazione di messaggi di posta (e-mail) imputabili ad un uso inappropriato del servizio, mentre

le responsabilità derivanti da guasti e/o malfunzionamenti degli apparati di gestione del software sono regolate dal contratto di affidamento Servizio come per Legge.

7.4 Riservatezza Posta Elettronica

L'Azienda persegue la riservatezza e l'integrità dei messaggi durante il loro transito e la loro permanenza nel sistema di posta.
Per il raggiungimento di tale obiettivo l'Amministratore di Sistema si avvarrà anche di strumenti idonei a verificare, mettere in quarantena o cancellare i messaggi che potrebbero compromettere il buon funzionamento del servizio.

7.5 Doveri, divieti, limiti di utilizzo, responsabilità dell'utente

L'Utente si impegna, nei confronti dell'Azienda, a presidiare quotidianamente la propria casella elettronica, con l'apertura e lettura dei messaggi di posta, corrispondendo alla richiesta di avviso di recapito e monitorando costantemente le sue dimensioni per non superare il limite di spazio previsto.
L'Utente si impegna a non utilizzare il servizio per scopi illegali o non conformi al presente regolamento o che comunque possano recar danno o pregiudizio all'Azienda medesima o a terzi.
L'Utente si assume ogni responsabilità penale e civile ed il carico di ogni eventuale onere derivante dall'uso improprio del servizio; esonera contestualmente l'Azienda da ogni pretesa o azione che dovesse essere rivolta all'Azienda medesima da qualunque soggetto, in conseguenza di tale uso improprio del servizio.
L'Utente, inoltre, non può utilizzare il servizio in modo da danneggiare, disattivare, sovraccaricare, pregiudicare o interferire con l'utilizzo da parte di altri utenti.
L'Utente, salvo giustificabili eccezioni, di cui comunque risponde personalmente, non può utilizzare la posta elettronica per inviare, anche tramite collegamenti o allegati in qualsiasi formato (testo, fotografico, video, grafico, audio, codice, ecc.), messaggi che contengano o rimandino a:

- pubblicità non istituzionale, manifesta o occulta;
- comunicazioni commerciali private;
- materiale pornografico o simile, in particolare in violazione della Legge n. 269 del 1998 "Norme contro lo sfruttamento sessuale dei minori degli anni 18";
- materiale discriminante o lesivo in relazione a razza, sesso, religione, ecc.;
- materiale che violi la normativa vigente sulla protezione dei dati personali;
- contenuti o materiali che violino i diritti di proprietà di terzi;
- altri contenuti illegali.

In nessun caso l'Utente potrà utilizzare la posta elettronica per diffondere codici dannosi per i computer quali virus e simili.
L'Utente non può tentare di accedere, in modo non autorizzato, ad altri account, a sistemi o ad altre reti tramite operazioni di pirateria informatica, contraffazione della password o altri mezzi illeciti o fraudolenti.
L'utente si impegna a fare attenzione alle mail ingannevoli, controllando i file allegati di posta elettronica prima del loro utilizzo; deve evitare di aprire gli allegati e di cliccare i link contenuti in messaggi di mittenti sconosciuti, notificando l'accaduto all'Amministratore di sistema o al Referente informatico e cancellando tali mail.
Per l'invio a destinatari esterni di messaggi contenenti allegati relativi a dati personali particolari o giudiziari, l'Utente è tenuto a renderli preventivamente illeggibili, criptandoli con apposito software e comunicando al destinatario la password di cifratura attraverso un canale diverso dalla mail (ad esempio per lettera o per telefono).

L'Utente, infine, si impegna a non divulgare messaggi di natura ripetitiva (catene di varia denominazione) anche quando il contenuto sia volto a segnalare presunti o veri allarmi (esempio: segnalazioni di virus).

Di fronte a quest'ultima evenienza l'Utente dovrà limitarsi ad inoltrare un messaggio al Servizio Informatico.
L'Utente accetta di essere riconosciuto quale autore dei messaggi inviati dal suo account e assume l'onere di comunicare, tempestivamente, all'Amministratore di sistema, la ricezione di posta "indesiderata" per le opportune protezioni.
L'Azienda si riserva la facoltà di segnalare alle Autorità competenti, per gli accertamenti ed i provvedimenti del caso, le eventuali violazioni alle presenti condizioni di utilizzo.

7.6 Revoca del servizio

L'Utente riconosce e concorda che l'Azienda può revocargli l'account, ovvero sospenderne temporaneamente l'utilizzo, in caso di violazione del presente regolamento.
Inoltre, l'Azienda si riserva il diritto di interrompere o sospendere, in tutto o in parte, l'erogazione del Servizio per motivi tecnici o amministrativi.
In caso di interruzione del rapporto di lavoro a qualsiasi titolo, l'indirizzo di posta elettronica dell'Utente sarà disabilitato.

8.Gestione degli applicativi aziendali

Gli applicativi aziendali sono l'insieme dei programmi (software) che consentono l'inserimento, l'archiviazione, l'elaborazione e la consultazione dei dati aziendali, sfruttando i dispositivi hardware e le connessioni di rete dell'Azienda.
Essi devono rispondere ai requisiti di confidenzialità, integrità, continuità del dato e riconducibilità al singolo Utente, come prescritto dal Regolamento Europeo 2016/679 per il trattamento dei dati personali.
Gli Utenti e gli Amministratori di sistema devono possedere le sole autorizzazioni strettamente necessarie ad effettuare il loro compito. In ogni caso, ciascuno deve astenersi da effettuare operazioni che, ancorché tecnicamente consentite dai sistemi, non rientrano nella propria mansione specifica.
Pertanto, gli applicativi software devono prevedere profili di autorizzazione di ambito diverso per diversi incaricati, in modo da consentire che solo alcuni di essi possano effettuare alcuni trattamenti o accedere a certi tipi di dato.
L'abilitazione dell'Utente agli applicativi aziendali avviene su esplicita richiesta avanzata dal Responsabile della Struttura all'Amministratore di sistema o al Referente informatico.
Periodicamente, con cadenza almeno annuale, sono aggiornati gli ambiti del trattamento consentito agli addetti, a cura dell'Amministratore di sistema con il supporto dei responsabili delle UU.OO.CC..

Per un corretto utilizzo degli applicativi aziendali l'Utente deve:

- garantire la correttezza del dato, prevenendo il rischio di trattamenti impropri (inserimento di dati non corretti, mancato inserimento di dati, accesso a dati non pertinenti, ecc.);
- non utilizzare account assegnati ad altri Utenti;
- non comunicare ad altri le proprie credenziali personali di autenticazione, anche se solo temporaneamente;
- effettuare la pronta segnalazione di qualsiasi malfunzionamento.

9. Assistenza tecnica

Le attività di manutenzione, gestione ed implementazione sono eseguite da personale interno nominato dal Titolare quale autorizzato al trattamento ai sensi dell'art. 29 GDPR, a cui sono impartite apposite istruzioni, ovvero da personale afferente all'organizzazione di soggetti esterni previamente nominati dal Titolare quali responsabili del trattamento ai sensi dell'art. 28 GDPR.
Tali soggetti esterni, a cui sono impartiti specifici obblighi di riservatezza, devono essere in grado di fornire garanzie adeguate al fine di assicurare il pieno rispetto delle disposizioni in materia di trattamento dei dati personali, nonché di garantire la tutela dei diritti dell'interessato.
A seguito di chiamata dell'Utente o in caso di necessità per la rilevazione tecnica di problemi nel sistema informatico, l'Amministratore di sistema ed il suddetto personale incaricato del servizio sono autorizzati a compiere interventi nel sistema informatico aziendale per risolvere problemi tecnici e/o manutentivi, nonché per garantire la sicurezza e la salvaguardia del sistema.

Per le suddette finalità, gli interventi tecnici potranno anche comportare l'accesso ai dati trattati da ciascun Utente, ivi compreso l'accesso agli archivi di posta elettronica e la verifica dei siti internet a cui hanno avuto accesso gli Utenti abilitati alla navigazione esterna.
Il suddetto personale potrà collegarsi e visualizzare in remoto il desktop delle singole postazioni, dandone preventiva comunicazione all'interessato, qualora non si pregiudichi la necessaria tempestività e l'efficacia dell'intervento tecnico.

10. Accesso ai dati trattati dall'utente

L'Azienda, nel rispetto della normativa vigente sulla protezione dei dati, si riserva il diritto di accedere alla risorsa informatica in dotazione dell'Utente ed ai documenti in essa contenuti, per esigenze organizzative e produttive (attività di gestione, controllo, aggiornamenti ai fini della sicurezza del sistema e della rete), per la sicurezza del lavoro e per la tutela del patrimonio, nella considerazione che ogni dato trattato per mezzo degli strumenti e delle risorse informatiche appartenenti all'Azienda sarà considerato di natura aziendale e non riservata.
I **log relativi all'utilizzo degli strumenti**, reperibili nella memoria degli strumenti, ovvero sui server o sui router, ivi compresi i *file log* riferiti al traffico web ed alla connessione VPN, **sono registrati e possono essere oggetto di controllo** attraverso l'Amministratore di sistema.
Le informazioni raccolte sono, inoltre, utilizzabili a tutti i fini connessi al rapporto di lavoro, compresa la verifica del rispetto del presente Regolamento.
Il presente Regolamento Aziendale costituisce adeguata informazione in ordine al trattamento dei dati personali, alla modalità d'uso degli strumenti e di effettuazione dei controlli, ai sensi del Regolamento Europeo 2016/679 e dell'art.4 della Legge 20.5.1970, n. 300 e succ. mm. e ii..

11. Controlli

L'articolo 23 del recente D.lgs. 14 settembre 2015 n. 151 ("Jobs Act") ha modificato il contenuto dell'articolo 4 della Legge 300/1970, ora rubricato "Impianti audiovisivi e altri strumenti di controllo".
Alla luce delle suddette disposizioni, l'Azienda può effettuare controlli sugli strumenti informatici utilizzati dal lavoratore per rendere la prestazione lavorativa (personal computer, tablet, telefoni e smartphone), senza la necessità di accordi sindacali preventivi, fornendo al lavoratore un'adeguata informativa sulle regole previste per l'utilizzo lavorativo ed eventualmente personale degli strumenti di cui si tratta e sulle modalità e i casi in cui potranno essere effettuati i controlli.

Per quanto innanzi l'Azienda, in qualità di datore di lavoro, si riserva la facoltà di effettuare controlli, anche saltuari o occasionali, sui dispositivi utilizzati dall'Utente per rendere la prestazione lavorativa (computer, tablet, ecc.).
Gli eventuali controlli saranno eseguiti in conformità della normativa vigente, con particolare riferimento al Regolamento Europeo 2016/679, al D.Lgs. 196/2003 come modificato dal D.Lgs. 101/2018, all'articolo 4 comma 2 della Legge 300/1970, come modificato dal D.Lgs 14/09/2015 n°151 ed ai provvedimenti emanati dal Garante.

A tale scopo, con il presente Regolamento aziendale, all'Utente è fornita *adeguata informazione in ordine alla modalità d'uso degli strumenti e di effettuazione dei controlli, nonché informativa sul trattamento dei dati personali ai sensi dell'art. 13 del Regolamento UE 2016/679 (vedi successivo art. 13).*

I controlli sull'uso degli strumenti elettronici saranno tali da evitare un'interferenza ingiustificata sui diritti e sulle libertà fondamentali dei lavoratori e di soggetti esterni che ricevono o inviano comunicazioni elettroniche di natura personale o privata.
Gli eventuali controlli saranno commisurati allo scopo e saranno effettuati nel rispetto dei principi di necessità, pertinenza e non eccedenza, proporzionalità e gradualità.
Nel caso in cui un evento dannoso o una situazione di pericolo non sia stato impedito con preventivi accorgimenti tecnici, l'Azienda può adottare eventuali misure che consentano la verifica di comportamenti anomali.
In tal caso, il personale incaricato effettuerà per quanto possibile un controllo preliminare su dati aggregati, riferiti all'intera struttura lavorativa o a sue aree.
Il controllo anonimo può concludersi 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 anche a dipendenti afferenti all'area o settore in cui è stata rilevata l'anomalia.
Sono, comunque, esclusi controlli prolungati, costanti o indiscriminati.
In caso di reiterate anomalie o irregolarità, ovvero di segnalazioni di attività non conformi alla normativa vigente ed al presente Regolamento, saranno effettuati controlli su base individuale, su singoli nominativi, basi e postazioni.
L'Azienda si riserva, comunque, le facoltà previste dalla normativa vigente di effettuare specifici controlli *ad hoc* nel caso di segnalazione di attività che hanno causato danno all'amministrazione, che ledono diritti di terzi o che, comunque, sono illegittime.

12. Informativa agli utenti resa ai sensi dell'art. 13 del regolamento UE n. 679/2016

Ai sensi dell' art. 13 del Regolamento UE 2016/679 ed in adempimento delle Linee Guida del Garante Privacy del 1 marzo 2007, l'Azienda Sanitaria Provinciale di Ragusa, **Titolare del trattamento** dei Dati Personali (d'ora in poi, per brevità, il "**Titolare**"), informagli gli Utenti, quale assegnatari di strumentazione informatica ed eventualmente abilitati ad internet e posta elettronica, connessione VPN(dipendenti, collaboratori, ecc.), che i dati personali raccolti per le finalità indicate nel presente Regolamento aziendale formeranno oggetto di trattamento nel rispetto della normativa vigente in materia di protezione dei dati personali.
In particolare, il trattamento dei dati sarà improntato al rispetto dei principi di liceità, correttezza, trasparenza, limitazione delle finalità e della conservazione, minimizzazione dei dati (i dati raccolti saranno adeguati, pertinenti e limitati a quanto strettamente necessario rispetto alle finalità per le quali sono trattati), esattezza, integrità e riservatezza.

I dati personali degli Utenti (ad es. nome utente, indirizzo IP, registrazione degli accessi in *file log* che comprendono gli orari in cui le operazioni vengono effettuate dall'Utente ed altre informazioni relative agli accessi alle risorse informatiche), saranno trattati esclusivamente per le seguenti **finalità**:

- esigenze organizzative e produttive, sicurezza del lavoro e tutela del patrimonio aziendale (ad es. sicurezza del sistema informativo, assistenza tecnica e sistemistica, controllo e programmazione dei costi aziendali, ecc.);
- effettuazione di controlli per verificare il rispetto delle regole dettate con il presente Regolamento interno;
- finalità difensive.

Quanto alla **base giuridica**, il trattamento dei dati personali è necessario per:

- l'esecuzione del contratto di cui l'interessato è parte;
- l'esecuzione di un compito di interesse pubblico;
- l'adempimento degli obblighi e l'esercizio dei diritti specifici del Titolare del trattamento o dell'interessato in materia di diritto del lavoro, in conformità alle norme vigenti in materia

Il conferimento dei dati personali è obbligatorio perle suddette finalità; in mancanza all'Utente non potrà essere consentito l'uso della strumentazione informatica di lavoro.
I dati saranno trattati sia in forma cartacea, che in formato digitale e con l'adozione di misure tecniche ed organizzative per assicurare adeguati livelli di sicurezza.
I dati saranno trattati da personale dipendente o da altri soggetti che collaborano con l'Azienda, tutti debitamente a ciò autorizzati dal Titolare o da un suo delegato, nonché da soggetti appositamente designati dal Titolare quali Responsabili del trattamento dei dati personali.
I dati personali non verranno in alcun modo diffusi e potranno essere comunicati all'Autorità Giudiziaria e/o all'Autorità di Pubblica Sicurezza ed ad altri Soggetti, nei casi previsti dalla legge.
I dati personali forniti e/o acquisiti dall'Azienda Sanitaria Provinciale di Ragusa verranno conservati nel rispetto dei termini previsti dalle disposizioni di legge e dalle vigenti procedure di scarto

Nella qualità di interessati al trattamento, gli Utenti hanno diritto di

- ottenere l'accesso ai propri dati personali ed alle informazioni relative agli stessi;
- ottenere l'aggiornamento, la rettifica dei dati inesatti o l'integrazione di quelli incompleti;
- ottenere la cancellazione, nei casi previsti;
- ottenere la limitazione del trattamento dei dati personali che li riguardano, nei casi previsti;
- opporsi al loro trattamento, in tutto o in parte, per motivi legittimi;
- ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che li riguardano forniti al Titolare del trattamento ed hanno diritto di trasmettere tali dati ad un altro Titolare del trattamento (se tecnicamente fattibile);
- proporre reclamo all'Autorità Garante per la Protezione dei dati personali, qualora ne ricorrano i presupposti, seguendo le procedure e le indicazioni pubblicate sul sito web dell'Autorità Garante www.garanteprivacy.it.

Per l'esercizio dei suddetti diritti, i soggetti interessati potranno presentare istanza in forma scritta a:

Titolare del trattamento:
Azienda Sanitaria Provinciale di Ragusa, in persona del Direttore Generale *pro-tempore*
Sede legale: Piazza Igea n.°1 97100 Ragusa
Email: direzione.generale@pec.asp.rg.it
Data Protection Officer (D.P.O.)
Dr.ssa Giovanna Di Stefano presso Presidio Ospedaliero "Civile"
Email: dpo@asp.rg.it

13. Gestione della sicurezza dei sistemi informativi

13.1. Backup

Le copie di backup delle informazioni, del software e delle immagini dei sistemi residenti sui server aziendali devono essere effettuati dall'Amministratore di sistema e/o dal personale incaricato all'uopo, con frequenza giornaliera.
A cura dell'Amministratore di sistema è predisposto un piano di verifica periodica del corretto funzionamento delle copie di Backup (le copie sono sottoposte a test periodici di *restore).*
Per assicurare il ripristino dei dati, le copie di backup della sala server devono essere replicate in un *datacenter* secondario (*disaster recovery*).

13.2. Protezione dal *malware*

Le informazioni e le infrastrutture IT di proprietà dell'Azienda devono essere protette dal *malware*.
In particolare, i programmi antivirus/antimalware devono essere installati su tutti gli apparati, sia server che postazioni di lavoro e devono essere aggiornati almeno semestralmente.
Per prevenire le vulnerabilità derivanti, l'Utente deve osservare comportamenti idonei a ridurre il rischio di attacco al sistema informatico aziendale.
In particolare, ogni Utente è obbligato a controllare la presenza e il regolare funzionamento del programma antivirus/antimalware aziendale e consentire i periodici aggiornamenti dello stesso.
Qualora il programma antivirus/antimalware rilevi la presenza di un malware, l'Utente dovrà sospendere ogni elaborazione in corso senza spegnere il computer e segnalare l'accaduto all'Amministratore di Sistema.
L'Utente è tenuto, altresì, a verificare mediante il programma antivirus/antimalware ogni dispositivo magnetico di provenienza esterna all'Azienda prima del suo utilizzo.

13.3. Sospensione automatica delle sessioni di lavoro.

La sospensione automatica della sessione di lavoro dopo un tempo minimo di inattività deve essere attivata su ogni postazione di lavoro (il sistema deve avviare un "screensaver" automatico protetto da password che oscuri la videata).
Il tempo minimo di inattività è stabilito da ciascuna Struttura Organizzativa in base alle proprie esigenze di servizio.

13.4. Procedure per il ripristino dei dati

A cura dell'Amministratore di sistema sono adottate idonee misure per garantire il ripristino dell'accesso ai dati, in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a 7 giorni.

13.5. Cifratura dei dati

I dati particolari salvati su sistemi di archiviazione digitale devono essere cifrati attraverso idonei sistemi di protezione.
Parimenti, quando vengono trasmessi da un sistema digitale ad un altro, i dati prima della trasmissione devono essere cifrati con adeguati sistemi di cifratura.

13.6. Amministratore di sistema

L'Amministratore di sistema è responsabile della sicurezza del sistema informatico dell'Azienda, in rapporto al proprio ambito di operatività e competenza.
Allo stesso spetta il compito di individuare, proporre e mettere in atto misure tecniche per garantire un livello di sicurezza adeguato al rischio (art. 32 del Regolamento).
Con riferimento alla policy di sicurezza relativa agli Amministratori di sistema si rinvia al **Regolamento aziendale sulla protezione dei dati personali per gli Amministratori di sistema**, nonché **Regolamento concernente la nomina e le funzioni dell'Amministratore di Sistema e gli adempimenti in materia di osservanza delle misure di sicurezza privacy**

13.7. Sanificazione digitale

Per il **reimpiego** e **smaltimento di rifiuti di apparecchiature elettroniche** occorre osservare un'adeguata politica di cancellazione per prevenire accessi non consentiti ai dati personali in esse contenuti.
Pertanto, per ottemperare agli obblighi imposti dal Regolamento UE 2016/679 e dal Garante per la protezione dei dati con provvedimento del 13 ottobre2008, in caso di dismissione o cessione di apparecchiature IT, occorre cancellare in modo sicuro, definitivo e permanente tutte le informazioni in essi presenti, utilizzando misure tecniche che consentano di garantire la loro non intelligibilità o l'effettiva cancellazione dei dati, come meglio descritte negli allegati A e B del suddetto provvedimento del Garante per la protezione dei dati.

Per quanto riguarda i supporti rimovibili contenenti dati particolari o dati giudiziari, gli stessi, se non utilizzati, devono essere distrutti o resi inutilizzabili; pertanto possono essere riutilizzati da altri soggetti solo se le informazioni precedentemente in essi contenute non sono più intelligibili, né in alcun modo tecnicamente ricostruibili.

E' compito dell'Amministratore di sistema e del personale eventualmente incaricato del servizio (anche esterno) di curare la suddetta attività di sanificazione digitale, su richiesta dei Direttori di Struttura

14. Sicurezza dei documenti e degli archivi cartacei

Il trattamento di archivi cartacei aziendali ed in particolar modo di quelli relativi a dati appartenenti a categorie particolari o ai dati giudiziari deve essere orientato ai principi di riservatezza, integrità e disponibilità analogamente a quanto previsto per il trattamento con strumenti informatici.
Le misure di sicurezza si devono applicare sia ai documenti originali che alle loro copie.
L'accesso agli archivi cartacei è permesso al solo personale autorizzato.
La protezione degli archivi cartacei è affidata a idonee misure di sicurezza fisica quali:

- controllo degli accessi ai locali;
- tracciamento degli accessi per gli archivi particolarmente riservati.

L'Utente, nel trattamento dei documenti cartacei, è tenuto ad osservare le seguenti prescrizioni:
a) i documenti contenenti dati personali devono essere conservati per la durata del trattamento e successivamente riposti in archivi ad accesso controllato e all'interno di archivi/cassetti/armadi muniti di serratura e chiusi a chiave; è infatti necessario identificare un luogo sicuro di custodia che dia sufficienti garanzie di protezione;

b) i suddetti documenti non devono essere lasciati incustoditi sulla scrivania e/o in luoghi aperti al pubblico in assenza di altri incaricati addetti al medesimo trattamento;
c) devono essere sempre controllati in modo che siano sempre completi ed integri;
d) non devono esser consultati da altri incaricati non autorizzati al trattamento;
e) non possono esser riprodotti o fotocopiati se non per esigenze connesse alla finalità del trattamento;
f) qualora sia necessario distruggere i documenti contenenti dati personali, devono essere utilizzati gli appositi apparecchi "distruggi documenti"; in assenza di tali strumenti, i documenti devono essere sminuzzati in modo da non essere più ricomponibili;
g) devono essere adottate idonee misure organizzative per salvaguardare la riservatezza dei dati personali (es. trasmissione dei documenti in buste chiuse);
h) in tutte le ipotesi in cui venga utilizzata una stampante condivisa da vari utenti situata al di fuori dei locali ove è posta la singola stazione di lavoro, le stampe devono essere raccolte immediatamente e custodite con le modalità descritte nei punti precedenti, qualora non sia possibile utilizzare un apposito codice personale di sblocco.

15. Comunicazione di dati personali

L'Utente può effettuare la comunicazione di dati personali a terzi, pubblici e privati, solo qualora sia espressamente consentito da una specifica disposizione di legge o di regolamento.
Anche in tal caso, deve fare particolare attenzione ad evitare il trattamento dei dati personali qualora le finalità da perseguire possano essere realizzate mediante l'utilizzo di dati anonimi o con opportune tecniche di crittografia.

16.Gestione del *Data Breach*

Il Data Breach è "*la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati*" dal Titolare del trattamento.
Poiché a norma dell'art. 33 del Regolamento Europeo 2016/679 ogni violazione di sicurezza che comporti un rischio per i diritti e le libertà delle persone fisiche deve essere notificata all'Autorità Garante, senza ingiustificato ritardo e, ove possibile, entro **72 ore**, dal momento in cui il Titolare è venuto a conoscenza della violazione, ogni Utente è obbligato a segnalare immediatamente ogni incidente (ad es. malfunzionamento PC, furto, ecc.) seguendo le istruzioni contenute nella **Procedura aziendale di gestione della violazione di dati (*Data Breach*),** pubblicata sul sito internet aziendale nel Link "Protezione dei dati personali", al quale si fa rinvio.

17. Sanzioni

La violazione delle disposizioni del presente Regolamento espone ogni *Utente* a responsabilità di carattere penale e civile, con conseguente risarcimento di eventuali danni causati all'Azienda e a terzi.
Nel caso in cui l'Utente sia dipendente della Azienda, saranno irrogate nei suoi confronti le sanzioni disciplinari previste dal CCNL di categoria e dal Codice Disciplinare Aziendale, all'esito del procedimento disciplinare attivato.
L'Utente si impegna a tenere indenne l'Azienda da qualsiasi danno, perdita, responsabilità, nonché dagli oneri di spesa che dovessero derivare da atti, fatti, comportamenti non corretti o illeciti o omissioni allo stesso imputabili, in quanto è personalmente responsabile dell'utilizzo delle risorse informative affidatigli, dei dati trattati per finalità aziendali, nonché dell'adozione di tutte le misure di sicurezza necessarie a prevenire eventuali violazioni di dati.

18. Norme finali

Le disposizioni del presente Regolamento si applicano, per quanto compatibili, anche alle ipotesi di collegamento alla rete aziendale da postazioni esterne all'Azienda.
Si applicano, altresì, per quanto compatibili, alla modalità di lavoro agile (smart-working), anche nel caso sia consentito l'utilizzo di strumenti propri dell'Utente. A questo proposito si rinvia all'Informativa specifica e connesse istruzioni operative pubblicate sul sito internet aziendale nel Link "Protezione dei dati personali".

19. Diffusione del regolamento

Il presente Regolamento dovrà essere divulgato in modo capillare.
A tal fine, dovrà essere trasmesso tramite e-mail a tutti i dipendenti e collaboratori da parte dei relativi Delegati al trattamento. Stante il forte impatto in termini di visibilità del processo di *accountability* aziendale del presente regolamento il Servizio Informatico ne curerà la pubblicazione all'interno della rete Intranet aziendale

20. Rinvio

Per quanto non previsto dal presente Regolamento, si fa riferimento alle vigenti disposizioni legislative e regolamentari in materia di protezione dei dati personali ed alle disposizioni civili e penali vigenti in materia.