REGOLAMENTO PER L'UTILIZZO DEGLI STRUMENTI E SERVIZI INFORMATICI DELL'E.R.S.U. DI MESSINA

(Approvato con Decreto del Presidente del C.d.A. n°39 del 18.05.2018)

INDICE

Art. 1
Premesse

L'utilizzo delle risorse informatiche e telematiche dell'E.R.S.U. di Messina, **nel prosieguo E.R.S.U.**, in applicazione di quanto disposto dagli artt. 2104 e 2105 c.c., deve avvenire nell'ambito del generale contesto di diligenza, fedeltà e correttezza che caratterizza il rapporto lavorativo fra l'E.R.S.U. e i propri dipendenti e adottando tutte le cautele e le precauzioni necessarie per evitare le possibili conseguenze dannose alle quali un utilizzo non avveduto di tali strumenti può produrre, anche in considerazione della difficoltà di tracciare una netta linea di confine tra l'attività lavorativa e la sfera personale e la vita privata del lavoratore e di terzi che interagiscono con quest'ultimo.

In tale contesto, il Garante ha emanato la Deliberazione n°13 del 01.03.2007 "*Lavoro: le linee guida del Garante per posta elettronica e internet*" con la quale 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, nello svolgimento del rapporto di lavoro, della posta elettronica e della rete internet.

La progressiva diffusione delle nuove tecnologie informatiche, le maggiori possibilità di interconnessione tra computer e l'aumento di informazioni trattate con strumenti elettronici aumentano infatti i rischi legati alla sicurezza e all'integrità delle informazioni oltre alle conseguenti responsabilità previste dalla normativa vigente in materia.

Il presente Regolamento è adottato al fine di richiamare le indicazioni e le misure necessarie e opportune per il corretto utilizzo nel rapporto di lavoro dei personal computer (fissi e portatili), dei dispositivi elettronici dell'Ente in generale, della posta elettronica e di internet, definendone le modalità di utilizzo nell'ambito dell'attività lavorativa e dando la massima diffusione alla cultura sulla sicurezza informatica.

Le disposizioni e le prescrizioni qui indicate vanno affiancate e integrano quelle già previste nel Documento Programmatico sulla Sicurezza (DPS).

In particolare, l'utilizzo delle risorse e dei servizi informatici deve avvenire:

- nel rispetto delle leggi e norme vigenti e in particolare delle leggi in materia di sicurezza, privacy, copyright, accesso e uso dei sistemi informatici e telematici;
- nel rispetto dei diritti alla riservatezza e alla dignità come sanciti dallo Statuto dei lavoratori e dal Codice sulla privacy, al fine di, garantire la massima efficienza delle risorse informatiche e del loro utilizzo;
- nel rispetto delle norme e procedure lavorative generali definite dall'Ente;
- nel rispetto dei diritti degli altri utenti e di terzi.

L'Ente deve provvedere a garantire un servizio continuativo, nel suo stesso interesse, e assicurare la riservatezza delle informazioni e dei dati, in maniera tale da evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla sicurezza nel trattamento dei dati o diminuire l'efficienza delle risorse informatiche.

L'E.R.S.U. riconosce il valore fondamentale dell'utilizzo di strumenti di comunicazione sia nella comunicazione interna che con l'utenza esterna, anche al fine di ridurre i tempi di risposta e di migliorare pertanto l'efficienza del proprio operato.

Art. 2
Oggetto e ambito di applicazione

Il presente Regolamento contiene le disposizioni relative alle corrette modalità di utilizzo della rete informatica dell'Ente e di tutte le risorse informatiche, in conformità e nel rispetto di quanto previsto dalla specifica normativa di settore e dalle ulteriori disposizioni emanate dall'Ente.

Gli strumenti informatici oggetto del presente Regolamento sono tutti i servizi e gli apparati di proprietà dell'Ente messi a disposizione degli Utenti al fine di permettere il quotidiano svolgimento delle proprie prestazioni lavorative.

Essi sono essenzialmente individuabili nei computer, negli apparati removibili, nei sistemi di identificazione e di autenticazione informatica, Internet e negli strumenti di scambio di comunicazioni e file, nella posta elettronica e in qualsiasi altro programma e apparecchiatura informatica destinata a memorizzare o a trasmettere dati e informazioni.

È responsabilità di tutti i soggetti che utilizzano gli strumenti informatici messi a disposizione, di applicare e rispettare puntualmente le disposizioni del presente Regolamento.

Ferme restando le disposizioni normative in materia, e tutte le prescrizioni previste per il trattamento dei dati sensibili o giudiziari, il contenuto del presente Regolamento costituisce disposizione di servizio e deve considerarsi integrativo di quanto previsto dal Documento Programmatico sulla Sicurezza (DPS).

Il presente Regolamento si applica a tutto il personale:
- a qualunque titolo in servizio all'Ente;
- utilizzato dall'Ente;
- dipendente di società esterne che per la loro attività utilizzano risorse informatiche dell'Ente senza distinzione di ruolo e/o livello, nonché a tutti i collaboratori a prescindere dal rapporto contrattuale con la stessa intrattenuto (collaboratori a progetto, stagisti e borsisti, liberi professionisti, collaboratori terzi, ecc.).

Sono esentati dall'applicazione del presente Regolamento, e limitatamente a quanto necessario per il corretto svolgimento delle proprie funzioni, gli Amministratori di Sistema.

Per qualsiasi dubbio relativo all'applicazione pratica o all'interpretazione autentica delle disposizione contenute nel presente Regolamento, è possibile rivolgersi al Coordinatore Informatico o al Responsabile del C.E.D. compilando apposito quesito o inviando una segnalazione all'indirizzo di posta elettronica afferente alla Struttura.

Art. 3
Entrata in vigore, pubblicità e revisione

Il presente Regolamento entra in vigore alla data della sua approvazione, che avviene mediante deliberazione del Consiglio di Amministrazione o di atto equipollente, e sarà pubblicato sulla Intranet dell'Ente fornendo apposita comunicazione a tutto il personale.

Il Regolamento potrà essere soggetto a revisione sulla base dell'evoluzione normativa e tecnologica nonché sulla base delle nuove esigenze di sicurezza e di azioni correttive che si dovranno eventualmente intraprendere. Le eventuali revisioni apportate verranno approvate mediante deliberazione del Consiglio di Amministrazione o di atto equipollente e di tali revisioni sarà data tempestiva comunicazione ai dipendenti.

Art. 4
Definizioni

Ai sensi del D.Lgs.196/03 e del Provvedimento del Garante per la protezione dei dati personali del 27.11.2008 intitolato "*misure e accorgimenti prescritti ai Titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema*", si intende per:

- *"**trattamento**"*, qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;
- "***trattamento informatico***", trattamento effettuato con l'ausilio di strumenti elettronici;
- "***dato personale***", qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;
- "***dati identificativi***", i dati personali che permettono l'identificazione diretta dell'interessato;
- "***dati sensibili***", i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;
- "***dati giudiziari***", i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da *a)* a *o)* e da *r)* a *u)*, del D.P.R. 14.11.2002, n°313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;
- "***titolare***", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;
- "***responsabile***", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali; in riferimento al trattamento dei dati con strumenti elettronici particolare rilevanza assume il "*responsabile del trattamento dei dati informatici e telematici*", di cui al punto successivo;
- "***coordinatore informatico***" responsabile del coordinamento di tutte le attività di office automation, di informatica e di telematica;
- "***responsabile del trattamento dati informatici e telematici***" (denominato D.I.T.), per le sue specifiche competenze è identificato nel Responsabile del C.E.D. Le competenze del Responsabile di cui sopra riguardano l'attività di controllo e gestione degli impianti di elaborazione o di sue componenti, di basi di dati, di reti, di apparati di sicurezza e di sistemi di software complessi (nella misura in cui consentono di intervenire su dati), l'individuazione e attuazione di tutte le procedure fisiche, logiche e organizzative per tutelare la sicurezza e la riservatezza nel trattamento dei dati informatici. Il Responsabile del trattamento dati informatici e telematici designa, per iscritto, gli amministratori di

sistema, previa individuazione delle caratteristiche di esperienza, capacità e affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

- "***incaricati***", le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;
- "***amministratore di sistema***", la persona fisica dedicata alla gestione e alla manutenzione di impianti di elaborazione o di sue componenti e tutte le figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati personali, quali gli amministratori di basi di dati, di reti informatiche, di apparati di sicurezza e di sistemi di software complessi, nella misura in cui consentano di intervenire sui dati personali; soggetti che, pur non essendo preposti ordinariamente a operazioni implicanti una comprensione del dominio applicativo (significato dei dati, formato delle rappresentazioni e semantica delle funzioni), possono, nelle loro consuete attività, essere concretamente responsabili di specifiche fasi lavorative comportanti elevate criticità rispetto alla protezione dei dati personali; Vanno considerati a tutti gli effetti alla stregua di trattamenti di dati personali il salvataggio dei dati (backup/recovery), l'organizzazione dei flussi di rete, la gestione dei supporti di memorizzazione e la manutenzione hardware, anche quando non consultati "in chiaro" dall'amministratore.
- "***interessato***", la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;
- *"**utente**"*, soggetto che accede e utilizza i servizi e gli strumenti del sistema informatico dell'Ente;
- "***comunicazione***", il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal Responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- "***diffusione***", il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- "***dato anonimo***", il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;
- "***banca di dati***", qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti;
- "***comunicazione elettronica***", ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico. Sono escluse le informazioni trasmesse al pubblico tramite una rete di comunicazione elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad un abbonato o utente ricevente, identificato o identificabile;
- "***reti di comunicazione elettronica***", i sistemi di trasmissione, le apparecchiature di commutazione o di instradamento e altre risorse che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, incluse le reti satellitari, le reti terrestri mobili e fisse a commutazione di circuito e a commutazione di pacchetto, compresa Internet, le reti utilizzate per la diffusione circolare dei programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica, nella misura in cui sono utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato;

- "***rete pubblica di comunicazioni***", una rete di comunicazioni elettroniche utilizzata interamente o prevalentemente per fornire servizi di comunicazione elettronica accessibili al pubblico;
- "***misure minime***", il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti all'art. 31 del D.Lgs. n°196/2003;
- "***risorse informatiche***":
  - i server;
  - le workstation, i personal computer, i notebook e qualsiasi altra tipologia di elaboratore elettronico;
  - le stampanti, i plotter, i fotocopiatori e i fax;
  - tutti gli strumenti informatici interconnessi con la rete dell'E.R.S.U.;
  - gli apparati di rete;
  - tutto il software e i dati acquisiti o prodotti da parte degli utenti o di terzi autorizzati;
  - file di qualsiasi natura, archivi di dati anche non strutturati e applicazioni informatiche.

Art. 5
Principi generali

I trattamenti devono rispettare le garanzie in materia di protezione dei dati e svolgersi nell'osservanza di alcuni cogenti principi:

- il principio di necessità, secondo cui i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi in relazione alle finalità perseguite (*art. 3 del codice in materia di protezione dei dati personali; paragrafo 5.2 delle linee guida del Garante per posta elettronica e internet, GURI n°58 del 10.03.2007*);
- il principio di *correttezza*, secondo cui le caratteristiche essenziali dei trattamenti devono essere rese note ai lavoratori (*art. 11, comma 1, lett. a), del codice in materia di protezione dei dati personali*). Le tecnologie dell'informazione (*in modo più marcato rispetto ad apparecchiature tradizionali*) permettono di svolgere trattamenti ulteriori rispetto a quelli connessi ordinariamente all'attività lavorativa. Ciò, all'insaputa o senza la piena consapevolezza dei lavoratori, considerate anche le potenziali applicazioni di regola non adeguatamente conosciute dagli interessati (*paragrafo 3 delle linee guida del Garante per posta elettronica e internet, GURI n°58 del 10.03.2007*);
- i trattamenti devono essere effettuati per finalità *determinate*, *esplicite* e *legittime* (*art. 11, comma 1, lett. b), del codice in materia di protezione dei dati personali: paragrafi 4 e 5 delle linee guida del Garante per posta elettronica e internet, GURI n°58 del 10.03.2007*), osservando il principio di *pertinenza* e *non eccedenza* (*paragrafo 6 delle linee guida del Garante per posta elettronica e internet, GURI n°58 del 10.03.2007*). Il datore di lavoro deve trattare i dati *"nella misura meno invasiva possibile"*; le attività di monitoraggio devono essere svolte solo da soggetti preposti (*paragrafo 8 delle linee guida del Garante per posta elettronica e internet, GURI n°58 del 10.03.2007*) ed essere *"mirate sull'area di rischio, tenendo conto della normativa sulla protezione dei dati e, se pertinente, del principio di segretezza della corrispondenza"* (*parere 8/2001 sul trattamento di dati personali nell'ambito dei rapporti di lavoro adottato il 13.09.2001, punti 5 e 12*).

Art. 6
Linee guida generali

L'E.R.S.U., consapevole delle potenzialità fornite dagli strumenti informatici e telematici, li mette a disposizione dell'Utente esclusivamente per finalità di tipo lavorativo.

Non è quindi permesso utilizzare questi strumenti per altre finalità non connesse all'attività lavorativa o in modo che violino le leggi italiane vigenti in materia. Ad esempio, non è consentito:

- accedere a siti e acquisire o comunque diffondere prodotti informativi lesivi del comune senso del pudore;
- diffondere prodotti informativi lesivi dell'onorabilità, individuale e collettiva;
- diffondere prodotti informativi di natura politica;
- diffondere in rete o con qualsiasi altro mezzo di comunicazione, informazioni riservate di qualunque natura;
- svolgere ogni tipo di attività commerciale;
- compiere attività che possano rappresentare una violazione della legge in materia di Copyright, fra le quali la copia non autorizzata di software, supporti audio e video, clonazione o programmazione di smart card;
- compiere attività che compromettano in qualsiasi modo la sicurezza delle risorse informatiche e della rete dell'Ente.

L'E.R.S.U. adotterà ogni accorgimento tecnico necessario a tutelarsi da eventuali comportamenti non permessi, salvaguardando il rispetto della libertà e della dignità dei lavoratori; gli eventuali trattamenti effettuati saranno ispirati a canoni di trasparenza.

Art. 7
Titolarità

L'E.R.S.U. è titolare di tutte le risorse hardware e software messe a disposizione degli utenti dell'Ente.

Tutto l'hardware e il software in dotazione alle Strutture deve essere acquisito in accordo con le specifiche tecniche fornite dal Coordinatore Informatico e/o dal Responsabile del C.E.D.

Tutte le risorse informatiche assegnate devono essere custodite con cura evitando ogni possibile forma di danneggiamento. Gli utenti sono responsabili del corretto utilizzo degli strumenti messi loro a disposizione e della loro custodia e sono tenuti a segnalare tempestivamente al Coordinatore Informatico o al Responsabile del C.E.D., eventuali guasti o difetti di funzionamento dei dispositivi hardware e software.

Art. 8
Competenze e responsabilità

Il Responsabile del C.E.D. è tenuto a:

- elaborare le regole per un utilizzo ragionevolmente sicuro del sistema informativo dell'Ente;
- implementare, con l'ausilio del personale incaricato interno/esterno, le regole di sicurezza sul sistema informativo dell'Ente;
- monitorare, con l'ausilio di personale incaricato della Struttura Semplice Informatica e

Innovazione Tecnologica, e/o di personale incaricato interno/esterno, i sistemi per individuare un eventuale uso scorretto degli stessi, nel rispetto della privacy degli utenti;
- segnalare prontamente ai Dirigenti delle Strutture interessate ogni eventuale attività non autorizzata sul sistema informativo dell'Ente;
- attenersi alle prescrizioni previste nel "*Documento di adozione delle misure e accorgimenti prescritti dal Garante per la Protezione dei Dati Personali ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema*".

I Dirigenti dell'Ente sono tenuti a:
- informare il personale dipendente e/o assimilato sulle disposizioni in merito all'uso consentito delle risorse del sistema informativo dell'Ente;
- assicurare che il personale a loro assegnato si uniformi alle regole e alle procedure descritte nel presente regolamento;
- assicurare che i fornitori e/o il personale incaricato esterno si uniformino alle regole ed alle procedure descritte nel presente regolamento;
- adempiere a tutti gli obblighi inerenti la responsabilità loro affidata in materia di trattamento di dati personali e sensibili gestiti dall'Ente;
- segnalare prontamente al Coordinatore Informatico o al Responsabile del C.E.D. ogni eventuale attività non autorizzata sul sistema informativo dell'Ente.

Il Responsabile del C.E.D. e l'eventuale personale esterno incaricato che concorre alla gestione/implementazione del sistema informativo dell'Ente è tenuto a:
- garantire la massima riservatezza sulle informazioni acquisite direttamente o indirettamente nell'esercizio delle proprie funzioni;
- segnalare prontamente al Coordinatore Informatico ogni eventuale attività non autorizzata sul sistema informativo dell'Ente.

Gli Utenti del sistema informativo dell'Ente sono responsabili per ciò che concerne:
- il rispetto delle regole dell'Ente per l'uso consentito del sistema informativo;
- l'uso delle credenziali di autenticazione loro assegnate secondo le modalità previste nel presente Regolamento;
- la pronta segnalazione al competente Dirigente in merito a ogni eventuale attività non autorizzata sul sistema informativo dell'Ente di cui vengano a conoscenza.

Art. 9
Credenziali di accesso

I sistemi di controllo degli accessi assolvono il compito di prevenire che persone non autorizzate possano accedere a un sistema informatico e alle relative applicazioni.

Lo scopo è di cautelare l'Ente e i suoi dipendenti da ogni tipo di manomissione, furto o distruzione di dati oltre che di limitare l'accesso a specifici dati da parte di personale non autorizzato.

Art. 10
Password

Ove l'accesso al sistema avviene tramite autenticazione delle credenziali (normalmente nome utente e password), l'Utente dovrà:

- custodire con diligenza le proprie credenziali e non comunicarle ad altre persone (es.: non scrivere la password su carta o post-it lasciandoli sulla scrivania o attaccati al monitor; non comunicare, né condividere con altri la propria password);
- durante la digitazione della propria password, assicurarsi che nessuno stia osservando la tastiera con l'intenzione di memorizzarla.

La password deve essere composta da almeno otto caratteri e deve essere "robusta". Una password si dice robusta quando è difficile ricostruirla e cioè quando risponde ad alcuni principi:
- all'aumentare della sua lunghezza, aumenta la difficoltà a carpirla;
- include cifre, lettere e caratteri speciali come: ':;£$(,.ç@&/!;
- non contiene il proprio nome o cognome, il soprannome, la data di nascita, il nome di persone familiari, parole comuni, nomi di paesi, animali e così via;
- non contiene parole che si trovano nei dizionari di qualsiasi lingua, anche se digitate al contrario, in quanto esistono software in grado di individuarle;
- non sono composte da semplici sequenze di tasti, come ad esempio "asdfghjkl", o da ripetizioni del proprio nome utente (ad es. se il proprio utente è rossi; la password "rossi rossi" sarà inopportuna);
- è composta con più parole contenenti errori ortografici o con sillabe combinate costituite da parole non correlate tra loro.

L'Utente si impegna a comunicare quanto prima al Coordinatore Informatico l'eventuale furto o smarrimento della propria password. In particolare, in caso di furto, l'Utente si impegna a modificare tempestivamente la password utilizzando le procedure automatiche a sua disposizione. In ogni caso, resta inteso che l'Utente sarà responsabile delle conseguenze derivanti dal furto, dalla perdita o dallo smarrimento di tale password.

Art. 11
Ceritificati digitali

Il certificato digitale, in generale è nominativo e strettamente personale. Per specifiche procedure può essere intestato alla Struttura. Occorre provvedere all'installazione del certificato digitale sul proprio "*profilo*" onde evitare che la propria identità venga utilizzata da parte di Terzi per l'accesso e la registrazione su procedure informatiche.

In caso di utilizzo di certificati digitali su postazioni di lavoro condivise, ove consentito, occorre attivarne la protezione mediante l'impostazione della password con le caratteristiche di "robustezza" sopra indicate.

L'Utente si impegna a comunicare quanto prima al Coordinatore Informatico l'eventuale furto o smarrimento del proprio certificato digitale.

Art. 12
Computer

Il computer è uno strumento di lavoro fornito dall'Ente e rappresenta una dotazione strumentale della sede ove è ubicato. Il suo eventuale utilizzo non inerente all'attività lavorativa è vietato perché può contribuire a innescare disservizi, costi di manutenzione e soprattutto, minacce alla sicurezza dell'intera infrastruttura tecnologica di E.R.S.U. Il computer può essere affidato a uso singolo o condiviso, sulla base della richiesta effettuata

dal Responsabile della Struttura e tenuto conto della prevalenza delle funzioni che devono essere espletate.

Il computer viene fornito con configurazione software predefinita che non può essere per alcun motivo modificata da parte dell'utente.

Le richieste di installazione di nuovo software o di modifica della configurazione devono essere approvate dalla Struttura di appartenenza e dal Coordinatore Informatico, che solo a seguito di tale accettazione provvederà ad effettuarle con l'ausilio del personale interno/esterno incaricato. L'utente non può modificare le impostazioni autonomamente.

Di conseguenza:

- non verranno forniti privilegi di "*amministratore*" a eccezione di specifiche e motivate esigenze avanzate formalmente da parte del Responsabile della Struttura interessata e dietro specifica autorizzazione rilasciata dal Coordinatore Informatico e/o dal Responsabile del C.E.D.;
- non è consentita l'installazione sul proprio PC di mezzi di comunicazione propri (come ad esempio modem e dispositivi bluetooth);
- non è consentito utilizzare strumenti software e/o hardware atti a intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici;
- non è consentito copiare sul proprio computer file contenuti in supporti magnetici, ottici e dispositivi USB non aventi alcuna attinenza con la propria prestazione lavorativa;
- il computer deve essere spento (ove possibile mediante scollegamento dalla presa elettrica) ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio o in caso di suo inutilizzo;
- occorre bloccare il computer o disconnettersi, in caso di postazioni condivise, qualora ci si allontani dalla propria postazione (per il sistema operativo WINDOWS premendo contemporaneamente i tasti Alt+Ctrl+Canc e cliccando su blocca computer o in alternativa attivando la protezione sul proprio screen saver);
- non è consentito utilizzare strumenti potenzialmente in grado di consentire accessi non autorizzati alle risorse informatiche (es.: programmi di condivisione quali IRC, ICQ, AudioGalaxy o software di monitoraggio della rete in genere);
- non è consentito configurare o utilizzare servizi diversi da quelli messi a disposizione da parte del Coordinatore Informatico e/o dal Responsabile del C.E.D. (quali DNS, DHCP, server internet (Web, FTP,…);
- non è consentito intercettare pacchetti sulla rete (sniffer) o software dedicati a carpire, in maniera invisibile, dati personali, password e ID dell'utente oppure a controllare ogni attività, ivi inclusa la corrispondenza e i dati personali;
- non è consentito impostare password nel bios;
- non è consentito disassemblare il computer, asportare, scollegare, aggiungere, spostare o semplicemente scambiare tra un PC e l'altro qualsiasi apparecchiatura in dotazione all'Utente salvo diretta e specifica indicazione del Coordinatore Informatico dell'Ente;
- non è consentito avviare il personal computer con sistemi operativi diversi da quello installato dal Coordinatore Informatico o da un suo incaricato, incluse versioni live;
- non è consentito utilizzare connessioni in remoto per l'accesso a risorse di E.R.S.U., al di fuori del perimetro dell'Ente e fatte salve le connessioni realizzate e autorizzate da parte del Coordinatore Informatico o da un suo incaricato.

Si rammenta che i dischi o le altre unità di memorizzazione locale (es. disco C:) non devono essere utilizzate per salvare documenti frutto dell'attività lavorativa e quindi non sono soggette a salvataggio da parte del Coordinatore Informatico o da un suo incaricato. Nel caso di altra tipologia di dati la responsabilità del salvataggio e dell'integrità dei dati ivi contenuti è pertanto a carico del singolo Utente.

In deroga a quanto sopra riportato, ed esclusivamente presso le sedi dell'Ente dove non vi sono server dedicati all'archiviazione dei dati o nell'impossibilità di utilizzare in modo efficiente lo spazio sui server remoti, l'archiviazione dei dati lavorativi potrà essere effettuata sul disco locale del personal computer affidato.

In questo caso, il backup dei dati deve essere effettuato a cura dell'utente, previa verifica tecnica preliminare effettuata da parte del Coordinatore Informatico o da un suo incaricato. tesa a individuare la soluzione tecnica più idonea (salvataggio su CD/DVD, pen drive o altri supporti esterni).

Art. 13
Computer dedicati ad attività specifiche

Il collegamento alla rete dell'Ente di computer dedicati ad attività specifiche, deve essere richiesto dal Responsabile della Struttura interessata al Coordinatore Informatico o ad un suo incaricato che provvederà alla verifica della fattibilità e della compatibilità tecnica del collegamento.

In caso di interventi di manutenzione effettuati da Ditte esterne su computer dedicati ad attività specifiche collegati alla rete dell'Ente, questi devono essere preventivamente valutati e concordati unitamente con il Coordinatore Informatico e/o dal Responsabile del C.E.D.

Eventuali installazioni di ulteriori programmi devono essere preventivamente assoggettate a verifica di compatibilità e autorizzazione da parte del Coordinatore Informatico o da un suo incaricato.

Al fine di poter permettere l'utilizzo condiviso di una singola risorsa da parte di più Utenti è consentita la creazione e l'uso di utenze generiche, la cui responsabilità e assegnazione è del Responsabile della Struttura. Le utenze generiche non possono effettuare trattamenti su dati personali.

L'esecuzione dei backup dei dati residenti sui computer dedicati ad attività specifiche deve essere effettuata a cura del personale della Struttura che ha in carico l'apparecchiatura, in particolare:

- computer in rete con salvataggio dei dati sul server: il backup viene eseguito automaticamente secondo le modalità definite dal Responsabile del C.E.D.;
- computer non in rete o in rete senza salvataggio dei dati sul server: il backup viene effettuato dal Responsabile del C.E.D. che ne valuta la modalità più idonea (salvataggio su CD/DVD, su pen drive e altri supporti esterni);
- computer che non permettono alcun tipo di backup: in questo caso il Responsabile del C.E.D., in collaborazione con la ditta esterna incaricata della manutenzione, valuteranno l'investimento tecnologico necessario per rendere il computer idoneo all'esecuzione del backup dei dati (schede USB, dismissione,…).

Art. 14
Computer portatili

L'Utente è responsabile dell'integrità del PC portatile affidatogli dal Responsabile della Struttura di appartenenza e dei dati ivi contenuti. L'Utente è tenuto a custodirlo con diligenza sia durante l'utilizzo nel luogo di lavoro sia durante i suoi spostamenti.

Ai PC portatili si applicano le regole di utilizzo previste per i personal computer. Nel caso di utilizzo comune con altri Utenti, prima della riconsegna occorre provvedere alla rimozione definitiva di eventuali file elaborati.

I dischi dovranno essere criptati al fine di evitare, in caso di furto o di smarrimento, l'accesso a dati riservati e/o personali da parte di soggetti non autorizzati.

Art. 15
Privilegi di amministrazione locale

Su specifica e motivata esigenza e richiesta rappresentata da parte del Responsabile della Struttura interessata al Coordinatore Informatico possono essere concessi a particolari utenti i privilegi di amministrazione locale della propria postazione di lavoro. Tali utenti saranno tenuti ad adottare le seguenti misure minime per mantenere inalterati gli attuali livelli di sicurezza informatica dei sistemi interessati e della rete dell'Ente:

- utilizzo di privilegi di amministrazione secondo la modalità e la regolamentazione prevista – Procedura Gestionale – Gestione della sicurezza dei dati e delle registrazioni;
- adozione e gestione di password definite, nella composizione e nella modalità di modifica, secondo la normativa vigente;
- tenere traccia, ove possibile, delle operazioni effettuate su appositi file di log in occasione di nuove installazioni;
- aderenza alle disposizioni riportate nel Documento Programmatico sulla Sicurezza adottato dall'Ente ai sensi del D. Lgs. 196/2003 Codice in materia di protezione dei dati personali e s.m.i.

In caso di particolari situazioni, opportunamente rappresentate e motivate al Coordinatore Informatico, ove per esigenze tecniche vi siano computer per i quali l'utilizzo di particolari programmi richieda la disponibilità dei privilegi di amministrazione sulla singola macchina, l'Utente è tenuto a:

- adottare regole e politiche per la configurazione di procedure e software di protezione concordate col Coordinatore Informatico dell'E.R.S.U.;
- aggiornare le procedure e i software di protezione con cadenza almeno mensile.

In caso di utilizzo e presenza di sistemi operativi o applicativi non gestiti o forniti da parte del Coordinatore Informatico o da un suo incaricato, non verrà fornita assistenza sulla parte software.

Art. 16
Stampanti

Per quanto concerne l'utilizzo delle stampanti, gli utenti sono tenuti a:

- stampare documenti e atti solo se strettamente necessari per lo svolgimento delle proprie funzioni lavorative;

- prediligere le stampanti di rete in luogo di quelle locali al fine di ridurre l'utilizzo di materiali di consumo (toner, cartucce,…);
- prediligere le stampanti laser in luogo di quelle che prevedono consumi maggiori, quali stampanti a getto di inchiostro;
- stampare in bianco/nero e fronte/retro al fine di ridurre i costi, laddove possibile.

Le stampanti locali devono essere spente ogni sera prima di lasciare gli uffici o in caso di loro inutilizzo.

Qualora il dipendente dovesse stampare documenti contenenti dati o informazioni riservate, dovrà aver cura di monitorare la stampante e preservare, limitatamente alle oggettive possibilità, la conoscibilità di tali dati o informazioni da parte di terzi non autorizzati.

Art. 17
Rete

In assenza di specifica autorizzazione da parte del Coordinatore Informatico o del Responsabile del C.E.D. non è consentito accedere ai locali e ai box riservati alle apparecchiature di rete.

Non è consentito collegare alle prese di rete apparecchiature non autorizzate da parte del Coordinatore Informatico o del Responsabile del C.E.D., quali: hub, switch, access point o altre componenti personali).

Non è inoltre consentito installare o utilizzare qualsiasi altra apparecchiatura atta a gestire comunicazioni, salvo specifica autorizzazione rilasciata dal Coordinatore Informatico o dal Responsabile del C.E.D., quali, a titolo esemplificativo: modem, router, Internet key, ecc.

Non è inoltre consentito effettuare spostamenti o modifiche di risorse collegate alla rete dell'Ente (es.: pc, stampanti, fotocopiatori e altro) senza una preventiva autorizzazione da parte del Coordinatore Informatico o del Responsabile del C.E.D.

Art. 18
Risorse di rete

Gli spazi delle unità di rete messi a disposizione, sono aree di condivisione e di archiviazione di informazioni strettamente lavorative e non possono pertanto essere utilizzate per la memorizzazione di file non attinenti ad attività lavorative.

In queste aree dovranno essere necessariamente salvati tutti i documenti lavorativi afferenti alla Struttura di appartenenza, al fine di renderli disponibili, in caso di necessità, agli altri utenti della Struttura.

Su queste unità vengono svolte regolari attività di controllo statistico, amministrazione, backup e restore da parte del Responsabile del C.E.D.

Gli accessi nelle unità di rete condivise devono essere autorizzati da parte del Responsabile del trattamento dei dati di pertinenza, il quale provvederà a richiedere al Responsabile del C.E.D., la creazione/rimozione dei diritti di accesso e a effettuare periodicamente la verifica delle abilitazioni attive.

Possono essere fornite ulteriori aree deputate allo scambio di file tra strutture diverse (es.: cartella *"common"*, file scannerizzati da scanner di rete). Onde evitare la saturazione di

questi spazi, cessato lo scopo contingente, i file salvati nelle aree comuni dovranno essere rimossi a cura dell'utente che li ha memorizzati, diversamente, verranno rimossi mediante la programmazione di apposite procedure di cancellazione automatica la cui frequenza verrà resa nota agli Utenti interessati.

Laddove consentito, sulla base della disponibilità di risorse, E.R.S.U. fornisce ad ogni utente una cartella ad accesso nominativo (home directory) al fine di poter archiviare documenti concernenti la propria vita lavorativa (ad esempio documenti, manuali, appunti,...) e per le quali non è dovuta la condivisione del contenuto con altri Utenti.

Le "home directory" hanno validità per tutta la durata della permanenza in servizio dello stesso dipendente titolare; hanno una dimensione predefinita e non estendibile.

In nessuna risorsa di rete è consentito salvare file audio, video, eseguibili e archivi di posta a eccezione di quelli strettamente attinenti a esigenze lavorative e dietro specifica e motivata richiesta da parte del Responsabile di Struttura. Per tali tipologie di file e archivi sono effettuati interventi di pulizia attivati d'ufficio da parte del Responsabile del C.E.D.; vengono inoltre definiti e attivati, a priori, filtri che ne vietano il loro salvataggio sui server dell'Ente.

L'accesso straordinario alla home directory nominativa da parte di un soggetto terzo, può avvenire esclusivamente previa autorizzazione da parte della Direzione e nei casi di prolungata assenza dal servizio o impedimento da parte del titolare della cartella che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema.

Art. 19
Internet

L'utilizzo della connessione Internet dell'Ente è consentita per i soli scopi lavorativi e nell'ambito delle mansioni affidate ai singoli lavoratori.

L'utilizzo degli strumenti dell'Ente può essere richiesto e concesso per svolgere attività che non rientrano tra i compiti istituzionali per assolvere incombenze amministrative e burocratiche senza allontanarsi dal luogo di lavoro (ad esempio per adempimenti nei confronti di pubbliche amministrazioni), purché contenuta nei tempi strettamente necessari allo svolgimento delle transazioni.

A titolo esemplificativo, non è consentito:
- l'upload o il download di software, di documenti o file di qualsiasi altra natura, se non strettamente attinenti all'attività lavorativa e previa verifica dell'attendibilità dei siti in questione;
- ogni forma di registrazione utilizzando riferimenti dell'Ente a siti i cui contenuti non siano strettamente legati all'attività lavorativa;
- la partecipazione a Forum non professionali, l'utilizzo di chat, di social network, di strumenti di condivisione, di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (nickname) se non espressamente autorizzati dal proprio Responsabile.

Al fine di prevenire, per quanto e ove possibile, comportamenti scorretti durante la navigazione in Internet, o per esigenze tecniche, l'Ente si avvale di appositi filtri

opportunamente configurati che impediscono l'accesso a siti non ritenuti idonei e che ne comunicano la motivazione dell'impedimento.

I filtri sopracitati limitano l'accesso ai siti Internet che presentano i seguenti contenuti:
- illegali o non etici, stupefacenti, razzismo e odio, estremismo, violenza, occultismo, plagio;
- materiale per adulti, nudità, pornografia;
- giochi, scommesse, intermediazione e trading, download software freeware;
- social network, radio e tv via Internet (salvo i casi espressamente autorizzati dalla Direzione);
- peer to peer;
- malware, spyware, hacking, bypass proxy, phishing;

Qualsiasi altra tipologia di contenuti o siti che la Direzione riterrà di non dover rendere accessibile dalla rete dell'Ente, verrà preventivamente comunicata agli utenti.

La navigazione, ovvero l'accesso ai siti Internet, potrebbe avvenire previa autenticazione dell'Utente sul proxy. I file contenenti le registrazioni della navigazione sul web sono conservati per il tempo strettamente necessario, determinato dalle norme in vigore e da esigenze di sicurezza.

Art. 20
Posta Elettronica

Il servizio di posta elettronica è un mezzo istituzionale di comunicazione dell'Ente e il suo utilizzo deve avvenire nel rispetto delle norme in materia di protezione dei dati personali.

Sono attribuiti indirizzi di posta elettronica:
- a strutture organizzative e per lo svolgimento di particolari funzioni (es: affari.generali@E.R.S.U..me.it - borsedistudio@E.R.S.U..me.it);
- a indirizzi nominativi (es: nome.cognome@E.R.S.U..me.it) assegnati individualmente ai dipendenti dell'Ente.

L'uso degli indirizzi di Struttura deve essere dedicato alle comunicazioni ufficiali sia interne che esterne all'Ente.

Non è consentito l'utilizzo dell'indirizzo di posta nominativo o di Struttura per scopi diversi da quelli prettamente lavorativi.

L'assegnazione di un indirizzo di posta elettronica avviene contestualmente all'assegnazione delle credenziali di autenticazione dell'Utente; di norma l'indirizzo di posta viene creato utilizzando il nome ed il cognome di quest'ultimo, associato al dominio istituzionale: @ersu.me.it. I casi di omonimia sono gestiti distintamente.

L'accesso al servizio di posta elettronica da parte di un Utente avviene mediante delle credenziali di autenticazione (nome utente e password).

Gli utenti assegnatari delle caselle di posta elettronica sono i diretti responsabili del corretto utilizzo delle stesse e rispondono personalmente dei contenuti trasmessi.

In particolare l'Utente è tenuto a rispettare quanto segue:
- non utilizzare il servizio per scopi illegali o non conformi al presente Regolamento o in maniera tale da recar danno o pregiudizio all'Ente o a terzi;

- non utilizzare il servizio in modo da danneggiare, disattivare, sovraccaricare, pregiudicare o interferire con la fruibilità del servizio da parte degli altri utenti.
- non utilizzare la posta elettronica per inviare, anche tramite collegamenti o allegati in qualsiasi formato (testo, fotografico, video, grafico, audio, codice, ecc.), messaggi che contengano o rimandino ad esempio a:
  - pubblicità non istituzionale, manifesta o occulta;
  - prodotti di natura politica;
  - comunicazioni commerciali private;
  - materiale pornografico o simile;
  - materiale discriminante o lesivo in relazione a razza, sesso, religione, ecc.;
  - materiale che violi la legge sulla privacy;
  - contenuti o materiali che violino i diritti di proprietà di terzi;
  - altri contenuti illegali.

In nessun caso l'Utente potrà utilizzare la posta elettronica per diffondere codici dannosi per i computer quali virus e simili.

Di seguito si elencano alcune norme di comportamento che ciascun Utente è tenuto ad osservare al fine di preservare l'efficienza del servizio di posta elettronica e delle comunicazioni con esso veicolate:
- l'Utente è tenuto a visionare regolarmente la casella di posta elettronica di propria competenza;
- i messaggi devono essere preferibilmente di solo testo, evitando ove possibile ogni formattazione e inserzione di immagini;
- è buona norma inviare messaggi sintetici che descrivano in modo chiaro il contenuto;
- è necessario indicare sempre chiaramente l'oggetto, in modo tale che il destinatario possa immediatamente individuare l'argomento del messaggio ricevuto, facilitandone la successiva ricerca per parola chiave;
- non superare la dimensione complessiva di 10 Megabyte degli allegati inviati con un singolo messaggio;
- limitare l'invio di messaggi di posta elettronica a indirizzi plurimi (decine di destinatari) e trasmetterli solo in casi motivati da esigenze di servizio.

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

Allo scopo di facilitare l'interscambio di informazioni relative a scopi istituzionali, è previsto l'uso delle liste di distribuzione (mailing list).

In linea di principio sarebbe da perseguire, per gli interscambi formali all'interno dell'Ente e verso l'esterno, l'uso delle liste di distribuzione di struttura. Occorre incentivare e favorire l'uso di tali liste evitando trasmissioni al singolo dipendente ma favorendo gli invii delle comunicazioni formali da indirizzi di struttura verso le liste delle strutture cui afferiscono i destinatari. Per facilitare lo scambio di informazioni funzionali alle attività svolte, è possibile far attivare più liste all'interno della stessa Struttura che rispecchino particolari funzioni: la soluzione deve essere funzionale all'organizzazione delle Strutture ed all'ottimizzazione della comunicazione interna e per questo, quindi, deve rispondere a principi di semplificazione.

Al fine di non duplicare le comunicazioni è opportuno che una comunicazione e-mail inviata ad una lista di distribuzione non venga anche contemporaneamente inviata all'indirizzo individuale.

La richiesta di attivazione di una lista di distribuzione (es: account di Struttura, di progetto o di una particolare attività o funzione condivisa), deve essere avanzata da parte di un Responsabile (di Struttura, di progetto o di funzione) e contenere l'elenco dei nominativi che devono essere inseriti nella relativa lista di distribuzione.

Il Responsabile sopracitato è tenuto a verificare, almeno annualmente, la necessità di mantenere attive le liste di distribuzione a lui afferenti e l'elenco dei nominativi abilitati.

Questi indirizzi potranno essere utilizzati nelle pubblicazioni cartacee a carattere informativo realizzate dall'Ente e pubblicate sul portale Internet dell'Ente.

Una lista generale di distribuzione comprendente tutti gli utenti, è gestita centralmente da parte degli amministratori di posta. L'utilizzo di questa lista è consentito a particolari Strutture appositamente autorizzate da parte della Direzione.

Alle Rappresentanze sindacali interne è assegnata apposita casella di posta elettronica con denominazione indicata dalle stesse. Tra i rappresentanti sindacali, viene formalmente individuato il responsabile della casella sia in termini di utilizzo che di gestione.

Le caselle di posta hanno una dimensione predefinita e non estendibile, occorre pertanto mantenere in ordine la propria casella di posta provvedendo a ripulirla con regolarità e salvando gli allegati ingombranti.

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'Ente eventualmente affiancandoli a quelli individuali.

In caso di assenza prolungata programmata del dipendente, 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 dell'Ente presso cui presta la propria attività lavorativa.

Nell'ipotesi di assenza o impossibilità, temporanea o protratta nel tempo, del dipendente, qualora per ragioni di sicurezza o comunque per garantire l'ordinaria operatività dell'Ente sia necessario accedere a informazioni o documenti di lavoro presenti sul personal computer del dipendente, inclusi i messaggi di posta elettronica in entrata ed in uscita, il dipendente può delegare un altro dipendente a sua scelta (fiduciario) il compito di verificare il contenuto di messaggi e inoltrare al responsabile della Struttura in cui lavora quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. Di tale attività deve essere redatto apposito verbale e informato sia il Coordinatore Informatico che il dipendente interessato alla prima occasione utile.

In caso di assenza o impossibilità, temporanea o protratta nel tempo, del dipendente, qualora per ragioni di sicurezza o comunque per garantire l'ordinaria operatività dell'Ente sia necessario accedere a informazioni o documenti di lavoro presenti sul personal computer del dipendente, inclusi i messaggi di posta elettronica in entrata e in uscita, e il dipendente non abbia delegato un altro dipendente (fiduciario), secondo quanto sopra

specificato, il responsabile della struttura cui afferisce il dipendente può chiedere al Coordinatore Informatico o 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 deve informare il dipendente appena possibile, fornendo adeguata spiegazione e redigendo apposito verbale.

Le caselle di posta individuali hanno validità pari alla durata della permanenza in servizio del dipendente, fatte salve eventuali situazioni di congedo, distacco e comando. Nel caso il cui il dipendente non presti più la sua attività lavorativa presso E.R.S.U., la casella di posta elettronica sarà prontamente disattivata. Su richiesta dell'interessato al Coordinatore Informatico, la casella di posta potrà restare attiva per ulteriori 3 mesi dalla data di cessazione del rapporto di lavoro, durante il quale sarà inserita una risposta automatica d'ufficio.

Se per esigenze lavorative sorge 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 al Coordinatore Informatico o all'Amministratore di Sistema.

Art. 21
Creazione di programmi o documenti automatizzati

In caso di creazione di software e altre procedure informatiche da parte di Strutture dell'Ente o commissionati a soggetti terzi, devono essere resi disponibili all'Ente:

- l'accesso al codice sorgente e alle base dati;
- l'analisi e la documentazione sul funzionamento e l'installazione;
- i metadati sulle strutture dati, eventualmente implementate.

La proprietà di quanto sopra, inclusi i diritti derivanti, sono dell'Ente salvo il diritto di essere riconosciuto autore dell'invenzione (*Titolo IX del Libro Quinto del Codice Civile, D.Lgs. 518 del 29.12.1992 che novella la legge 633/41*).

Art. 22
Creazione di programmi o documenti automatizzati

Tutto il software in uso nel sistema informativo dell'Ente in cui sia prevista una licenza d'uso deve essere registrato a nome dell'E.R.S.U.

Tutto il software deve essere individuato dall'Area Funzionale competente in materia, anche dietro suggerimento da parte delle Strutture dell'Ente.

Non è possibile installare, duplicare o utilizzare software acquisiti al di fuori di quanto consentito dagli accordi di licenza.

Tutti gli utenti sono tenuti al rispetto delle leggi in materia di tutela della proprietà intellettuale, sia per quanto riguarda il software che per quanto riguarda i file di qualsiasi altra natura.

Art. 23
Crittografia e controllo dei dati informatici

Fatto salvo quanto previsto dal D.Lgs. 196/2003 e s.m.i in materia di archiviazione, gestione, trattamento e trasmissione di dati sensibili, è fatto divieto di applicare sistemi di crittografia dati, se non espressamente richiesto e/o autorizzato dal Coordinatore Informatico o dal Responsabile del C.E.D.

Art. 24
Utilizzo e conservazione dei supporti rimovibili

Tutti i supporti di memorizzazione rimovibili (dischetti, hard disk esterni, CD e DVD riscrivibili, supporti USB, ecc.), contenenti dati sensibili nonché informazioni costituenti know-how dell'Ente, devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto o, recuperato successivamente alla cancellazione.

In ogni caso, i supporti contenenti dati sensibili devono essere adeguatamente custoditi, possibilmente in cassetti e armadi provvisti di chiusura. A tal proposito si ricorda che l'utente è responsabile non solo della custodia dei supporti ma anche dei dati dell'Ente in essi contenuti.

Nel caso di utilizzo condiviso dei medesimi supporti da parte di più utenti, occorre provvedere alla cancellazione delle informazioni ivi contenute mediante programmi formattazioni a basso livello.

Nel caso di smaltimento, i supporti dovranno essere precedentemente distrutti mediante punzonatura o deformazione meccanica o distruzione fisica o demagnetizzazione.

Art. 25
Protezione antivirus

Il sistema informatico e i pc collegati alla rete dell'E.R.S.U. sono protetti da software antivirus aggiornati quotidianamente.

Ogni Utente è comunque tenuto a comportarsi in modo tale da ridurre il rischio di attacco al sistema informatico dell'Ente da parte di virus o attraverso qualsiasi altro software "aggressivo". Medesime condizioni dovranno essere rispettate da parte di Soggetti terzi fornitori/gestori di apparecchiature e servizi informatici che vengono utilizzati a qualsiasi titolo all'interno della rete dell'Ente.

Art. 26
Fax

Questo Ente da tempo privilegia l'utilizzo del fax server in luogo del fax tradizionale favorendo l'uso adesso più diffuso dell'invio di allegati alle e-mail.

Non è consentito installare apparati fax tradizionali o software di gestione fax diversi da quelli forniti dal Responsabile del C.E.D. e previa autorizzazione e supporto da parte di questo.

Si raccomanda di non lasciare documenti incustoditi negli apparati tradizionali e nelle stampanti dedicate.

Art. 27
Teleassistenza

Per lo svolgimento di normali attività di manutenzione su personal computer connessi alla rete, il Coordinatore Informatico o il Responsabile del C.E.D. potranno utilizzare specifici software di connessione remota. Tali programmi vengono utilizzati per assistere l'utente al fine di effettuare interventi di assistenza informatica e di manutenzione su applicativi e hardware in uso presso l'Utente. L'attività di assistenza e manutenzione avviene previa autorizzazione da parte dell'utente interessato e possibilmente mediante visualizzazione di un indicatore visivo sul monitor dell'utente che segnala la connessione in remoto del tecnico.

Art. 28
Monitoraggio

E.R.S.U. adotterà ogni accorgimento tecnico necessario a tutelare l'Ente da eventuali comportamenti non consentiti, salvaguardando il rispetto della libertà e della dignità dei lavoratori; gli eventuali trattamenti effettuati saranno ispirati a canoni di trasparenza e rispetteranno il principio di pertinenza e non eccedenza.

La Direzione, attraverso il Responsabile del C.E.D., effettua monitoraggi periodici su dati anonimi allo scopo di verificare l'attuazione del presente Regolamento, i possibili rischi alla sicurezza informatica e le possibili problematiche inerenti l'utilizzo degli strumenti informatici.

Questi monitoraggi si possono classificare in:
- analisi del traffico di rete: effettuati attraverso specifici log dei dispositivi di rete;
- analisi del traffico Internet: effettuati attraverso specifici log dei dispositivi di connessione ad Internet;
- inventario Hardware e Software: effettuati attraverso procedure prevalentemente automatiche per le apparecchiature collegate in rete e in maniera semiautomatica per le macchine non appartenenti al dominio.

Il monitoraggio delle risorse hardware e software non coinvolge in alcun modo i dati personali e i documenti presenti sulle singole postazioni di lavoro e viene effettuato per finalità organizzative e gestionali.

I dati del traffico telematico verranno gestiti secondo le modalità e le tempistiche previste dalla normativa vigente in materia di sicurezza dei dati del traffico telefonico e telematico.

L'Ente si riserva la facoltà di procedere alla rimozione di ogni file o applicazione che riterrà pericolosa per la sicurezza del sistema informatico ovvero acquisita o installata in violazione del presente Regolamento.

Art. 29
Controlli

L'E.R.S.U. si riserva di effettuare controlli per verificare il rispetto del Regolamento.

Riguardo a tali controlli il presente Regolamento costituisce preventiva e completa informazione nei confronti dei dipendenti.

In base al principio di correttezza (*richiamato nell'art. 5*), l'eventuale trattamento deve essere ispirato ad un canone di trasparenza, come prevede anche la disciplina di settore (*art. 4, secondo comma, Statuto dei lavoratori*).

I dati devono essere gestiti soltanto dai soggetti preventivamente designati quali responsabili e incaricati del trattamento (*art. 30 del codice in materia di protezione dei dati personali*).

Nel caso in cui emerga un evento dannoso, una situazione di pericolo o utilizzi non aderenti al presente Regolamento, che non siano stati impediti con preventivi accorgimenti tecnici o rilevati durante i monitoraggi o da attività di gestione degli strumenti informatici, la Direzione, attraverso il Coordinatore Informatico o il Responsabile del C.E.D., potrà adottare le eventuali misure che consentano la verifica di tali comportamenti preferendo, per quanto possibile, un controllo preliminare su dati aggregati riferiti all'intera Struttura organizzativa o a sue articolazioni.

Il controllo su dati anonimi si concluderà con una comunicazione al Responsabile della Struttura analizzata che si preoccuperà di inviare un avviso generalizzato relativo a un utilizzo non corretto degli strumenti dell'Ente, invitando i destinatari ad attenersi scrupolosamente al presente Regolamento.

Qualora le anomalie e irregolarità dovessero persistere, si procederà circoscrivendo l'invito al personale afferente alla Struttura in cui è stata rilevata l'anomalia.

In caso di reiterate anomalie o irregolarità, saranno effettuati controlli su base individuale.

In nessun caso, a eccezione di specifica richiesta da parte dell'Autorità Giudiziaria, verranno poste in essere azioni sistematiche quali:

- la lettura e la registrazione dei messaggi di posta elettronica (al di là di quanto tecnicamente necessario per lo svolgimento del servizio di gestione e manutenzione della posta elettronica);
- la riproduzione ed eventuale memorizzazione delle pagine web visualizzate dal lavoratore;
- la memorizzazione di quanto visualizzato sul monitor.

Oltre a ciò l'E.R.S.U. si riserva di effettuare specifici controlli sui software caricati sui personal computer utilizzati dai dipendenti 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.

Oltre a tali controlli di carattere generale, l'E.R.S.U. si riserva comunque le facoltà previste dalla normativa vigente di effettuare specifici controlli *ad hoc* nel caso di segnalazioni di attività che hanno causato danno all'amministrazione, che ledono diritti di terzi o che, comunque, sono illegittime.

Art. 30

Sanzioni

È fatto obbligo a tutti gli utenti di osservare le disposizioni contenute nel presente Regolamento.

Il mancato rispetto o la violazione delle indicazioni ivi contenute è perseguibile nei confronti del personale dipendente con provvedimenti disciplinari e risarcitori previsti dal vigente CCRL, nonché con le azioni civili e penali conseguenti previste dalla normativa vigente in materia.

Ogni dipendente dovrà assumersi la piena responsabilità per le proprie azioni e dovrà farsi garante per l'Ente e tenerla indenne da responsabilità e richieste di rimborsi di danni, avanzate da soggetti terzi.

Con riferimento ai collaboratori e/o prestatori d'opera, qualora questi per l'espletamento del loro incarico si servissero degli strumenti dell'Ente considerati dal Regolamento, deve essere previsto nell'ambito del contratto l'obbligo di rispettare il presente Regolamento, con diritto di E.R.S.U., nei casi di violazione di particolare gravità, di risolvere il contratto stesso.