AZIENDA OSPEDALIERA DEI COLLI

(Monaldi - Cotugno - C.T.O.) di NAPOLI

REGOLAMENTO AZIENDALE

SULL'UTILIZZO DEI

SISTEMI INFORMATICI

(*POSTA ELETTRONICA, RETE INTRANET / INTERNET, POSTAZIONI DI LAVORO*)

(approvato con deliberazione del Direttore Generale n. **1015** del **22/12/2020**)

In vigore dal _____

Sommario

Art. 1 - Premessa

La progressiva diffusione delle nuove tecnologie informatiche e, in particolare, il libero accesso alla rete Internet dai Personal Computer, espone l'Azienda e gli utenti (dipendenti e collaboratori della stessa) a rischi di natura patrimoniale, oltre alle responsabilità penali conseguenti alla violazione di specifiche disposizioni di legge (legge sul diritto d'autore e legge sulla privacy, fra tutte), creando evidenti problemi alla sicurezza ed all'immagine dell'Azienda stessa.

Premesso quindi che l'utilizzo delle risorse informatiche e telematiche deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito dei rapporti di lavoro, l'Azienda Ospedaliera dei Colli ha adottato un Regolamento interno diretto ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla sicurezza nel trattamento dei dati. Il medesimo ha valenza di codice comportamentale specifico per i dipendenti aziendali e contribuisce a promuovere l'investimento dinamico dell'Azienda nella sicurezza informatica e nella protezione dei dati personali in ossequio al Regolamento (UE) 2016/679 del parlamento europeo e del Consiglio del 27 aprile 2016 (GDPR General Data Protection Regulation). Porre vincoli e limiti all'utilizzo delle risorse costituisce modalità atta a garantire la correttezza e sicurezza nella pratica, anche in relazione a quanto stabilito dal "Regolamento recante il codice di comportamento dei dipendenti pubblici, a norma dell'art. 54 del D.Lgs. 30 marzo 2001, n. 165" di cui al D.P.R. 16 aprile 2013, n. 62, che all'art. 11, comma 3, stabilisce "*Il dipendente utilizza il materiale o le attrezzature di cui dispone per ragioni d'ufficio e i servizi telematici nel rispetto dei vincoli posti dall'amministrazione.* ".

L'art. 10 del Codice di Comportamento aziendale (Deliberazione n. 339 del 27 aprile 2020) che prevede espressamente che il dipendente "utilizza il materiale e le attrezzature di cui dispone per ragioni d'ufficio e i servizi telematici e telefonici dell'ufficio nel rispetto dei vincoli posti dall'amministrazione, salvo casi di urgenza".

Art. 2 - Ambito di applicazione

Il disciplinare si applica a tutti i dipendenti e a tutti i collaboratori dell'azienda, quale sia il rapporto contrattuale in essere (consulenti, lavoratori somministrati, collaboratori a progetto, in stage, volontari, tirocinanti, ditte esterne autorizzate, convenzionati, ecc..).

Ciascun utilizzatore, in base al proprio profilo "base" o "evoluto", dovrà attuare le norme che sono allo stesso indirizzate e, nel caso di dubbi di applicazione delle stesse, rivolgersi all'U.O.C. Servizio Informativo Aziendale (d'ora innanzi indicato per brevità UOC SIA).

Art. 3 - Scenario normativo

Le realtà aziendali sono andate caratterizzandosi in questi ultimi anni per l'elevato uso delle tecnologie informatiche e telefoniche, che se da un lato hanno consentito l'introduzione di innovative tecniche di gestione, dall'altro hanno anche dato origine a numerose problematiche relative all'utilizzo degli strumenti informatici forniti dall'Azienda ai propri collaboratori per lo svolgimento delle mansioni e compiti affidati.

In questo senso, viene fortemente sentita la necessità di porre in essere adeguati sistemi di controllo sull'utilizzo di tali strumenti da parte dei dipendenti/collaboratori nel rispetto dei criteri e dei principi stabiliti dal Garante per la protezione dei dati personali (provvedimento n. 13 del 01/03/2007) e di valutare conseguentemente gli usi scorretti che, oltre ad esporre l'Azienda stessa a rischi, tanto patrimoniali quanto penali, possono di per sé considerarsi contrari ai doveri di diligenza e fedeltà previsti dagli artt. 2104 e 2105 del Codice Civile.

I controlli sull'uso degli strumenti informatici/telefonici tuttavia, devono garantire tanto il diritto dell'Ente di proteggere la propria organizzazione, essendo i computer aziendali strumenti di lavoro la cui utilizzazione personale è preclusa, quanto il diritto del lavoratore a non vedere invasa la propria sfera personale, e quindi il diritto alla riservatezza ed alla dignità come sanciti dallo Statuto dei lavoratori (legge n. 300/1970) e dal Codice sul trattamento dei dati personali (D.Lgs. n. 196/2003, come integrato dalle disposizione del Regolamento UE/679/2016 GDPR e dal D.Lgs 101/2018).

Il regolamento ha lo scopo di informare gli interessati sulle finalità dell'utilizzo degli strumenti informatici, del controllo e sulle specifiche metodologie adottate per effettuarlo.

Il regolamento, inoltre, oltre a dettare una disciplina per l'utilizzo degli strumenti informatici aziendali, vuole costituire un utile strumento per sensibilizzare il personale su altri aspetti altrettanto importanti nella gestione dei sistemi informatici aziendali, quali il rispetto della normativa sulla tutela legale del software (e quindi il controllo sulla regolarità del software presente nello stesso sistema informatico), e quella sulla tutela dell'attività aziendale, quando queste importanti informazioni di proprietà dell'Azienda sono custodite nel sistema informatico.

Il presente Regolamento disciplina le modalità di accesso e fornitura dei servizi informatici e di rete dell'Azienda, sia all'interno sia all'esterno delle sedi di lavoro.

L'utilizzo delle risorse e dei servizi informatici e di rete è subordinato al rispetto da parte degli utenti del presente Regolamento, oltre che delle norme civili, penali e amministrative applicabili.

A tale proposito occorre sottolineare che la violazione degli stessi, laddove operata con intenti fraudolenti, si configura come "Crimine Informatico" e pertanto, il presente documento fa riferimento anche alla vigente normativa in materia qui riportata:

- Legge 22 aprile 1941 n. 633 e successive integrazioni sulla tutela della proprietà intellettuale: In particolare devono essere rispettate le politiche indicate dall'aziende atte a tutelare il diritto d'autore sull'utilizzo del software e dei prodotti informatici. La violazione della tutela del diritto d'autore costituisce, infatti, un illecito penale;
- Art. 615 ter c.p: Accesso abusivo ad un sistema informatico o telematico;
- Art. 615 quater c.p: Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici;
- Art. 615 quinquies c.p.: Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico;
- Art. 616 e 617 sexies c.p.: Violazione di corrispondenza telematica;
- Art. 617 quater c.p: Intercettazione di e-mail;
- Art. 621 c.p: Rivelazione del contenuto di documenti segreti;
- Art. 635 bis c.p: Danneggiamento di sistemi informatici e telematici;
- Art. 640 ter c.p: Alterazione dell'integrità dei dati allo scopo di procurarsi un ingiusto profitto (Frode informatica);
- Art. 491 bis c.p: Falsificazione di documenti informatici;
- Articolo 392 codice penale: Esercizio arbitrario delle proprie ragioni con violenza;
- Legge n. 547 del 23 dicembre 1993: Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica.

Il Regolamento si applica a tutte le tipologie di servizi e dati, nelle modalità operative descritte nelle sezioni di seguito indicate.

Art. 4 - Definizioni

Per gli scopi del presente regolamento si definiscono:

- *Account istituzionale:* account fornito dall'Azienda a ciascun Utente per accedere ai servizi informatici e di rete in accordo con il relativo Profilo Utente;

- *A.O.*: Azienda Ospedaliera;
- *BIOS:* Basic Input-Output System;
- *ERP:* Enterprise Resource Planning. È un software di gestione che integra tutti i processi di business rilevanti di un'azienda (vendite, acquisti, gestione magazzino, contabilità ecc.);
- *Internet:* rete di accesso pubblico alla quale la Rete Interna accede e si presenta con i propri servizi;
- *LOG:* registrazione sequenziale e cronologica delle operazioni effettuate, da un utente, un amministratore o automatizzate, man mano che vengono eseguite dal sistema o applicazione;
- *NAS:* Network Attached Storage;
- *PdL*: Postazione di Lavoro che si basa su strumenti informatici (PC, *smartphone*, ecc.) tramite i quali l'Utente accede ai servizi informatici e di rete dell'Azienda, sia dalla Rete Interna sia da Internet;
- *Profilo utente:* tipologia di Utente con accesso ad un numero predefinito di servizi informatici e di rete;
- *Struttura:* Unità Operativa (Semplice o Complessa) dell'Azienda;
- *UOC:* Unità Operativa Complessa;
- *UOSD:* Unità Operativa Semplice Dipartimentale;
- *UOS:* Unità Operativa Semplice;
- *Responsabile di Struttura:* Direttore Dipartimento o UOC, responsabile di UOSD o UOS;
- *Rete Interna:* insieme delle risorse di rete che consentono il collegamento informatico e telematico tra le diverse sedi dell'Azienda;
- *SIA.:* Servizio Informativo Aziendale;
- *Sistema:* dispositivo in grado di erogare servizi informatici o di rete (*server*, *router, ecc.*);
- *System Administrator:* è un (professionista) tecnico specializzato che si occupa della gestione aggiornamento e monitoraggio di un sistema informatico;
- *Utente:* soggetto con diritto di accesso ai servizi informatici e di rete, in accordo con il proprio profilo di appartenenza e il presente Regolamento;
- *VPN*: Virtual Private Network. Una VPN è una rete privata virtuale instaurata tra soggetti che utilizzano un sistema di trasmissione pubblico e condiviso come Internet;
- *PC*: Personal Computer;
- *PEC*: Posta Elettronica Certificata. È definita in tal modo la corrispondenza inviata via web tramite un gestore del servizio che rilascia al mittente una ricevuta quale prova legale dell'avvenuta spedizione del messaggio e degli eventuali allegati.

Art. 5 - Entrata in vigore del Regolamento e pubblicità

Con l'entrata in vigore del presente regolamento tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi abrogate e sostituite dalle presenti. Copia del regolamento, sarà disponibile sulla intranet aziendale e nella sezione Amministrazione Trasparente.

Il nuovo regolamento si applica a tutti i dipendenti, senza distinzione di ruolo e/o livello, nonché a tutti i collaboratori dell'Azienda, a prescindere dal rapporto contrattuale con la stessa intrattenuto (lavoratori somministrati, collaboratore a progetto, in stage, ecc.).

Art. 6 - System Administrator

È un (professionista) tecnico specializzato che si occupa dell'installazione, configurazione, gestione/manutenzione, aggiornamento e monitoraggio di un sistema operativo e più in generale di uno o più sottosistemi di un sistema informatico.

Il ruolo del sistemista, in osservanza al disciplinare tecnico allegato al previgente Codice della privacy (D.Lgs. 30 giugno 2003, n. 196) e sue successive modifiche ed aggiornamenti, nonché al provvedimento a carattere generale del 27 novembre 2008 emanato dall'Autorità Garante Italiana, è quello di gestire, a livello infrastrutturale, il buon governo dell'hardware e del software del sistema affinché essi funzionino in modo corretto, ovvero, affinché l'insieme dei servizi offerti dal sistema informativo possa essere erogato nella maniera più efficiente possibile agli utenti, divenendone dunque responsabile. Assieme allo sviluppo (programmazione) costituisce il filone produttivo di *business* nell'ambito dell'informatica aziendale.

6.1 - Compiti

I principali compiti di un system administrator sono:

- installare e configurare nuovo hardware e software sia lato client che lato server;
- rispondere alle esigenze della direzione della struttura gestita (azienda, ente statale, università, ecc.) (es. vincoli prestazionali e di affidabilità, rispetto di policy di sicurezza ecc...);
- ottenere le migliori prestazioni possibili con l'hardware a disposizione (ottimizzazione delle risorse);
- eseguire configurazioni di sistema opportune o desiderate in rispettivi file di configurazione;
- gestire gli account utente;
- pianificare e verificare la corretta esecuzione di operazioni pianificate come ad es. backup;
- applicare le patch e gli aggiornamenti necessari ai sottosistemi;
- rendere costantemente disponibili i servizi associati al sistema a favore degli utenti;
- analizzare i cosiddetti file di log;
- porre rimedio ai problemi/guasti tramite tecniche di troubleshooting;
- monitorare la struttura e gli apparati di rete, compreso i sistemi di protezione, in collaborazione con l'amministratore di rete;
- adottare adeguati programmi antivirus, firewall ed altri strumenti software o hardware, atti a garantire la massima misura di sicurezza nel rispetto di quanto dettato dalla normativa in materia di protezione dati;
- sovraintendere all'operato di eventuali tecnici esterni all'amministrazione e vigilare sugli interventi informatici diretti al sistema informatico del Titolare effettuati da eventuali operatori esterni;
- collaborare con i responsabili del trattamento dati ed il responsabile della protezione dei dati (D.P.O.);
- coordinare con il titolare e/o i responsabili del trattamento le attività operative del trattamento nello svolgimento delle mansioni loro affidate per garantire un corretto, lecito e sicuro trattamento dei dati personali nell'ambito del sistema informatico e collaborare con essi per l'attuazione delle prescrizioni impartite dall'Autorità Garante per la Protezione dei Dati;
- verificare il rispetto delle norme sulla tutela del diritto d'autore sui programmi installati nei sistemi informatici del titolare;
- comunicare prontamente al titolare del trattamento dei dati qualsiasi situazione, di cui sia venuto a conoscenza, che possa compromettere il corretto trattamento informatico dei dati personali, nonché eventuali casi di non corrispondenza con le norme di sicurezza e su eventuali incidenti;
- rispondere ai quesiti degli utenti;
- documentare le operazioni effettuate.

Il System administrator collabora attivamente con un'altra figura tipica del mondo IT: l'*application manager* che è, invece, colui il quale si occupa della gestione di una specifica applicazione software (un ERP ad

esempio). Una tipica attività sistemistica è quella del cosiddetto *presidio* aziendale di server.

Il System administrator, per l'espletamento delle sue funzioni, ha la facoltà, in qualunque momento, di accedere ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica interna ed esterna. Il System Administrator potrà accedere ai dati ed agli strumenti informatici esclusivamente per permettere alla stessa Azienda, titolare del trattamento, di accedere ai dati trattati da ogni incaricato con le modalità fissate al solo fine di garantire l'operatività, la sicurezza del sistema ed il normale svolgimento dell'attività aziendale nei casi in cui si renda indispensabile ed indifferibile l'intervento, come ad esempio, in caso di prolungata assenza od impedimento dell'incaricato, informando tempestivamente l'incaricato dell'intervento di accesso realizzato.

Art. 7 - Utilizzo del personal computer

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

Il personal computer deve essere custodito con cura evitando ogni possibile forma di danneggiamento.

Eventuali, motivate, modifiche alla configurazione fisica possono essere effettuate solo dai tecnici dell'UOC SIA. Eventuale e motivato spostamento del personal computer può essere effettuato solo se autorizzati dai tecnici dell'UOC SIA.

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

Il personale incaricato dell'UOC SIA ha la facoltà di collegarsi e visualizzare in remoto il desktop delle singole postazioni PC, al fine di garantire l'assistenza tecnica e la normale attività operativa, nonché la massima sicurezza contro virus, spyware, malware, etc. L'intervento viene effettuato esclusivamente su chiamata dell'utente o, in caso di oggettiva necessità, a seguito della rilevazione tecnica di problemi nel sistema informatico e telematico. In quest'ultimo caso, e sempre che non si pregiudichi la necessaria tempestività ed efficacia dell'intervento, verrà data comunicazione della necessità dell'intervento stesso.

Non è consentito l'uso di programmi diversi da quelli ufficialmente installati dal personale dell'UOC SIA per conto dell'Azienda, né viene consentito agli utenti di installare autonomamente programmi provenienti dall'esterno, sussistendo infatti il grave pericolo di introdurre Virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti. L'inosservanza della presente disposizione espone la stessa A.O. a gravi responsabilità civili; si evidenzia inoltre che le violazioni della normativa a tutela dei diritti d'autore sul software, che impone la presenza nel sistema di software regolarmente licenziato, o comunque libero e quindi non protetto dal diritto d'autore, vengono sanzionate anche penalmente.

Salvo preventiva espressa autorizzazione del personale dell'UOC SIA, non è consentito all'utente modificare le caratteristiche impostate sul proprio personal computer, né procedere ad installare dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori. Modem, modem USB, dispositivi di memorizzazione USB ecc…).

Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il personale dell'UOC SIA nel caso in cui siano rilevati virus.

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

Sul personal computer non devono essere presenti file personali, quali ad esempio: fotografie, file musicali, file video, file di attività extra lavorative. I tecnici dell'UOC SIA monitorano con strumenti automatizzati la tipologia di file presenti e procedono, senza nessun preavviso, alla rimozione degli stessi. Durante le operazioni di cambio/sostituzione, del Personal computer (ammodernamento del parco macchine), il tecnico addetto alla sostituzione, rimuoverà, se presenti, tutti i file "non inerenti all'attività lavorativa".

Art. 8 - Politiche di utilizzo delle risorse informatiche aziendali

Le politiche adottate dalla struttura sanitaria ed in particolare dal Titolare del trattamento dei dati personali, in merito all'utilizzo delle risorse informatiche aziendali garantiscono il rispetto dei requisiti di sicurezza stabiliti dal Regolamento (UE) 2016/679 ed in conformità ai piani di sicurezza adottati ai sensi degli artt. 32 (Sicurezza del trattamento) e 35 (Valutazione d'impatto sulla protezione dei dati). Ovvero devono essere finalizzate a garantire la riservatezza, l'integrità e la disponibilità delle informazioni e dei dati del Titolare. In particolare:

- la confidenzialità o riservatezza riguarda la conoscibilità e fruibilità delle informazioni ai soli soggetti autorizzati;
- l'integrità è relativa alla completezza ed inalterabilità delle informazioni;
- la disponibilità concerne l'accessibilità ed usabilità delle informazioni nel tempo da parte dei soggetti autorizzati.

8.1 - Accesso ed utilizzo delle risorse informatiche

Gli utenti possono accedere alle risorse informatiche previa autorizzazione ed esclusivamente per finalità compatibili con le attività lavorative svolte.

Al fine di garantire la corretta operatività delle attività lavorative mediante l'utilizzo di tali strumenti, è vietato:

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

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

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

8.2 - Password Policy e Gestione degli Account

I dipendenti della struttura sanitaria, incluso il personale esterno con cui la struttura sanitaria intrattiene rapporti di collaborazione, accede alle risorse informatiche solo ed esclusivamente previa presentazione e delle proprie credenziali di identificazione ed autenticazione.

Le credenziali di identificazione ed autenticazione sono composte da un identificativo univoco dell'utenza (user-id) e da una password, quest'ultima strettamente personale, non comunicabile e non condivisibile con

terze persone. Pertanto, tutti gli utenti che hanno accesso ad una qualsiasi delle risorse informative aziendali, sono tenuti alla stretta osservanza delle seguenti regole comportamentali:

- l'utente non deve mai condividere le proprie password con nessun altro utente, inclusi colleghi, manager, membri dello staff IT, o utenti Amministratori;
- l'utente non deve mai condividere le proprie password con nessun individuo esterno all'azienda, incluso chiunque affermi di avere una legittima urgente necessità di accedere ad un sistema;
- l'utente deve adottare le dovute accortezze per evitare di cadere vittima di truffe online mirate al furto di credenziali di accesso o altri dati personali (Phishing), tenendo presente che nessuna operazione di sicurezza che richieda la digitazione delle password personali, viene comunicata e gestita tramite la posta elettronica aziendale;
- l'utente deve evitare di trascrivere le proprie password su qualsiasi tipo di supporto, digitale o cartaceo, inclusi i telefoni o altri dispositivi mobili.

Per quanto riguarda la scelta della password, l'utente deve:

- scegliere una password ragionevolmente complessa con una lunghezza di almeno 14 caratteri (il sistema rifiuta password inferiori a 10 caratteri) e composta da una combinazione di lettere maiuscole-minuscole, numeri, e altri caratteri speciali e non deve contenere riferimenti agevolmente riconducibili all'incaricato (es. nome, cognome, codice fiscale ecc.);
- evitare l'utilizzo di parole di senso comune o presenti in un dizionario, o semplici (ad es: "password1", "pa$$word") tali da essere facilmente individuate dai comuni programmi di rilevamento delle password;
- evitare di utilizzare per il proprio account lavorativo una password già utilizzata per un account personale (uso sistematico della medesima password in contesti diversi);
- evitare la memorizzazione della password in funzioni di log-in automatico o nel browser utilizzato per la navigazione Internet;
- nel rispetto della vigente normativa in tema di privacy cambiare periodicamente tutte le password, almeno ogni tre mesi, ovvero con maggior frequenza sulla base della criticità dell'account in questione e ogni qualvolta si abbia il sospetto che la propria password possa essere stata compromessa;
- cambiare appena possibile e comunque al primo accesso la password ricevuta a seguito della creazione di un nuovo account aziendale.

La password dovrà essere custodita dall'incaricato con la massima diligenza e non dovrò essere divulgata per nessun motivo.

Non è consentito in nessun modo l'attivazione della password di accensione (BIOS).

Ogni violazione o sospetta violazione delle proprie credenziali e/o rilevamento di accessi non autorizzati alla propria postazione di lavoro deve essere prontamente comunicata, telefonicamente o mediante la posta elettronica ai tecnici dell'UOC SIA. Nel caso si rilevino accessi non autorizzati a sistemi che trattano dati personali, deve essere prontamente inoltrata una comunicazione anche al Titolare del trattamento dei dati personali e all'Ufficio Privacy.

Le credenziali di autenticazione per l'accesso alla rete vengono assegnate dal personale dell'UOC SIA, previa formale richiesta del responsabile del servizio nell'ambito del quale verrà inserito ed andrà ad operare il nuovo utente.

Art. 9 - Utilizzo della rete locale

Per l'accesso alla rete locale dell'Azienda ciascun utente deve essere in possesso della specifica credenziale di autenticazione.

Le credenziali costituiscono l'Account Istituzionale dell'Utente presso l'Azienda.

Le credenziali vengono revocate alla chiusura del rapporto tra Utente ed Azienda.

L'Utente, preso atto che la conoscenza della password da parte di terzi può consentire agli stessi l'accesso ai servizi in nome dell'Utente titolare e l'accesso ai dati cui il medesimo è abilitato si impegna a:

- non cedere, una volta superata la fase di autenticazione, l'uso della propria Postazione di Lavoro (PdL) a persone non autorizzate;
- non lasciare incustodita ed accessibile la propria PdL una volta connesso al sistema con le proprie credenziali di autenticazione;
- conservare la password nella massima riservatezza e con la massima diligenza avvisare prontamente l'ufficio competente al riguardo nell'ipotesi di smarrimento dei dati di accesso, non utilizzare credenziali di altri utenti nemmeno se fornite volontariamente o di cui si ha casualmente conoscenza.

Risulta opportuno che, con regolare periodicità (almeno ogni tre mesi), ciascun utente provveda alla pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati, essendo infatti necessario evitare un'archiviazione ridondante.

Le unità di rete (file server) sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto qualunque file che non sia legato all'attività lavorativa non può essere registrato, nemmeno per brevi periodi, in queste unità. Su queste unità vengono svolte regolari attività di controllo, amministrazione e backup.

Il system administrator può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza sia sui pc degli incaricati che sulle unità di rete.

L'utilizzo di dispositivi mobili personali come notebook, tablet, smartphone, PDA (Personal Digital Assistance), pone una serie di minacce ai dati memorizzati e/o processati attraverso l'uso di tali dispositivi. Tali minacce, dovute ad esempio alla perdita/furto del dispositivo mobile o la presenza di codice malevolo, possono causare l'accesso non autorizzato ai dati aziendali.

Per tali motivi, non è autorizzato l'utilizzo di dispositivi mobili personali da parte degli utenti per lo svolgimento delle proprie attività lavorative.

È altresì vietata la connessione dei suddetti dispositivi alle reti wireless e wired della struttura sanitaria, nonché la connessione via cavo o bluetooth alle postazioni di lavoro, anche se disconnesse dalla rete aziendale.

9.1 - Regole di utilizzo

Servizi informatici e di rete potranno essere utilizzati dagli Utenti previa autenticazione e nel rispetto del Profilo Utente diappartenenza.

A ciascun Profilo Utente è associato un insieme di servizi informatici e di rete predefiniti.

Ciascun Utente può accedere ed utilizzare unicamente i servizi disponibili per il proprio profilo Utente.

L'Utente è autorizzato all'utilizzo dei servizi unicamente nell'ambito delle proprie funzioni istituzionali dell'Azienda.

Il collegamento alla rete aziendale di dispositivi privati, se ammesso, deve avvenire esclusivamente all'interno di sotto reti appositamente predisposte (es. la rete ospiti per accesso a internet).

Per ciascun Utente, in fase di utilizzo dei servizi, è vietato:

- violare la privacy di altri Utenti o dell'integrità di dati personali;
- compromettere l'integrità dei sistemi o dei servizi;
- consumare risorse in misura tale da compromettere l'efficienza di altri servizi di rete;
- compiere atti di criminalità informatica;
- accedere alla Rete Interna per conseguire l'accesso non autorizzato a risorse di rete interne od esterne all'Azienda;

- fornire il servizio di connettività di rete a soggetti non autorizzati all'accesso alla Rete Interna;
- usare false identità, l'anonimato o servirsi di risorse che consentono di restare anonimi;
- violare gli obblighi contrattualmente assunti dall'Azienda per la realizzazione e la gestione della Rete Interna, particolarmente in materia di copyright, licenze d'uso di software e regolamenti dei fornitori di connettività di rete;
- svolgere attività che causino malfunzionamento, diminuiscano la regolare operatività, distraggano risorse (persone, capacità, elaboratori), danneggino o restringano l'utilizzabilità o le prestazioni della Rete Interna;
- violare la sicurezza di archivi e banche dati, compiere trasferimenti non autorizzati di informazioni (software, basi dati, ecc.), intercettare, tentare d'intercettare o accedere a dati in transito sulla Rete Interna, dei quali non si è destinatari specifici;
- compiere azioni in violazione delle norme a tutela delle opere dell'ingegno, del diritto d'autore e del software;
- distruggere o tentare di distruggere, danneggiare o tentare di danneggiare, intercettare o tentare di intercettare, accedere o tentare di accedere senza autorizzazione alla posta elettronica o ai dati di altri utenti o di terzi, usare, intercettare o diffondere o tentare di intercettare o diffondere password o codici d'accesso o chiavi crittografiche di altri utenti o di terzi, e in generale commettere o tentare di commettere attività che violino la riservatezza di altri utenti o di terzi;
- creare o diffondere immagini, dati o altro materiale potenzialmente offensivo, diffamatorio, o dal contenuto osceno;
- utilizzare la Rete dell'Azienda e i servizi da essa offerti a scopi commerciali e per propaganda politica o elettorale.

Art. 10 - Utilizzo e conservazione dei supporti rimovibili

Tutti i supporti magnetici rimovibili (dischetti, CD e DVD riscrivibili, dischi esterni, memorie a stato solido, ecc.), contenenti dati personali/particolari/giudiziari nonché informazioni costituenti know-how aziendale, devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto o, successivamente alla cancellazione, recuperato.

Al fine di assicurare la distruzione e/o inutilizzabilità di supporti magnetici rimovibili contenenti dati personali, ciascun utente dovrà contattare il personale dell'UOC SIA e seguire le istruzioni da questo impartite.

E' vietato l'utilizzo di supporti rimovibili personali.

L'utente è responsabile della custodia dei supporti e dei dati aziendali in essi contenuti.

L'eventuale utilizzo di supporti magnetici esterni (es. dischi rigidi USB, USB Pen Drive, SD (Secure Digital mini, micro e nano), unità CD/DVD-ROM USB ecc.) contenenti dati personali, particolari e giudiziari è possibile solo internamente all'Azienda e previa autorizzazione del Direttore dell'UOC SIA e la loro custodia deve avvenire solo in armadi ignifughi chiusi a chiave. Eventuali manomissioni nella custodia ed esposizione a possibili utilizzi dei supporti da parte di terzi devono considerarsi quali potenziali violazioni alla protezione e sicurezza dei dati (cd. data breach) che se riguardanti dati personali, particolari e giudiziari vanno notificati al Garante Protezione Dati Personali entro 72 ore dall'evento (art. 33 GDPR) ed eventualmente agli interessati (art. 34 GDPR).

Art. 11 - Utilizzo di personal computer portatili

L'utente è responsabile del Personal Computer portatile assegnatogli e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

I Personal Computer portatili utilizzati all'esterno, solo in casi particolari (Forum, manutenzione e/o monitoraggio dei sistemi informatici Aziendali da remoto) e in ogni caso su esplicita autorizzazione della Direzione Strategica Aziendale, devono essere custoditi con diligenza, adottando tutti i provvedimenti che le circostanze rendono necessari per evitare danni o sottrazioni.

Nella fattispecie l'utilizzo di dispositivi cellulari e computer portatili, all'esterno dei locali dell'Azienda, deve essere oggetto di particolare cura ed attenzione da parte degli Utenti perché tale utilizzo rappresenta una fonte di rischi particolarmente rilevante in termini di sicurezza, sia delle risorse in sé sia dei dati nelle stesse contenuti. Tali dispositivi, infatti, possono essere soggetti a smarrimento, furti, distruzione o compromissione dei dati, tentativi di frode e/o accesso non autorizzato ovvero essere "*infettati*" da virus o codice malevole che potrebbero diffondersi e ripercuotersi all'intera rete informatica dell'Amministrazione, una volta che tali dispositivi siano collegati direttamente alla rete interna.

È necessario, pertanto, adottare ulteriori norme comportamentali nonché specifiche procedure, di seguito descritte, che gli Utenti sono chiamati ad applicare in modo scrupoloso:

- cifrare i dati (laddove possibile e previa analisi dei rischi/costi-benefici);
- fare periodicamente delle copie di back-up dei dati e verificarle regolarmente;
- mantenere abilitato l'antivirus;
- non disabilitare le impostazioni di sicurezza originariamente impostate dall'Amministrazione;
- evitare di accedere e navigare in siti web "pericolosi" per la sicurezza informatica, a prescindere dal fatto che ciò avvenga al di fuori dell'orario di lavoro;
- non mantenere abilitati protocolli insicuri di comunicazione, come ad es. il bluetooth, oltre il tempo strettamente necessario.

Infine, per essi valgono i medesimi obblighi di notifica di violazione della protezione dei dati personali in analogia a quanto indicato nel precedente paragrafo relativo all'uso dei supporti e unità di memorizzazione.

I Personal Computer portatili, se non dotati di connessione VPN, per garantire il corretto aggiornamento degli applicativi installati, devono essere connessi alla rete aziendale, almeno ogni due settimane, per il tempo necessario all'aggiornamento.

Art. 12 - Uso della posta elettronica

La casella di posta elettronica (e-mail) assegnata all'utente è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

È fatto divieto di utilizzare le caselle di posta elettronica *nome.cognome@ospedalideicolli.it* per motivi diversi da quelli strettamente legati all'attività lavorativa.

L'accesso alla posta elettronica aziendale viene fornito al personale al fine di svolgere le attività lavorative o in adempimento di contratti di collaborazione con persone esterne all'azienda. Essendo l'utilizzo della posta elettronica aziendale legato ai vincoli contrattuali, questa può essere oggetto di monitoraggio da parte dell'Azienda.

L'utente deve utilizzare la posta elettronica avendo consapevolezza delle minacce a cui è potenzialmente esposto questo mezzo, evitando ad esempio l'apertura di allegati ai messaggi di posta (anche se provenienti da persone conosciute) il cui nome del file termini in (abbia estensione)

.COM .EXE .VBS .SCR .PIF, ZIP, RAR o che abbia un'estensione ambigua o sconosciuta (gli allegati possono, infatti, contenere virus o codici nascosti di natura dolosa che possono comportare la divulgazione di password o la compromissione di dati aziendali).

Ogni casella di posta è assegnata in maniera nominale ed univoca ad una persona fisica, pertanto ogni utente è direttamente responsabile sia da un punto di vista disciplinare che giuridico del suo utilizzo e del contenuto dei messaggi inviati.

L'utente deve utilizzare la posta elettronica aziendale evitando di inviare e-mail che contengano:

- informazioni che violano le normative vigenti e le policy aziendali;
- materiale che possa diffamare, danneggiare, o arrecare un danno reputazionale alla struttura sanitaria o qualsiasi altra persona fisica o giuridica;
- messaggi di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;
- fotografie, filmati o brani musicali (es.mp3) non legati all'attività lavorativa.

È inoltre vietato l'utilizzo della mail aziendale per:

- falsificare il mittente dei messaggi allo scopo di simulare l'identità di un altro utente (Spoofing);
- inviare e-mail originate dalla rete della struttura sanitaria per conto di altri Internet Service Provider;
- utilizzare l'indirizzo di posta elettronica aziendale per partecipare a discussioni su forum, aste on line, newsgroup o mailing-list, salvo diversa ed esplicita autorizzazione.

L'utente è pertanto responsabile sia disciplinarmente che giuridicamente dei danni arrecati attraverso l'uso privato, improprio o illecito della posta elettronica aziendale.

La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati di dimensioni rilevanti.

La documentazione elettronica che costituisce per l'azienda "know-how" aziendale tecnico o commerciale protetto (tutelato in base all'art. 6 bis del r.d. 29.6.1939 n.1127), e che, quindi, viene contraddistinta da diciture od avvertenze dirette ad evidenziarne il carattere riservato o segreto a tutela del patrimonio dell'impresa, non può essere comunicata all'esterno senza preventiva autorizzazione della Direzione Strategica.

Per la trasmissione di file all'interno dell'Azienda Ospedaliera dei Colli è possibile utilizzare la posta elettronica, prestando attenzione alla dimensione degli allegati. È obbligatorio controllarei file attachment di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).

È vietato inviare catene telematiche (o di Sant'Antonio). Non si devono in alcun caso attivare gli allegati di tali messaggi.

È possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario, ma di norma per la comunicazione ufficiale è obbligatorio avvalersi degli opportuni strumenti quali ad esempio la PEC.

La Legge 9 agosto 2013, n. 98 "Conversione in Legge, con modificazioni, del Decreto Legge 21 giugno 2013, n. 69, recante disposizioni urgenti per il rilancio dell'economia" (G.U. n. 194 del 20/08/2013 - Suppl. Ordinario n. 63) ed in vigore dal 21 agosto, con l'art. 14 ha modificato l'art. 47 del D.Lgs 82/2005 Codice dell'Amministrazione Digital - CAD relativo alle comunicazioni tra PA. In particolare è stata introdotta la frase "*È in ogni caso esclusa la trasmissione di documenti a mezzo fax*".

L'Azienda è dotata di un certo numero di e-mail certificate (PEC). La posta elettronica certificata è il sistema attraverso il quale è possibile inviare e-mail con valore legale equiparato ad una raccomandata con ricevuta di ritorno come stabilito dalla vigente normativa. Questo sistema presenta delle forti similitudini con il servizio di posta elettronica "tradizionale", cui però sono state aggiunte delle caratteristiche tali da fornire agli utenti la certezza, a valore legale, dell'invio e della consegna (o meno) dei messaggi e-mail al destinatario. La Posta Elettronica Certificata ha lo stesso valore legale della raccomandata con la ricevuta di ritorno con attestazione dell'orario esatto di spedizione. Con il sistema di Posta Certificata è garantita la certezza del contenuto: i protocolli di sicurezza utilizzati fanno sì che non siano possibili modifiche al contenuto del messaggio e agli eventuali allegati. La Posta Elettronica Certificata, garantisce, in caso di contenzioso, l'opponibilità a terzi del messaggio. Allo stesso modo, il gestore del destinatario invia al mittente la ricevuta di avvenuta consegna.

Art. 13 - Accesso ad internet

Il PC abilitato alla navigazione in Internet costituisce uno strumento aziendale necessario allo svolgimento della propria attività lavorativa. È, pertanto, assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa stessa.

È fatto divieto all'utente lo scarico di software gratuito (freeware) e shareware prelevato da siti Internet, se non espressamente autorizzato dal Direttore dell'UOC SIA.

La user ID assegnata al singolo utente ed abilitato alla navigazione in Internet costituisce uno strumento aziendale utilizzabile esclusivamente per lo svolgimento della propria attività lavorativa. È quindi assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa. In questo senso l'utente non potrà utilizzare internet per:

- l'upload o il download di software, nonché l'utilizzo di documenti provenienti da siti web o http, se non strettamente attinenti all'attività lavorativa (filmati e musica) e previa verifica dell'attendibilità dei siti in questione (nel caso di dubbio, dovrà venir a tal fine contattato il personale dell'UOC SIA);
- ogni forma di registrazione e accesso a siti i cui contenuti non siano strettamente legati all'attività lavorativa;
- la partecipazione a Forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche (è un'utilità interattiva che permette ai visitatori di un sito web di poter lasciare firme e commenti) anche utilizzando pseudonimi (o nicknames) se non espressamente autorizzati dal Responsabile del Servizio.

L'accesso ad Internet è consentito da tutte le postazioni di lavoro, previa autorizzazione del Responsabile della struttura, mediante policy di accesso basate su gruppi "Active Directory" attribuite dall'UOC SIA.

È da evitare ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa. E' stata individuata una tabella contenente i siti raggiungibili "White List" e una tabella contenente i siti non raggiungibili "Black List" da parte degli utenti autorizzati ad accedere ad Internet.

Dalle ore 13,30 (quando si riduce notevolmente l'affluenza agli sportelli aperti al pubblico) alle ore 16,30 (orario dopo il quale iniziano sia le attività di back-office degli uffici aperti al pubblico che le operazioni di manutenzione e backup da parte dei tecnici dell'UOC SIA) è possibile navigare senza limitazioni accedendo a tutti i siti ad eccezione di quelli presenti nella tabella "Blacklist".

I Direttori di UOC e di UOSD per le funzioni ricoperte, hanno libero accesso ad internet ad esclusione dei siti contenuti nella tabella "Black List".

L'Utente è direttamente e totalmente responsabile dell'uso di Internet, delle informazioni che immette, delle modalità con cui opera, dei siti web o pagine internet ai quali abbia stabilito collegamento tramite link.

Inoltre, nell'ottica di migliorare la sicurezza informatica, e tenuto conto delle disposizioni impartite dal Ministero per la pubblica Amministrazione e l'Innovazione Tecnologica, dall'Autority per l'informatica e dagli atri organismi del settore, l'Azienda si dota di appositi strumenti hardware e software (firewall, antivirus, Vulnerabilty Assessment) opportunamente predisposti e configurati per impedire accessi non autorizzati alla rete aziendale (haker, spoofing, sniffing, hijacking) e attacchi di tipo virale o malware (worm, spyware, trojan, dialer, ramsonware, backdoor, etc.).

Sempre nell'ottica di migliorare la sicurezza informatica ed in osservanza dei principi dettati dal D.Lgs. 14 settembre 2015 n. 151, l'Azienda può disporre, sempreché non prolungati e previa adeguata informativa fornita al lavoratore, eventuali controlli senza necessità di accordi sindacali preventivi, compiuti dal personale incaricato della UOC SIA, mirati alla verifica di eventuali violazioni al presente regolamento; tali interventi potranno avvenire mediante un sistema di controllo dei contenuti (Web Filtering) o mediante "file di log" della navigazione svolta. Il controllo sui file di log non è continuativo ed i file stessi vengono conservati non oltre 30 giorni, ossia il tempo indispensabile per il corretto perseguimento delle finalità organizzative e di sicurezza dell'azienda.
Infine è fatto assoluto divieto dell'utilizzo, su PC o Notebook connessi alla rete aziendale, di connessioni attraverso dispositivi removibili come Internet Key, chiavette USB, dispositivi PCMCIA o similari per la navigazione in Internet, se non espressamente forniti e autorizzati dall'UOC SIA.

Art. 14 - Protezione antivirus

Il sistema informatico dell'A.O. è protetto da software antivirus, aggiornato quotidianamente. Ogni utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale mediante virus o mediante ogni altro software aggressivo.

Nel caso il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente sospendere ogni elaborazione in corso, senza spegnere il computer e segnalare l'accaduto al personale dell'UOC SIA.

Ogni supporto di memoria di provenienza esterna all'Azienda dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, dovrà essere prontamente consegnato al personale dell'UOC SIA.

Art. 15 - Gestione della VPN

I dipendenti e/o i fornitori, per l'accesso in VPN (Virtual Private Network), devono usare esclusivamente dispositivi aziendali. È vietato l'uso di dispositivi personali salvo casi particolari, che dovranno di volta in volta, essere autorizzati dal Titolare del trattamento insieme al Responsabile del Trattamento interno e al Direttore dei Sistemi Informativi Aziendali.

È espressamente vietato utilizzare le risorse informatiche e la rete aziendale per scopi incompatibili con quelli stabiliti nel presente Regolamento ed eventualmente ad un Regolamento più specifico qualora esistente. In particolare, a titolo esemplificativo e non esaustivo, è vietato:

- accedere all'infrastruttura del Titolare per conseguire l'accesso non autorizzato a risorse di rete interne od esterne al Titolare;
- fornire il servizio di connettività di rete a soggetti non autorizzati all'accesso all'infrastruttura;
- violare gli obblighi contrattualmente assunti dal Titolare per la realizzazione e la gestione della propria infrastruttura, particolarmente in materia di copyright, licenze d'uso di software e regolamenti dei fornitori di connettività di rete;
- svolgere attività che causino malfunzionamento, diminuiscano la regolare operatività, danneggino o restringano l'utilizzabilità o le prestazioni dei sistemi del Titolare;
- violare la sicurezza di archivi e banche dati, compiere trasferimenti non autorizzati di informazioni (software, basi dati, ecc.), intercettare, tentare d'intercettare o accedere a dati in transito sull'infrastruttura del Titolare, dei quali non si è destinatari specifici;
- compiere azioni in violazione delle norme a tutela delle opere dell'ingegno, del diritto d'autore e del software;
- distruggere o tentare di distruggere, danneggiare o tentare di danneggiare, intercettare o tentare di intercettare, accedere o tentare di accedere senza autorizzazione alla posta elettronica o ai dati di altri Utenti o di terzi, usare, intercettare o diffondere o tentare di intercettare o diffondere password o codici d'accesso o chiavi crittografiche di altri Utenti o di terzi, e in generale commettere o tentare di commettere attività che violino la riservatezza di altri Utenti o di terzi, così come tutelata dalle norme civili, penali e amministrative applicabili.

Il Titolare può disattivare, in qualsiasi momento, le credenziali o disconnettere un accesso VPN, senza necessità di preventivo avviso, qualora la disattivazione sia necessaria all'integrità o al funzionamento dei propri servizi ICT, oppure qualora vi sia fondato sospetto che l'Utente VPN abbia violato il presente Regolamento. Il Titolare utilizzerà sia sistemi di monitoraggio della rete che sistemi in grado di verificare che l'operato dell'Utente VPN risponda a quanto previsto dal presente Regolamento e nel rispetto delle normative vigenti.

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

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

Art. 16 - Richieste di acquisto apparecchiature informatiche

Le Unità Operative potranno richiedere all'UOC SIA l'acquisto di postazioni informatiche utilizzando esclusivamente l'apposito modulo, reperibile sul sito aziendale mediante il link http://www.ospedalideicolli.it/moduli/modello-richiesta-acquisto-hardware.pdf sul quale dovranno essere evidenziate le tipologie di apparecchiature da acquistare (PC, portatili, stampanti, multifunzione ecc) senza esplicitare le caratteristiche tecniche che saranno sempre definite dall'UOC SIA in base alla finalità della richiesta. Si precisa che, come indicato nel modulo sopra richiamato, la richiesta dovrà essere corredata del visto del Direttore del Dipartimento di afferenza. La stessa, successivamente, sarà trasmessa al management per l'autorizzazione e, quindi, in caso positivo, all'UOC Provveditorato per la definizione della procedura di acquisizione.

Art. 17 - Sistemi di controllo graduali

In caso di anomalie, il personale incaricato dell'UOC SIA effettuerà controlli anonimi, che si concluderanno con avvisi generalizzati diretti ai dipendenti dell'area o del settore in cui è stata rilevata l'anomalia, nei quali si evidenzierà l'utilizzo irregolare degli strumenti aziendali con l'invito ad attenersi scrupolosamente alle istruzioni impartite.

Art. 18 - Osservanza delle disposizioni in materia di privacy

È obbligatorio attenersi alle disposizioni in materia di Privacy di cui al D.Lgs. 196/2003 e ss.mm.ii. e ed al Regolamento UE 679/2016, nonché alle disposizioni organizzative, alle istruzioni, alle misure di sicurezza ed alle procedure aziendali adottate dal Titolare in materia.

Art. 19 - Sanzioni

È fatto obbligo a tutti gli utenti di osservare le disposizioni portate a conoscenza con il presente regolamento. Il mancato rispetto o la violazione delle regole sopra indicate viene valutata ai fini disciplinari, fermo restando l'eventuale responsabilità civile, amministrativa, penale e contabile, qualora ve ne siano i presupposti.

Art. 20 - Aggiornamento e revisione

Tutti gli utenti possono proporre integrazioni al presente Regolamento. Le proposte verranno esaminate dalla Direzione Strategica e dall'UOC SIA.

II presente Regolamento è soggetto a revisione.