AZIENDA SANITARIA LOCALE AVELLINO

ORIGINALE ☐

COPIA ☐

IL DIRETTORE GENERALE

Deliberazione n. 1637 **del** 22-12-2017

OGGETTO: Sicurezza dati. Adozione Nuovo Regolamento

PUBBLICAZIONE

Dichiarazione di conformità del trattamento dei dati ex D.lgs. n. 196/2003 e ss.mm.ii.

Premesso che il D.l.vo196/2003 e ss.mm.ii. contiene principi e prescrizioni per il trattamento dei dati personali, anche con riferimento alla loro "diffusione", il Proponente la presente deliberazione dichiara di aver valutato la rispondenza del testo, compreso degli eventuali allegati, destinato alla diffusione per il mezzo dell'Albo Pretorio alle suddette prescrizioni e ne dispone la pubblicazione nei modi di legge.

(Firma del proponente)

ATTESTATO PUBBLICAZIONE

Si attesta che la presente deliberazione è stata affissa all'Albo Pretorio il giorno: 22 DIC. 2017

ai sensi dell'art.124 c.1 L.vo 267/2000, per giorni 15

Il Responsabile Ufficio Delibere e Determine

DICHIARAZIONE DI REGOLARITÀ CONTABILE:

il presente atto trova capienza di spesa all'autorizzazione :

n. del

n. del

n. del

In presenza di fattura di importo superiore a € 10.000,00 prima dell'emissione del relativo mandato di pagamento l'UOC Contabilità Generale effettuerà il controllo "Equitalia

Il Direttore U.O.C Contabilità Generale

☒ Il presente provvedimento è reso immediatamente esecutivo.

IL DIRETTORE GENERALE

Dr.ssa Maria Morgante

PROPOSTA DI DELIBERA

Oggetto: Sicurezza dati. Adozione Nuovo Regolamento

Il Dott. Gaetano Antonio Capone in qualità di Direttore/ Responsabile dell' U.O.C S.I.A.

PREMESSO che:

- il Decreto del Commissario ad Acta n. 18 del 18/02/2013 " Atto di indirizzo per l' adozione dell' Atto Aziendale delle Aziende Sanitarie della Regione Campania " al punto 11.3 *Regolamenti* , così recita: *" I Direttori Generali o i Commissari Straordinari, entro 90 gg dalla approvazione dell' Atto Aziendale da parte degli organismi regionali competenti, ai fini di una sua corretta e completa applicazione, procedono all'adozione di regolamenti interni; tutti i regolamenti adottati dovranno essere pubblicati sui siti web aziendali";*
- l' Atto Aziendale della ASL Avellino con delibera n. 1154 del 13/09/2017, al punto 3. Regolamenti ed al punto 2 capo VI " Adozione dei Regolamenti interni " ribadisce quanto indicato al punto 11.3 Regolamenti del succitato DCA n. 18/2013;
- il Decreto del Commissario ad Acta della regione Campania n. 40 del 25/09/2017 approva l' Atto Aziendale dell' Azienda Sanitaria Locale Avellino;

CONSIDERATO che:

- il Direttore Generale ha chiesto, ai dirigenti aziendali interessati, con nota prot. n. 11725/DG del 05 dicembre 2016 e con nota prot. n. 11726/DG del 06 dicembre 2016 di avviare la stesura o la revisione dei Regolamenti, relativi a svariate materie sia previste al punto 3 dell' Atto Aziendale sia ulteriori, e con successivi solleciti prot. n. 2124/ del 14 marzo 2017, prot. n. 1512/DG e 8513/DG del 07 novembre 2017, e con apposita riunione convocata con nota prot. n. 7838/DG del 06 ottobre 2017;

VISTO :

- il testo del Regolamento "Sicurezza dati" allegato al presente provvedimento e che ne forma parte integrante e sostanziale;

DATO ATTO CHE:

- Tutta la documentazione originale a supporto del presente atto è depositata e custodita presso la U.O.C. proponente;

DICHIARATA la regolarità giuridico amministrativa della presente proposta di provvedimento, a seguito dell'istruttoria effettuata, nel rispetto delle proprie competenze, funzioni e responsabilità;
Tutto ciò premesso, argomentato ed attestato, il sottoscritto Direttore

PROPONE AL DIRETTORE GENERALE

L'adozione del presente provvedimento e, nello specifico:

1. L'adozione del Regolamento **"sicurezza Dati"**

Direttore UOC S.I.A.
Dott. Gaetano Capone

IL DIRETTORE GENERALE

dell'Azienda Sanitaria Locale Avellino, Dott.ssa Maria Morgante, nominato con D.G.R.C. n. 427 del 27/07/2016 e immesso nelle funzioni con D.P.G.R.C. n.179 del 01/08/2016, coadiuvato dal Direttore Amministrativo dr. Ferdinando Memoli e dal Direttore Sanitario Dott.ssa Emilia Anna Vozzella ha adottato la seguente delibera:

Vista

la *suesposta proposta del Direttore dell' U.O.C. Sistemi Informativi Aziendali avente ad oggetto: "*

Sicurezza dati" Adozione nuovo Regolamento"

Preso atto

- Dell'espressa dichiarazione di regolarità giuridico amministrativa resa dal Direttore dell' U.O.C. S.I.A. a seguito della istruttoria dallo stesso effettuata e come dallo stesso attestato ed articolato;
- Di tutto quanto riportato nella proposta di delibera;

Ritenuto

Di prendere atto, quale parte integrante e sostanziale del presente provvedimento, della suesposta proposta resa dal Direttore dell' U.O.C. S.I.A. e sulla scorta ed in conformità della stessa;

Con i pareri favorevoli resi, alla luce di tutto quanto sopra riportato ed attestato, dal Direttore Sanitario e dal Direttore Amministrativo con la sottoscrizione della presente proposta di provvedimento;

Il Direttore Amministrativo
Dr. Ferdinando Memoli

Il Direttore Sanitario
Dott.ssa Emilia Anna Vozzella

DELIBERA

- **di prendere atto**, quale parte integrante e sostanziale del presente provvedimento, della suesposta proposta resa dal Direttore dell' U.O.C. S.I.A. e sulla scorta ed in conformità della stessa;
- **di adottare** il Regolamento dal titolo **" Sicurezza dati";** che, allegato al presente provvedimento, ne forma parte integrante e sostanziale;
- **di disporre** che il succitato Regolamento sia pubblicato sul sito web istituzionale, a cura del dirigente proponente;
- **di inviare** la presente deliberazione ai sensi della normativa vigente al Collegio Sindacale, e al dirigente proponente per il seguito di competenza.

Il Direttore Generale
Dr.ssa Maria Morgante

☐ Esecutiva in data _____

INVIO AL COLLEGIO SINDACALE

Prot. n. - 2750 - *del* 22 DIC. 2017

Il Responsabile Ufficio
Delibere e Determine

UOC SIA

REGOLAMENTO SICUREZZA
Sicurezza dati

Premessa

L'esigenza di adottare un regolamento per l'utilizzo dei personal computer fissi e portatili, dei dispositivi elettronici aziendali in genere (quali a titolo esemplificativo, fotocopiatrici, scanner, masterizzatori, telefoni fissi, cellulari aziendali, pen drive e supporti di memoria), della posta elettronica e di internet nasce dal ricorso sempre più frequente a tali strumenti nell'organizzazione e nell'espletamento dell'attività lavorativa.

In applicazione di quanto disposto dagli artt. 2104 e 2105 c.c., l'utilizzo di tali indispensabili risorse deve realizzarsi nell'ambito del generale contesto di diligenza, fedeltà e correttezza che caratterizzano il rapporto di lavoro, adottando tutte le cautele e le precauzioni necessarie per evitare le possibili conseguenze dannose che un utilizzo non avveduto degli strumenti in questione può provocare.

Limitatamente al settore del pubblico impiego, l'art. 10 del Codice di comportamento dei dipendenti delle pubbliche amministrazioni, allegato al C.C.N.L. del 22/01/2004, stabilisce che *"Il dipendente non utilizza a fini privati materiale o attrezzature di cui dispone per ragioni di ufficio"*. Tale disposizione, in quanto richiamata dal Codice regolamento del C.C.N.L. del comparto, costituisce non solo norma di valenza etico- comportamentale, ma altresì un vero o proprio obbligo la cui inosservanza è passibile di sanzione penale e/o regolamento.

Per finalità esclusivamente di tutela della sicurezza dei dati e del sistema informatico, come prescritto dagli artt. 33 e seguenti del D.Lgs. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali", il DPS del 2011, comunque, prevedeva misure di sicurezza per il trattamento dei dati personali, un apposito regolamento contenente, tra l'altro, istruzioni in ordine all'utilizzo di personal computer e della rete Aziendale, della posta elettronica e di internet, nonché degli altri dispositivi elettronici nell'ambiente di lavoro.

In tale contesto, con deliberazione n. 13 del 1° marzo 2007, il Garante per la protezione dei dati personali ha inteso prescrivere ai datori di lavoro alcune misure per conformare alle disposizioni vigenti il trattamento di dati personali effettuato, per verificare il corretto utilizzo nel rapporto di lavoro della posta elettronica e della rete internet.

La stesura di una specifica regolamentazione in materia di utilizzo di strumenti informatici da parte dei dipendenti — nello specifico pubblici — è stata di recente auspicata anche dalla Presidenza del Consiglio dei Ministri, Dipartimento della Funzione pubblica, con la Direttiva n. 2 del 26 maggio 2009 del Ministro per la Pubblica Amministrazione e l'Innovazione.

Art. 1 Principi generali

1. Il presente regolamento è adottato per assicurare la funzionalità e il corretto impiego dei dispositivi elettronici aziendali in generale, della posta elettronica e di internet da parte degli utenti; a tale fine, definisce le modalità d'uso di tali strumenti nell'organizzazione dell'attività lavorativa e amministrativa e di controllo.
2. Le presenti disposizioni e prescrizioni affiancano ed integrano quelle già previste nel contratto di lavoro e, in generale, nelle disposizioni pattizie o regolamentari vigenti.
3. Il luogo di lavoro è una formazione sociale nella quale è assicurata la tutela dei diritti, delle libertà fondamentali e della dignità degli interessati garantendo che, in una cornice di reciproci diritti e doveri, sia assicurata l'esplicazione della personalità del lavoratore e una ragionevole protezione della

sua sfera

riservatezza nelle relazioni personali e professionali (artt. 2, 15 e 41, secondo comma, Costituzione, Art. 2087 c.c., art. 2, comma 5, Codice dell'amministrazione digitale, D.lgs. 7 marzo 2005, n. 82).

4. Le regole che disciplinano l'utilizzo dei dispositivi elettronici aziendali, della posta elettronica e di internet ed i relativi controlli, si conformano, pertanto, ai seguenti principi generali:

Principio di necessità (ex art. 3 del D.lgs. 30 giugno 2003, n. 196)

I sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità.

Per quanto riguarda l'attività di controllo, essa può essere intrapresa solo in caso di fondato sospetto di compimento di attività illecite da parte degli utenti o per esigenze legate alla sicurezza del sistema informatico/informativo aziendale.

Principio di correttezza (ex art. 11, comma 1, lett. a) del D.lgs. 30 giugno 2003, n. 196)

Le caratteristiche essenziali del trattamento sono rese note ai lavoratori. Ciò assume particolare rilievo nel caso di trattamenti di dati acquisiti dall'elaborazione di informazioni relative alla corrispondenza elettronica, poiché un simile trattamento postula necessariamente il ricorso a tecnologie dell'informazione che, in modo più marcato rispetto ad apparecchiature tradizionali, permettono di svolgere trattamenti ulteriori rispetto a quelli connessi ordinariamente all'attività lavorativa.

Principio di determinatezza e legittimità delle finalità del trattamento (ex art. 11, comma 1, lett. b) del D.Lgs. 30 giugno 2003, n. 196)

Principio di pertinenza e non eccedenza

Il datore di lavoro deve trattare i dati nella misura meno invasiva possibile e per uno scopo predeterminato, esplicito e legittimo. Le attività di controllo sono svolte solo da soggetti preposti e devono essere mirate sull'area di rischio, tenendo conto della normativa sulla protezione dei dati e, se pertinente, del principio di segretezza della corrispondenza.

Art. 2 Diffusione del regolamento e sua efficacia

1. Gli utenti dell'ASL Avellino saranno informati dell'adozione del presente regolamento tramite apposita circolare e con pubblicazione sulla "Intranet Aziendale".
2. Il regolamento potrà essere aggiornato ogniqualvolta se ne presenti l'opportunità e di tali revisioni sarà data tempestiva comunicazione ai dipendenti.
3. Le disposizioni contenute nel presente regolamento si applicano a tutti i Sigg. operatori di ogni livello Aziendale, nonché a tutti i soggetti rispetto ai quali verranno espressamente riconosciute applicabili, ad esempio facendo riferimento al presente regolamento nei relativi contratti (es. collaboratori esterni, stagisti, borsisti, consulenti).
4. E' responsabilità di tutti i soggetti che utilizzano il personal computer ed altri dispositivi elettronici, la posta elettronica e internet messi a disposizione dall'ASL Avellino, applicare e rispettare puntualmente le disposizioni del presente regolamento.Fonti normative di riferimento:
    - D.lgs. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali";
    - Linee guida del Garante per la Protezione dei Dati personali per posta elettronica e internet (Deliberazione n. 13 del 1° marzo 2007 del Garante);
    - Contratti collettivi nazionali per i dipendenti del comparto Regioni/Enti locali,

categorie e per i dipendenti di Area Dirigenziale e rispettivi contratti collettivi decentrati integrativi;

- Statuto dei Lavoratori, il contenuto del presente regolamento costituisce, per i dipendenti, disposizione di servizio e deve considerarsi integrativo di quanto previsto da:
  - informative in materia di trattamento dei dati personali rilasciate ai dipendenti ai sensi dell'art. 13 del Codice in materia di protezione dei dati personali,
  - lettere di incarico destinate a responsabili e incaricati e le istruzioni ivi contenute, così come qualsiasi altra prescrizione in materia di protezione dei dati personali.

Art. 3 Valutazione del rischio

La rete informatica dell'ASL Avellino, l'accesso alla rete internet e alla posta elettronica, il PC ed altri strumenti informatici affidati al dipendente, sono strumenti di lavoro. Su di essi si effettuano regolari attività di controllo e non possono in alcun modo essere utilizzati per scopi diversi in quanto ogni utilizzo non inerente l'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. In relazione all'utilizzo non corretto di detti strumenti si individuano i seguenti rischi possibili e conseguenti effetti:

Attività	Rischio	Motivazione	Possibile effetto
Manutenzione di periferiche hardware interne (schede video, memoria, etc.)	Alto	Possono essere danneggiati componenti interni e il PC	Danneggiamento dei PC
Manutenzione di periferiche hardware esterne (tastiere, mouse, etc.)	Basso		
Download non controllato o non programmato di aggiornamenti relativi ad applicazioni installate dal responsabile di rete	Alto	Possono essere scaricate applicazioni non verificate con il pericolo di portare Virus informatici o di alterare la stabilità delle applicazioni dell'elaboratore	Danneggiamento del software del PC o della rete informatica interna.
Download di dati non inerenti alle attività lavorative (musica, giochi, etc.)	Alto	Possono essere scaricate applicazioni non verificate con il pericolo di portare Virus informatici o di alterare la stabilità delle applicazioni dell'elaboratore.	Danneggiamento del software del PC o della rete informatica. Gravi responsabilità civili e penali per l'Istituto in caso di violazione della normativa a tutela dei diritti d'autore.
Installazione di applicazioni senza l'autorizzazione del responsabile della rete	Alto	Possono essere installate applicazioni non compatibili	Danneggiamento del software del PC o della rete informatica interna.
Accesso alla rete effettuato da PC di proprietà dell'utente	Alto	Accessi non autorizzati alla rete	Furto di dati
Apertura di allegati di posta elettronica di incerta provenienza	Alto	Contenere Malware/Spyware	Danneggiamento del software del PC o della rete informatica interna Divulgazione di password e dati riservati
Elaboratore connesso alla rete lasciato incustodito o divulgazione di password	Alto	Possibile utilizzo da parte di terzi	Uso indebito di dati riservati, danneggiamento della rete informatica interna.

Utilizzo di supporti removibili esterni non autorizzati	Alto	Possono essere trasferite applicazioni dannose per il PC nella rete informatica	Danneggiamento dei PC o della rete informatica interna Furto di dati
Mancata distruzione o perdita accidentale di supporti magnetici riutilizzabili (dischetti, nastri, DAT, chiavi USB, CD riscrivibili) contenente dati sensibili e giudiziari	Alto	Recupero di dati memorizzati anche dopo la loro cancellazione	Uso indebito di dati riservati

Art. 4 Regole relative all'utilizzo del personal computer e degli altri dispositivi elettronici aziendali

1. I personal computer fissi e portatili ed i programmi su di essi installati sono uno strumento di lavoro. L'uso per fini personali è da considerarsi pertanto escluso. Contenendo anche dati e informazioni personali di terzi, ai sensi del D.lgs. 30 giugno 2003 n. 196, detti strumenti devono essere utilizzati e conservati, insieme alla relativa documentazione esplicativa, con diligenza e cura, attenendosi alle prescrizioni fornite dal datore di lavoro e dal presente regolamento.
2. Le impostazioni dei personal computer e dei relativi programmi installati sono predisposti dagli addetti informatici incaricati, sulla base di criteri e profili decisi dall'amministrazione, in funzione delle mansioni del dipendente cui questo è adibito, nonché delle decisioni e della politica di utilizzo di tali strumenti stabilita dall'Amministrazione stessa. L'utente non può modificarli autonomamente e può ottenere dall'Amministratore di Sistema cambiamenti nelle impostazioni solo, previa autorizzazione, motivata, da parte del proprio Dirigente.
3. Le UU.OO. Aziendali preposte all'acquisto prima di procedere all'acquisto, noleggio o leasing di qualsiasi strumento informatico Hardware o Software (quali a titolo esemplificativo personal computer fissi, portatili, fotocopiatrici, scanner, masterizzatori, telefoni fissi, cellulari aziendali, pen drive, supporti di memoria, applicativi software o altro) sono tenuti ad acquisire il parere dell'Amministratore di Sistema o alla U.O.C. SIA/Informatica, al fine di verificare la compatibilità dell'hardware con il sistema informatico Aziendale.
4. Non è consentito installare, collegare o allacciare autonomamente al sistema informatico Aziendale nessun dispositivo elettronico (quali a titolo esemplificativo personal computer fissi, portatili, fotocopiatrici, scanner, masterizzatori, telefoni fissi, cellulari aziendali, pen drive e supporti di memoria) senza preventiva autorizzazione dell'Amministratore di Sistsema.
5. L'installazione sui personal computer di sistemi operativi e programmi applicativi e, in generale, di software avviene ad opera dei tecnici informatici incaricati, che operano seguendo i necessari criteri di sicurezza. 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.
6. Senza preventiva autorizzazione dell'Amministratore di Sistema, non è consentito installare autonomamente programmi provenienti dall'esterno, né utilizzare programmi diversi da quelli distribuiti ed installati ufficialmente. L'inosservanza di questa disposizione, infatti, oltre al rischio di diffondere virus informatici e di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre l'Amministrazione a gravi responsabilità civili ed anche penali, in caso di violazione della normativa a tutela dei diritti d'autore sul software, (D.Lgs. 518/92 sulla tutela giuridica del software e L. 248/2000 nuove norme di tutela del diritto d'autore) che impone la presenza nel sistema di software regolarmente licenziato o comunque libero (open surce). Abusi o utilizzi illeciti saranno puniti conformemente alle disposizioni che disciplinano il rapporto di lavoro. In ogni caso, l'utente sarà responsabile e sarà chiamato a manlevare e tenere indenne l'Amministrazione da qualsiasi danno o richiesta di risarcimento avanzata da terzi.
7. Tutti i software caricati sul sistema operativo ed in particolare i software necessari per la protezione

dello stesso o della rete internet (quali antivirus) non possono essere disinstallati o in nessun modo manomessi, salvo quando questo sia richiesto dall'Amministratore di Sistema per compiere attività di manutenzione o aggiornamento.

8. Il personal computer va spento prima di lasciare gli uffici. In caso di allontanamento, anche temporaneo, dalla stazione di lavoro, l'utente del PC non deve lasciare il sistema operativo aperto con la propria password inserita. Al fine di evitare che persone estranee effettuino accessi non permessi, lo stesso deve attivare il salvaschermo con password o deve bloccare il computer dopo essere uscito da tutti gli applicativi.
9. Nell'ipotesi di assenza o impossibilità, temporanea o protratta nel tempo, dell'utente del PC e qualora, per ragioni di sicurezza o comunque per garantire l'ordinaria operatività aziendale, sia necessario accedere a informazioni o documenti di lavoro presenti sul suo personal computer, inclusi i messaggi di posta elettronica in entrata ed in uscita, e l'utente non abbia ottemperato a quanto sopra specificato, il responsabile della struttura a cui è assegnato il dipendente può richiedere con apposita e motivata richiesta all'Amministratore del Sistema di accedere alla postazione e/o alla casella di posta elettronica del dipendente assente, in modo che si possa prendere visione delle informazioni e dei documenti necessari. Contestualmente, il responsabile della struttura ha l'obbligo di informare l'utente del PC dell'avvenuto accesso appena possibile, fornendo adeguata motivazione.
10. Per finalità di assistenza, manutenzione e aggiornamento e previo consenso esplicito dell'utente, l'Amministratore di Sistema o soggetti appositamente incaricati allo svolgimento di tale attività, potrà accedere da remoto al personal computer dell'utente attraverso un apposito programma software.
11. L'Amministratore di sistema effettuerà, inoltre, attività di monitoraggio e verifica dell'efficacia delle protezioni predisposte sul sistema informativo rispetto ad aggressioni esterne senza che siano date ulteriori informative.
12. I programmi antivirus e, in generale, i software necessari per la protezione del sistema operativo, delle singole postazioni di lavoro e della rete internet, sono aggiornati in modo automatico.
13. L'utente del PC al fine di garantire la disponibilità dei documenti di lavoro deve assicurare il backup e ha obbligo di custodire lo stesso in luogo sicuro onde evitare accessi involontari alle informazioni. Senza la preventiva autorizzazione del proprio Dirigente (responsabile del trattamento) non è consentita la creazione di nuove ed autonome banche dati personali.
14. Non è consentita l'installazione sul proprio personal computer di nessun dispositivo di memorizzazione, comunicazione o altro (come ad esempio, modem, pen usb smartphone ...), se non previa autorizzazione espressa dell'Amministratore di Sistema, nel qual caso, deve prestare la massima attenzione, avvertendo immediatamente l'Amministratore di Sistema nel caso in cui vengano rilevati virus.
15. L'utente è tenuto ad osservare le medesime prescrizioni, precauzioni e cautele, ove queste siano applicabili e pertinenti rispetto allo specifico strumento utilizzato, in relazione a tutti gli altri dispositivi elettronici aziendali di cui fa uso (fotocopiatrici, scanner, masterizzatori, telefoni fissi, cellulari aziendali, pen drive e supporti di memoria).
16. supporti di memoria portatili e comunque riutilizzabili, qualora sono necessari, dovranno essere custoditi con la massima cura ed utilizzati adottando le necessarie cautele affinché soggetti estranei non possano venire a conoscenza dei documenti e delle informazioni ivi contenute.

Art. 5 Selezione e gestione della password

1. L'accesso al personal computer, ai programmi applicativi e alle varie funzionalità avviene previa autenticazione, che consiste nella verifica dell'identità dell'utente attraverso l'uso di un codice

identificativo e di una parola chiave (*password*) nonché, quando richiesto dal sistema, di una smart card personale.

2. Scelta, custodia, modifica e utilizzo della *password* devono rispettare le seguenti prescrizioni:
   - la *password* è attribuita e comunicata all'utente dall'Amministratore di Sistema;
   - appena digitata, il sistema obbliga immediatamente l'utente a sostituirla con una a sua scelta;
   - quest'ultima può essere formata da lettere (maiuscole o minuscole) e numeri, ricordando che lettere maiuscole e minuscole hanno significati diversi per il sistema; deve essere composta da almeno otto caratteri (la sua sicurezza è direttamente proporzionale alla sua lunghezza) e non deve contenere riferimenti agevolmente riconducibili all'utente (nome, cognome, data di nascita ecc..);
   - sono da ritenersi di soddisfacente sicurezza le password che presentano le seguenti caratteristiche:
     a) composte da caratteri maiuscoli e minuscoli ovvero da una miscela di numeri e lettere
     b) composte anche da caratteri di interpunzione (es. @ , #, *, ", ecc.)
     c) facilmente digitabili senza dover guardare la tastiera, per ridurre al minimo il tempo di digitazione ed il rischio di essere osservati da terzi;
   - l'utente ha la responsabilità di custodire con diligenza la propria password (ed i dispositivi fisici eventualmente in suo possesso); è fatto assoluto divieto di inserire la propria password in messaggi di posta elettronica e non, di scriverla su un qualunque documento o foglio, di archiviarla in un qualunque tipo di sistema di elaborazione (incluso il telefono cellulare, il computer palmare e simili) senza utilizzare un algoritmo di cifratura. In nessuna circostanza l'utente è autorizzato a condividere le proprie credenziali di autenticazione (User-Id, password) con altri o terze persone, fatto salvo quanto più sopra previsto in caso di assenza o impossibilità;
   - l'utente è obbligato dal sistema a cambiare la propria password su base almeno semestrale, non riutilizzando le tre password precedentemente usate; nel caso di trattamento di dati sensibili e di dati giudiziari la periodicità della variazione deve essere ridotta a tre mesi (come previsto dal punto 5 del regolamento tecnico allegato al D.lgs. 196/2003).
   - l'Amministratore di Sistema ha la responsabilità di assicurare che la componente pubblica delle credenziali di autenticazione (il "codice utente" o User-Id) non sia più riutilizzata per identificare altri utenti del sistema, neanche in tempi diversi o successivi.
3. In caso di furto o smarrimento e nel caso in cui, l'utente, abbia fondato motivo di ritenere che possa essere compromessa la riservatezza della password o comunque che ne sia stato fatto un utilizzo indebito. Qualora l'utente venga a conoscenza della password di altro, è tenuto a darne immediata notizia al proprio Dirigente ed all'Amministratore di sistema.

Art. 6 Disattivazione del profilo di autenticazione

1. Il mancato utilizzo della credenziale di autenticazione per un periodo superiore a sei mesi comporta l'automatica disattivazione della stessa. L'utente, per riprendere l'operatività, dovrà contattare il proprio Dirigente.
2. La credenziale di autenticazione sarà disattivata nel caso in cui l'utente cessi il suo rapporto con l' ASL Avellino, oltre che nei casi espressamente e tassativamente previsti dalla normativa.

Art. 7 Disattivazione del profilo di autorizzazione

1. Il profilo di autorizzazione concesso a ciascun utente decade automaticamente ogni 6 mesi e in caso di cambiamento di mansioni o di incarico, la revoca dell'account è fatta dal Dirigente.

Art. 8 Utilizzo della rete dell'amministrazione

1. Le unità di rete sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto qualunque files che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità, vengono svolte regolari attività di controllo, di esame del *log* di sistema, di amministrazione e di *backup*.
2. Le password d'ingresso alla rete ed ai programmi sono segrete e vanno gestite secondo le istruzioni. E' assolutamente proibito entrare nella rete e nei programmi con altri nomi utente.
3. L'Amministratore di sistema può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza sia sui PC degli utenti sia sulle unità di rete.
4. Costituisce buona regola la periodica (almeno ogni sei mesi) pulizia degli archivi, con cancellazione dei file obsoleti o inutili e con la pulizia del "cestino". Particolare attenzione deve essere prestata alla duplicazione dei dati. E' infatti assolutamente da evitare un'archiviazione ridondante.
5. E' cura dell'utente effettuare la stampa dei dati solo se strettamente necessaria e di ritirarla prontamente dai vassoi delle stampanti comuni.
6. E' buona regola evitare di stampare documenti o file non adatti (molto lunghi o non supportati, come ad esempio il formato pdf o file di contenuto grafico) su stampanti locali.
7. La stampa di elaborati di grosse dimensioni e a colori va eseguita ove possibile in bozza prima di creare le copie definitive.

Art. 9 Regole applicabili all'utilizzo di internet

1. La rete internet può essere utilizzata unicamente per svolgere attività rientranti tra i compiti istituzionali.
2. E' fatto divieto all'utente lo scarico di software gratuito (freeware) e shareware prelevato da siti Internet, se non espressamente autorizzato dall'Amministratore di sistema, al quale va inviata richiesta scritta, motivata e vistata dal Dirigente.
3. E' tassativamente vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, salvo i casi direttamente autorizzati dal rispettivo Dirigente e con il rispetto delle vigenti procedure di acquisto.
4. E' da evitare ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.
5. È vietata la partecipazione a Forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames).
6. Con riferimento a quanto previsto al paragrafo 3, ultimo periodo, della direttiva n. 2 del 26.05.2009 del Dipartimento della Funzione Pubblica della Presidenza del Consiglio dei Ministri, l'Amministrazione tollera l'utilizzo delle proprie risorse informatiche di comunicazione per attività non istituzionali da parte di coloro che ne sono assegnatari nei seguenti casi:
    a. per il ricorre di motivi di comprovata necessità ed urgenza;
    b. per assolvere incombenze amministrative e burocratiche senza allontanarsi dal luogo di lavoro (ad es, per effettuare adempimenti online nei confronti di pubbliche amministrazioni e di concessionari di servizi pubblici, ovvero per tenere rapporti con istituti bancari ed assicurativi).

    Tale utilizzo, a carattere occasionale, non deve compromettere le normali attività d'istituto e deve essere contenuto nei tempi strettamente necessari. L' Amministratore di sistema non è responsabile in alcun modo di furto di dati sensibili/economici (phishing) ai danni dell'utente.
7. L'accesso ad Internet è protetto da sistemi di verifica dell'identità dell'utente ed i siti accessibili

sono diversificati in relazione al profilo professionale rivestito.

8. Al fine di ridurre il rischio di un utilizzo improprio di internet e, allo stesso tempo, di evitare per quanto possibile controlli che potrebbero comportare il trattamento di dati personali, anche sensibili e giudiziari, sono di seguito evidenziati i principi che devono essere rispettati e le misure che l'Amministrazione si riserva di adottare:
   - rispetto della normativa vigente in materia di protezione di diritti di proprietà intellettuale nell'acquisizione, riproduzione, condivisione di immagini, di musica, filmati e software;
   - utilizzo di internet nel rispetto delle leggi vigenti e del presente regolamento, prestando particolare cautela al fine di non importare *virus, spam* o altri programmi informatici dannosi;
   - utilizzo di ulteriori sistemi e filtri che possono prevenire determinate operazioni — reputate incoerenti con l'attività amministrativa — quali l'upload o l'accesso a determinati siti e/o il download di file o software, aventi particolari caratteristiche (quali ad esempio dimensionali o di tipologia di dato), con individuazione di categorie e liste di siti cui è concesso l'accesso e categorie di siti cui non è concesso l'acceso *("blacklists")*, in quanto non correlati con l'attività lavorativa/amministrativa.
9. I *log* di connessione sono eliminati automaticamente dal sistema ogni sei mesi come previsto dal D.lgs. 196/2003 Un eventuale prolungamento del tempo di conservazione è possibile, in via eccezionale, in relazione:
   - a particolari esigenze tecniche o di sicurezza
   - all'indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria
   - all'obbligo di custodire o di consegnare dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria.

Art. 10 Regole applicabili all'utilizzo della posta elettronica

1. La casella di posta elettronica è uno strumento finalizzato allo scambio di informazioni nell'ambito dell'attività svolta presso l'Amministrazione.
2. La casella di posta elettronica deve necessariamente appartenere al dominio istituzionale "xxxx@aslavellino.it" e " xxxxx@pec.aslavellino.it" per quella certificata.
3. E' fatto divieto di utilizzare le caselle di posta elettronica non istituzionali del tipo libero.it, gmail.com ecc.
4. E' fatto divieto di utilizzare le caselle di posta elettronica per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail-list, salvo diversa ed esplicita autorizzazione.
5. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.
6. Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti deve essere visionata od autorizzata dal proprio Dirigente e, in ogni modo, è opportuno fare riferimento alle procedure in essere per la corrispondenza ordinaria.
7. Per la trasmissione di comunicazioni all'interno della Azienda dovrà essere privilegiato l'uso della posta elettronica (art. 33 - comma 1 lett. m) - della legge 18 giugno 2009 n. 69), prestando attenzione alla dimensione degli allegati.
8. E' obbligatorio controllare i file attachment di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).
9. E' vietato inviare catene telematiche (o di Sant'Antonio). Se si dovessero ricevere messaggi di tale tipo, si deve procedere all'immediata cancellazione. Non si devono in alcun caso attivare gli allegati di tali messaggi.
10. I messaggi di posta elettronica "sospetti" o provenienti da soggetti estranei o sconosciuti non

devono essere aperti prima dell'intervento dell'Amministratore di sistema. Gli utenti non devono mai aprire allegati con il suffisso ".exe., .bat ecc.".

11. L'utente assegnatario di casella di posta elettronica è responsabile del corretto utilizzo della stessa. Le comunicazioni via posta elettronica devono avere un contenuto espresso in maniera professionale e corretta, nel rispetto della normativa vigente e devono contenere un avvertimento ai destinatari del seguente tenore: "Il presente messaggio contiene informazioni di natura professionale attinente all'attività lavorativa; ai fini dello svolgimento dell'attività lavorativa le eventuali risposte potranno essere rese note da altri soggetti nell'ambito dell'organizzazione del mittente. Questo messaggio di posta elettronica e il suo contenuto sono riservati e confidenziali e il loro utilizzo è consentito esclusivamente al destinatario del messaggio, per le finalità indicate nel messaggio stesso. Se per errore ricevete questo messaggio o non siete il soggetto destinatario o delegato dal destinatario alla lettura, Vi preghiamo di darcene immediatamente notizia via e-mail e di procedere alla distruzione del messaggio stesso, cancellandolo dal Vostro sistema; costituisce comportamento contrario ai principi dettati dal D.lgs. 196/2003 il trattenere il messaggio stesso, divulgarlo anche in parte, distribuirlo ad altri soggetti, copiarlo, diffonderne comunque il contenuto".
12. Al fine di garantire la continuità all'accesso dei messaggi da parte dei soggetti adibiti ad attività lavorative che richiedono la condivisione di una serie di documenti, si consiglia e si incoraggia l'utilizzo abituale di caselle di posta elettronica condivise tra più lavoratori o delle caselle di posta istituzionali dell'Azienda, eventualmente affiancandole a quelle individuali.
13. In caso di assenza prolungata programmata, si consiglia e si raccomanda al dipendente di attivare il sistema di risposta automatica ai messaggi di posta elettronica ricevuti, indicando nel messaggio di accompagnamento, le coordinate di un collega o della struttura di riferimento che può essere contattata in sua assenza e/o altre modalità utili di contatto della struttura organizzativa presso cui presta la propria attività lavorativa.
14. In caso di cessazione dell'attività presso l'Amministrazione, la casella di posta elettronica sarà prontamente disattivata. Se per esigenze lavorative sorgesse la necessità di accedere al contenuto di tale casella di posta, il responsabile della struttura organizzativa a cui il dipendente è assegnato potrà inoltrare motivata richiesta all'Amministratore di Sistema.
15. Qualora si verifichino anomalie nell'invio e ricezione dei messaggi di posta elettronica dovrà essere prontamente informato l'Amministratore di Sistema.

Art. 11 Controlli sull'osservanza del regolamento

1. Per garantire la funzionalità e la sicurezza del sistema informatico, l'Amministrazione si riserva di effettuare controlli per accertare l'osservanza del presente regolamento. Rispetto a tali controlli il presente regolamento costituisce preventiva e completa informazione nei confronti dei dipendenti e degli amministratori.
2. Gli eventuali controlli, generali ed estesi, atti a verificare condotte non conformi al presente regolamento, avverranno preliminarmente su dati aggregati (c.d. "controllo anonimo") riferiti all'intera struttura lavorativa, ovvero al Settore o al Dipartimento qualora il Settore, per caratteristiche intrinseche alla struttura organizzativa, non offrisse garanzie di completa anonimità della verifica. Nel caso vengano rilevate anomalie o irregolarità, potrà essere inviato un avviso generalizzato ai dipendenti che richiami questi ultimi all'utilizzo corretto degli strumenti elettronici aziendali nel rispetto della normativa vigente e dei diritti dei terzi, con l'invito ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite.
3. Qualora le anomalie o le irregolarità dovessero persistere, si procederà circoscrivendo l'invito al personale afferente all'area in cui è stata rilevata l'anomalia. In caso di ripetute anomalie o

irregolarità, si procederà a controlli su base individuale, su singoli nominativi, basi e postazioni.

4. Qualora venga constatata la violazione del presente regolamento, l'Amministrazione potrà irrogare le sanzioni previste dai contratti collettivi vigenti, nel rispetto delle procedure stabilite dagli stessi contratti.
5. Oltre a tali controlli di carattere generale, l'Amministrazione si riserva comunque la facoltà 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 sono, comunque, illecite.
6. L'Amministrazione si riserva, inoltre, di effettuare specifici controlli sui software caricati sui personal computer al fine di verificarne la regolarità sotto il profilo delle autorizzazioni e delle licenze, nonché, in generale, la conformità degli stessi alla normativa vigente e, in particolare, alle disposizioni in materia di proprietà intellettuale.