Politica per la sicurezza e l'utilizzo degli strumenti informatici

Approvato con Determina dell'Amministratore Unico
del 14/06/2018 nr. 27

Documento	**IOPD 02-003**	**Politica per la sicurezza e l'utilizzo degli strumenti informatici**

Revisione 02 del 21/05/2018

ARCA Jonica
(Agenzia Regionale per la Casa e l'Abitare di Taranto)
Via Pitagora, 144 - TARANTO - P.IVA: 00091580738
Centralino Tel. 099.45.39.411 - Fax 099. 45.35.992
PEO: info@arcajonica.gov.it - PEC: arcajonica@pec.it

Premessa

Le informazioni sono un bene che hanno un valore per **ARCA JONICA Taranto** e, di conseguenza, necessitano di essere protette adeguatamente.

La sicurezza delle informazioni protegge le informazioni stesse da un'ampia gamma di minacce per assicurare la continuità dell'attività commerciale, per minimizzare il danno commerciale e per massimizzare il ritorno degli investimenti e delle opportunità commerciali.

Le informazioni possono essere presenti in molte forme. Possono essere stampate o scritte su carta, memorizzate elettronicamente, trasmesse per posta o utilizzando altri mezzi elettronici, visualizzate su pellicole o trasmesse in una conversazione. Qualunque forma abbiano le informazioni o qualunque sia il mezzo su cui è condivisa o memorizzata una informazione, questa dovrebbe essere sempre protetta adeguatamente.

La sicurezza delle informazioni è definita qui come il mantenimento della:

a) **riservatezza**: l'assicurazione che le informazioni siano accessibili solo a coloro che sono autorizzati ad avere l'accesso;

b) **integrità**: salvaguardare la precisione e la completezza dell'informazione e del metodo di elaborazione;

c) **disponibilità**: l'assicurazione che gli utenti autorizzati abbiano accesso alle informazioni e ai beni quando richiesto.

La sicurezza delle informazioni è ottenuta realizzando un insieme adatto di controlli, che potrebbero essere criteri, pratiche, procedure, strutture organizzative e funzioni software.

L'utilizzo delle risorse informatiche e telematiche deve sempre ispirarsi, in applicazione di quanto disposto dagli artt. 2104 e 2015 c.c., al principio della diligenza, fedeltà e correttezza, comportamenti che normalmente si adottano nell'ambito dei rapporti di lavoro, adottando, quindi, 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.

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

L'Ente adotta un Regolamento interno diretto ad evitare che comportamenti inconsapevoli possano innescare problemi alla gestione della rete informatica aziendale e/o minacce alla sicurezza nel trattamento dei dati personali di qualsivoglia tipo (personale, sensibile e giudiziario) e per richiamare le indicazioni e le misure necessarie ed opportune per il corretto utilizzo, nel rapporto di lavoro, dei personal computer (fissi e portatili), dei dispositivi elettronici aziendali in genere, della posta elettronica e di Internet, definendone le modalità di utilizzo nell'ambito dell'attività lavorativa.

La progressiva diffusione delle nuove tecnologie informatiche ed, in particolare, il libero accesso alla rete Internet dai personal computer, espone la rete dell'Ente a rischi di natura patrimoniale, oltre alle responsabilità penali conseguenti alla violazione di specifiche disposizioni di legge, creando evidenti problemi alla sicurezza all'immagine di questo Ente. Pertanto le prescrizioni di seguito previste si aggiungono ed integrano le specifiche istruzioni fornite a tutti i responsabili ed Incaricati del trattamento dei dati personali in attuazione del Regolamento Europeo UE 2016/679.

L'Ente necessita di garantire un servizio continuativo, nel suo stesso interesse, ed 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.

Scopo della procedura

La presente procedura ha lo scopo di fornire indicazioni per l'utilizzo sicuro ed appropriato delle risorse informatiche (hardware, software, Internet, posta elettronica) date in uso al personale.

La Procedura si prefigge lo scopo di una gestione controllata, efficace, efficiente e conforme alla normativa tramite:

- l'informazione/formazione di tutto il personale aziendale coinvolto;
- la applicazione del presente regolamento;
- il monitoraggio del rispetto delle norme impartite con il seguente documento;
- la valutazione del grado di applicazione del presente regolamento, e la applicazione di opportuni interventi correttivi, sia tecnologici che sanzionatori.

Infine questo regolamento viene adottato alla luce del Provvedimento a carattere generale emesso Garante per la protezione dei dati personali il 1° marzo 2007, relativo all'utilizzo della posta elettronica e della rete Internet nel rapporto di lavoro.

Campo di applicazione

Le disposizioni contenute nella presente Procedura devono essere adottate e rigorosamente osservate all'interno dell'Ente da tutto il personale dipendente, al fine di evitare infrazioni alle leggi vigenti.

Le modalità operative devono essere applicate all'interno di ogni singolo contesto organizzativo.

La responsabilità relativa alla vigilanza e all'informazione del personale è attribuita ai responsabili di funzione presenti all'interno dell'Ente.

Il presente Regolamento si applica a tutti i dipendenti, senza distinzione di ruolo o livello, nonché a tutti i collaboratori di qualsiasi tipo; la applicazione, quindi, è estesa a chiunque operi su un sistema informatico all'interno del comprensorio sede dell'Ente o connesso con esso, a prescindere dal tipo di rapporto contrattuale con lo stesso intrattenuto (consulenti, tirocinanti, borsisti, volontari, ditte esterne autorizzate, ecc.), e dalla esistenza o meno di una remunerazione del medesimo Vale, al riguardo, la definizione fornita dal comma 1. a dell'art. 2 del D.Lgs. 81/2008.

Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche e telematiche, per "utente" deve intendersi ogni soggetto, in possesso di specifiche credenziali di autenticazione, operante su computeir in rete aziendale. Tale figura si configura quale "Soggetto autorizzato del trattamento". La presente politica contiene le disposizioni relative alle corrette modalità di utilizzo della rete informatica dell'Ente e di tutte le risorse aziendali, in conformità e nel rispetto di quanto previsto dalla specifica normativa di settore e dalle ulteriori disposizioni emanate.

Gli strumenti informatici oggetto della presente politica sono in uso nell'Ente (in proprietà, noleggio, service, comodato o qualsiasi altra forma contrattuale) e sono messi a disposizione degli Utenti al fine di permettere il quotidiano svolgimento delle proprie prestazioni lavorative.

Essi sono essenzialmente individuabili quali:

- Servers; computer, fissi o mobili; tablet e altri apparati mobili; sistemi di identificazione e di autenticazione informatica; smartphone concessi in uso dalla azienda;
- Internet, intranet e altri strumenti di scambio di comunicazioni e file, compresi quelli delocalizzati con tecnologia cloud; apparecchiature informatiche necessarie per l'uso di internet o intranet
- posta elettronica
- qualsiasi altro programma e apparecchiatura informatica destinata a memorizzare o a trasmettere dati e informazioni.

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

Per qualsiasi dubbio relativo all'applicazione pratica ed all'interpretazione autentica delle disposizioni contenute nel presente Regolamento, è possibile rivolgersi al Responsabile dei servizi informatici.

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

Per Amministratore di Sistema si intende il soggetto cui è conferito il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di base dati e di consentirne l'utilizzazione.

Devono essere nominati Amministratori di Sistema tutti coloro che, nell'espletamento delle loro consuete attività tecniche, sono "responsabili" di fasi lavorative che possono comportare elevate criticità rispetto alla protezione dei dati, quali:

- gestione dei sistemi di autenticazione e di autorizzazione;
- custodia delle credenziali di autenticazione e di autorizzazione;
- salvataggio dei dati (backup/recovery);
- organizzazione dei flussi di rete;
- gestione dei supporti di memorizzazione;
- manutenzione hardware.

Possono dunque qualificarsi quale Amministratori di sistema i seguenti soggetti:

- amministratori di sistemi di autenticazione e di autorizzazione;
- amministratori di server e pc;
- amministratori di apparati di rete;
- amministratori di base di dati;
- amministratori di apparati di sicurezza;
- amministratori di applicazioni.

Nel caso di servizi di amministrazione di sistema affidati in outsourcing, quale Responsabile esterno del Trattamento, l'Ente dovrà impegnarsi a conservare direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema.

Qualora l'attività degli amministratori di sistema riguardi servizi o sistemi che trattano informazioni di carattere personale di dipendenti, l'Ente è tenuta a rendere nota o conoscibile l'identità degli Amministratori di sistema nell'ambito della propria organizzazione.

Regole per l'utilizzo degli strumenti informatici

1. Utilizzo del personal computer

|| personal computer (fisso, mobile) affidato all'Utente è uno strumento di lavoro. Ogni utilizzo non inerente all'attività lavorativa **è vietato** perché può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. Il Pc deve essere custodito con cura evitando ogni possibile forma di danneggiamento.

Il personal computer dato in affidamento all'utente permette l'accesso alla rete aziendale solo attraverso specifiche credenziali di accesso ed autenticazione.

L'Ente rende noto che l'attuale ditta esterna affidataria del servizio di assistenza e manutenzione della rete informatica, nella qualità di Responsabile esterno del trattamento e nella fattispecie in qualità di Amministratore di Sistema, è autorizzato a compiere interventi nel sistema informatico, diretti a garantire lla sicurezza e la salvaguardia del sistema stesso, nonché per ulteriori motivi tecnici e/o manutentivi.

Detti interventi potranno anche comportare in qualunque momento, e anche in assenza dell'affidatario, come normato di seguito, l'accesso agli strumenti hardware e di conseguenza anche ai dati trattati da ciascuno, ivi compresi gli archivi su Pc e Server, nonché alla verifica sui siti internet acceduti dagli utenti abilitati.

La stessa facoltà, sempre ai fini della sicurezza del sistema e per garantire la normale operatività dell'Ente si applica anche in caso di assenza prolungata od impedimento del dipendente.

La ditta esterna di cui sopra ha la facoltà di collegarsi, di norma previa autorizzazione dell'Utente, e visualizzate in remoto il desktop delle singole postazioni PC al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza contro virus informatici in genere. L'intervento di norma viene effettuato esclusivamente su chiamata dell'utente ma, in caso di oggettiva necessità, ad esempio a seguito della rilevazione tecnica di problemi nel sistema informatico e telematico la cui risoluzione richieda l'accesso ai sistemi affidati al dipendente assente, l'intervento sarà comunque erogato. In quest'ultimo caso, e sempre fatta salva la necessaria tempestività ed efficacia dell'intervento, verrà data formale comunicazione via e-mail della necessità dell'intervento stesso o dell'avvenuto intervento.

Il personal 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 inviate ai tecnici esterni incaricati alla gestione dei servizi informatici. L'utente non può modificare le impostazioni del Pc autonomamente.

Di conseguenza:

1) non saranno forniti privilegi di "amministratore" ad eccezione di specifiche e motivate esigenze avanzate formalmente da parte del Responsabile della Struttura interessata e dietro specifica autorizzazione rilasciata dal Titolare, **previa richiesta al Responsabile dei servizi informatici**;
2) non è consentita l'installazione di mezzi di comunicazione personali (come ad esempio modem e dispositivi bluetooth, smartphone, chiavette per l'accesso ad internet etc.);
3) non e consentito utilizzare strumenti software e/o hardware non autorizzati dal Titolare, previa richiesta al Responsabile dei servizi informatici;
4) in particolare, non è consentito utilizzare strumenti software e/o hardware atti a intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici;
5) 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;
6) Il computer deve essere spento ogni sera prima di lasciare gli uffici nonché in caso di assenze prolungate dall'ufficio o in caso di suo inutilizzo;
7) non è consentito concedere ad alcuno l'utilizzo del proprio computer;
8) non è consentito lasciare un elaboratore incustodito acceso o non bloccato, soprattutto se connesso alla rete; ciò infatti potrebbe permettere l'utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso. Di conseguenza, qualora ci si allontani dalla propria postazione, occorre bloccare il computer (attivare la schermata di protezione) o disconnettersi (per il sistema operativo windows premendo contemporaneamente i tasti Alt+Ctrl+Canc e cliccando su blocca computer);
9) non è consentito utilizzare strumenti potenzialmente in grado di consentire accessi non autorizzati alle risorse informatiche (es: programmi di condivisione quali IRC, ICQ, o software di monitoraggio della rete in genere);
10) non è consentito configurare o utilizzare servizi diversi da quelli messi a disposizione da parte dell'Ente (quali DNS, DHCP, server internet Web, FTP, ...);
11) 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;
12) non è consentito impostare password nel bios; non è consentito modificare le impostazioni IP;
13) non è consentito spostare la posizione del computer senza intervento del personale tecnico autorizzato dal Responsabile dei servizi informatici (o tecnici esterni incaricati alla gestione dei servizi informatici);
14) non è consentito lo scambio di computer o di parti di esso (comprese le periferiche) tra utenti senza intervento del personale tecnico autorizzato dal **Responsabile dei servizi informatici di concerto con i tecnici esterni incaricati alla gestione dei servizi informatici**;
15) 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 personale tecnico dell'Ente;
16) non è consentito avviare il personal computer con sistemi operativi diversi da quello installato dal personale autorizzato;
17) non è consentito utilizzare connessioni in remoto per l'accesso alle risorse aziendali, al di fuori del perimetro aziendale e fatte salve le connessioni realizzate e autorizzate da parte del Titolare, previa richiesta al Responsabile dei servizi informatici;
18) salvo preventiva espressa formale autorizzazione del Responsabile dei servizi informatici di concerto con i tecnici esterni incaricati alla gestione dei servizi informatici non è consentito l'uso di programmi

diversi da quelli ufficialmente installati, né viene consentito agli utenti di installare autonomamente programmi provenienti dall'esterno o scaricati da internet, sussistendo infatti il grave pericolo di introdurre virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti. E' vietato installare il software scaricato da Internet o contenuto nei vari supporti distribuiti con le riviste, con i libri e con i quotidiani, anche se si tratta di software allegato a riviste del settore. Prima di installare questi programmi, qualora l'uso fosse collegato ad esigenze lavorative, sarà necessario il benestare del Titolare, previa richiesta al Responsabile dei servizi informatici di concerto con i tecnici esterni incaricati alla gestione dei servizi informatici. L'inosservanza della presente disposizione espone l'Ente a gravi responsabilità civili; si evidenzia inoltre, che le violazioni della normativa a tutela dei diritti d'autore sul software, che impone la presenza nel sistema di software regolarmente licenziato o comunque libero e quindi non protetto dal diritto d'autore, sono sanzionabili anche penalmente;

19) ogni Utente deve prestare la massima attenzione ai supporti di origine esterna, sottoponendoli sempre a scansione antivirus ed avvertendo immediatamente il personale tecnico preposto nel caso in cui siano rilevati virus di qualsivoglia natura;
20) in conseguenza del precedente punto, non è consentito copiare sul proprio computer file contenuti in supporti magnetici, ottici e dispositivi usb non forniti dell'Ente (e quindi non verificati dal punto di vista della possibile presenza di virus); eventuali eccezioni possono essere consentite solo previa verifica della integrità del supporto da parte dei tecnici dell'Ente;
21) non è consentito collegare alla rete informatica Personal Computer o Pc Portatili e, più in generale, qualsiasi dispositivo hardware non ascrivibili alla proprietà o altra forma di possesso dell'Ente, salvo specifica autorizzazione del Titolare, previa richiesta al **Responsabile dei servizi informatici**.
22) E' consentito l'uso di tecniche di cifratura dei dati trattati, solo se necessario, ed esclusivamente mediante software distribuiti dall'Ente. **Copia della chiave di decodifica (chiave privata,….) deve essere consegnata, in busta chiusa, al Responsabile dei servizi informatici**.

2. Hardware e Software

Tutto l'hardware ed il software potrà essere acquistato solo previa richiesta di parere tecnico favorevole da parte del Titolare, previa richiesta al Responsabile dei servizi informatici, che controllerà le richieste di acquisto al fine di valutarne la compatibilità e programmare l'applicazione delle misure di sicurezza informatica aziendali.

A tal fine le richieste di acquisto dell'hardware e del software dovranno essere indirizzate al Responsabile dei servizi informatici per la verifica tecnica di compatibilità o per la proposizione di soluzioni alternative. I supporti originali dei software acquistati e le relative licenze **devono essere conservati presso l'Ufficio del Responsabile dei servizi informatici**, così da consentire le operazioni di verifica della disponibilità di licenze e l'eventuale reinstallazione delle procedure.

Il software per elaboratori è considerato opera di ingegno e come tale è tutelato dalle Leggi sul diritto di autore. L'utilizzo del software è regolamentato da licenze d' uso che devono essere assolutamente rispettate da tutti. (Dlgs. 518/92 sulla tutela giuridica del software e L 248/2000 "nuove norme di tutela del diritto d'autore").

3. Backup dei dati

L'esecuzione dei backup dei dati residenti sul computer deve essere effettuata a cura del personale del services esterno, in particolare come di seguito specificato:

- computer in rete con salvataggio automatico dei dati sul server: Il backup viene eseguito automaticamente secondo le modalità definite dal Responsabile dell'Area Gestione Tecnica e Servizi Informativi;
- computer non in rete o in rete senza salvataggio automatico dei dati sul server. il backup viene effettuato dal personale che ha in carico il PC previa verifica preliminare da parte del Responsabile dei servizi informatici che ne valuta la modalità più idonea (salvataggio su CD/DVD su pen drive e altri supporti esterni), ai fini di garantire la maggiore sicurezza dei dati, *Responsabile dei servizi informatici ha predisposto spazi di archiviazione in remoto su server, raggiungibili sia via rete che via*

cloud (n.b. al momento il backup su cloud non è stato organizzato). E' cura dei responsabili della gestione dei dati attivare l' uso di tali spazi di archiviazione e l'aggiornamento periodico dei backup degli archivi;

- computer che non permettono alcun tipo di backup: in questo caso il Responsabile dei servizi informatici, in collaborazione con la ditta esterna incaricata della manutenzione, valuterà l'investimento tecnologico necessario per rendere il computer idoneo all'esecuzione del backup dei dati.

4. Computer portatili e tablet

L' Utente è responsabile dell'integrità del computer portatile/tablet affidatogli dall'Ente 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. A tali dispositivi si applicano le regole di utilizzo previste per i personal computer Nel caso di utilizzo condiviso con altri Utenti, prima della riconsegna occorre provvedere alla rimozione definitiva di eventuali file elaborati. I dischi rigidi, se contenenti dati sensibili, 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. Tutti i dispositivi portatili dovranno essere resi noti al Responsabile dei servizi informatici che provvederà all'applicazione di tutte le misure di sicurezza previste da disciplinare interno e dalla normativa vigente.

5. Stampanti e fotocopiatori

Per quanto concerne l'utilizzo delle stampanti, l'Utente è tenuto a osservare le seguenti disposizioni:

- stampare documenti e atti solo se la stampa è strettamente indispensabile, ovvero se oggettive motivazioni rendono impossibile la prosecuzione della attività lavorativa con mezzi diversi (es. consultando i documenti a schermo, condividendoli via rete, eccetera);
- in ogni caso, ogni utente é responsabile del fatto che la stampa, ove necessaria, riguardi comunque documenti strettamente necessari per lo svolgimento delle proprie funzioni lavorative; si ricorda che la stampa con mezzi dell'Ente di documenti/pubblicazioni personali costituisce reato penale;
- ogni utente è tenuto a 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;
- osservare in generale tutte le precauzioni finalizzate a conseguire il massimo contenimento dei costi; in tal senso, ad esempio: è vietato stampare documenti a colori senza una specifica necessità operativa; non è considerata "necessità operativa" la semplice qualità estetica dei documenti (compresa la carta da lettera); in ogni caso, laddove la stampa a colori sia necessaria (ad esempio per elaborazione di grafici), si eviterà il colore in tutte le versioni di bozza del documento, riservando tale tipologia di stampa solo nella versione definitiva; si prediligerà la stampa fronte/retro, laddove possibile; si useranno le impostazioni di stampa "economy" in tutte le versioni "in progress" dei documenti; si imposterà la qualità di stampa senza eccessi non giustificabili; eccetera

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.

E' fatto divieto di lasciare documenti incustoditi nei fax, nei fotocopiatori e nelle stampanti condivise.

6. Credenziali di accesso e gestione della password (parola chiave)

I sistemi di controllo degli accessi in rete informatica assolvono il compito di prevenire che persone non autorizzate possano accedere a un sistema informatico ed 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.

Ad ogni Utente "incaricato" sono assegnate o associate individualmente una o più credenziali per l'autenticazione (identificativo e password) necessarie per accedere alle risorse informatiche e alle

applicazioni software; l'incaricato deve adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo.

Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi. Le credenziali di autenticazione devono essere disattivate:

- se non utilizzate da almeno sei mesi, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica;
- in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.

Le credenziali di autenticazione nell'intranet (accesso rete aziendale), vengono inizialmente assegnate dal Responsabile dei servizi informatici, per il tramite del services esterno incaricato, e successivamente obbligatoriamente reimpostate dal dipendente stesso secondo criteri prestabiliti dalla normativa vigente e con modalità operative di seguito meglio specificate. Non sono ammesse impostazioni autonome della password al Bios del computer onde evitare impedimenti all'accesso in caso di prolungata assenza o impedimento dell'incaricato e considerata la necessità dell'Ente di garantire in ogni caso la continuità dei servizi aziendali.

Le credenziali di autenticazione per l'accesso alla rete informatica e per l'utilizzo del servizio di posta elettronica vengono assegnate dal Responsabile dei servizi informatici *previa formale richiesta da effettuarsi attraverso la compilazione dell'apposito modulo, sottoscritta dal Responsabile della funzione presso la quale l'Utente dovrà operare ((n.b. al momento la gestione non è strutturata così).*

Nel caso di collaboratori a progetto e coordinati e continuativi quali borsisti, tirocinanti, volontari etc. la preventiva richiesta, se necessaria, verrà inoltrata direttamente dalla Direzione Aziendale (ovvero al Responsabile della struttura con la quale il collaboratore si coordina nell'espletamento del proprio incarico). Sarà cura del Responsabile dare tempestiva comunicazione al Responsabile dei servizi informatici, previa compilazione di apposito modulo nell'eventualità che il collaboratore cessi o abbia cessato il rapporto con l'Ente prima del tempo indicato nel modulo di richiesta, al fine di evitare un possibile uso illecito dei servizi forniti. Stesso onere di comunicazione spetta al Responsabile nel caso in cui il collaboratore si trasferisca in altre strutture.

La credenziale di autenticazione (login) consiste in un codice per l'identificazione dell'Utente (user id), assegnato dal personale tecnico autorizzato dal Responsabile dei servizi informatici ed associato ad una parola chiave (password) riservata e modificata dall'Utente al primo accesso. Essa dovrà essere memorizzata, custodita con la massima diligenza e non divulgata (ad es.: non scrivere la password su carta o post-it lasciandoli sulla scrivania o attaccati al monitor; non comunicare o condividere con altri colleghi la propria password); durante la digitazione della propria password, assicurarsi che nessuno stia osservando la tastiera.

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 quali:

- all'aumentare della sua lunghezza, aumenta la difficoltà a carpirla;
- include cifre, lettere e caratteri speciali;
- evita il più possibile ripetizioni (ad esempio, alterna in modo caotico lettere maiuscole e minuscole, simboli, numeri);
- non contiene il proprio nome o cognome, il soprannome, la data di nascita, il nome di persone familiari o la loro data di nascita, 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 "qwerty", o da ripetizioni del proprio nome utente (ad es. se il proprio utente e rossi; la password "rossirossi" sarebbe inopportuna).

La password di accesso di ciascun Utente di rete sarà automaticamente reimpostata ogni 90 giorni. In base a tale procedura automatica, l'Utente, mediante idoneo avviso a video, dovrà inserire una nuova password, diversa dalla precedente, pena il blocco del computer con conseguentemente inibizione dell'accesso alla rete aziendale.

L'Utente potrà richiedere la modifica della password al personale tecnico autorizzato dal Responsabile dei servizi informatici al di fuori della decorrenza del termine sopra previsto in caso questi ravveda una potenziale perdita della riservatezza. Qualsiasi azione svolta sotto l'autorizzazione offerta dalla coppia userid e password sarà attribuita in termini di responsabilità all'utente titolare del codice userid, salvo che l'utente dia prova di illecito utilizzo della sua autorizzazione da parte di terzi.

7. Utilizzo della rete e accessi da remoto

Per l'accesso alla Rete (intranet aziendale) ciascun Utente deve essere in possesso delle specifiche credenziali sopra descritte.

È assolutamente vietato accedere alla rete informatica aziendale e/o nei programmi con un codice di identificazione Utente di un altro operatore.

La presenza di eventuali cartelle di rete condivise sono da considerarsi strumento di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi.

Si ricorda che tutti i dischi rigidi o altre unità di memorizzazione locali (es. dischi fissi interni o esterni al PC) non sono soggette a salvataggio da parte del personale incaricato dal Responsabile dei servizi informatici. La responsabilità del salvataggio dei dati ivi contenuti è pertanto a carico del singolo utente.

Il personale tecnico incaricato del Responsabile dei servizi informatici può in qualunque momento, senza preavviso, procedere alla rimozione dai computer in rete di ogni file e/o applicazione che riterrà essere pericolosi per la sicurezza dei dati e della rete.

Non è consentito collegare alle prese di rete apparecchiature non autorizzate da parte del Responsabile dei servizi informatici, quali: hub, switch, access point o similari. Non è inoltre consentito installare o utilizzare qualsiasi altra apparecchiatura atta a gestire comunicazioni, salvo specifica autorizzazione rilasciata dal Responsabile dei servizi informatici, quali, a titolo esemplificativo: modem, router, Internet key,... Non è inoltre consentito effettuare spostamenti o modifiche di risorse collegate alla rete aziendale (es.. pc, Stampanti, fotocopiatori e altro) senza una preventiva autorizzazione.

I tecnici delle ditte esterne (fornitori applicativi, sistemisti etc) dovranno richiedere l'autorizzazione del Responsabile dei servizi informatici prima di collegarsi fisicamente alla rete aziendale con dispositivi personali. Quest'ultimi saranno sottoposti alle politiche di sicurezza di questa Ente al fine di garantire la sicurezza generale della rete informatica.

Gli accessi da remoto verso la rete aziendale potranno essere effettuati solo previa autorizzazione del Responsabile dei servizi informatici che rilascerà apposite credenziali per l'autenticazione sicura dopo la compilazione di specifico modulo. Tutti gli accessi saranno monitorati e registrati.

Per garantire la manutenzione della sicurezza e della rete, soggetti autorizzati dal Titolare (di norma Amministratori di sistema e aziende esterne autorizzate) possono monitorare gli apparati, i sistemi ed il traffico in rete in ogni momento rispettando la riservatezza degli utilizzatori attraverso analisi aggregata ed anonima dei dati di traffico.

Controlli su base individuale saranno attivati solo in caso di reiterati comportamenti illeciti e non conformi e comunque dopo un avviso generalizzato relativo al rilevato utilizzo anomalo degli strumenti aziendali.

8. Utilizzo dei supporti rimovibili

Eventuali supporti magnetici contenenti dati sensibili devono essere adeguatamente custoditi dall'Utente in armadi o cassetti chiudibili a chiave. E' vietato l'utilizzo di supporti rimovibili personali (dischi rigidi e penne USB) compreso qualsiasi altro punto di memorizzazione tramite internet (c.d. "remote storage") nel caso si voglia trattare dati personali, sensibili e/o giudiziari. In caso di trasferimento di dati sensibili tra computer in rete, si devono necessariamente utilizzare "cartelle di lavoro condivise" e protette da password note solo agli utenti a ciò interessati. L'Utente è responsabile della custodia dei supporti e dei dati in essi contenuti.

I supporti rimovibili contenenti dati sensibili, giudiziari o di natura riservata se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri Utenti incaricati, non autorizzati al trattamento

degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcuni modo ricostruibili.

9. Uso della posta elettronica

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

La casella di posta elettronica assegnata all'Utente è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

La casella di posta elettronica aziendale ha la seguente estensione:

inziale nome.cognome@arcajonica.gov.it

Di conseguenza, ogni impostazione diversa dalla precedente dovrà essere debitamente motivata, e previamente autorizzata dal Responsabile Servizi Informatici. In assenza di tali autorizzazioni, le caselle di posta elettronica diverse dal form definito con tale impostazione dovranno essere dismesse.

È fatto divieto di utilizzare le caselle di posta elettronica assegnate dall'Ente per motivi diversi da quelli strettamente legati all' attività lavorativa.

Reciprocamente, è vietato usare per scopi istituzionali caselle di posta elettronica di providers diversi da quello istituzionale (es. libero, gmail eccetera).

In questo senso, a titolo puramente esemplificativo, l'Utente **non potrà** utilizzare la posta elettronica istituzionale (ordinaria e/o certificata) per:

- l'invio e ricevimento di corrispondenza personale;
- l'invio e/o ricevimento di allegati contenenti filmati o brani musicali (es. mp3) non legati all'attività lavorativa;
- invio e/o il ricevimento di messaggi legati ai propri interessi extralavorativi, ad esempio per la partecipazione a dibattiti, sondaggi e aste on-line;
- partecipare a catene tematiche (o di Sant'Antonio); non si dovrà in alcun caso procedere all'apertura degli allegati a tali messaggi.

La casella di posta elettronica deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti (in termini di centinaia di MB e, ancor più di GB).

È obbligatorio porre la massima attenzione nell'aprire i file allegati alle e-mail prima del loro utilizzo.

In linea di massima è vietato eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti; altrimenti, se obbligati, si dovrà sottoporre necessariamente detti file ad una "scansione approfondita" dell'antivirus prima del loro utilizzo.

L'Utente assegnatario della casella di posta elettronica istituzionale e il diretto responsabile del corretto utilizzo della stessa e risponde 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.

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:

- 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;
- non aprire allegati con estensione .zip , .rar, .exe e similari se la provenienza risulti dubbia;
- limitare l'invio ai soli destinatari interessati;

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

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

In caso di assenza prolungata programmata del dipendente, 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.

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 aziendale sia necessario accedere a informazioni o documenti di lavoro presenti sul personal computer del dipendente, inclusi 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 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 aziendale 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 Responsabile dei servizi informatici 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 in cui il dipendente non presti più la sua attività lavorativa presso questo Ente, la casella di posta elettronica sarà prontamente disattivata. Su richiesta dell'interessato la casella di posta potrà restare attiva per ulteriori tre mesi dalla data di cessazione del rapporto di lavoro, durante il quale sarà inserita una risposta automatica d' ufficio.

10. Navigazione Internet

Il PC assegnato all' Utente ed abilitato alla navigazione in internet costituisce uno strumento utilizzabile esclusivamente per lo svolgimento della propria attività lavorativa. È quindi assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all' attività lavorativa.

In questo senso, a titolo puramente esemplificativo, l'Utente non potrà utilizzare Internet per:

- l'upload o il download di software gratuiti se non espressamente autorizzati dal Responsabile dei servizi informatici;
- l'upload o il download di files non legati alla attività lavorativa, soprattutto se di intrattenimento (es. files mp3, mp4, m4v, mov, mpg o mpeg, wmv eccetera);
- utilizzo di documenti (soprattutto filmati e musica) provenienti da siti web o http, se non strettamente attinenti all'attività lavorativa;
- l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, fatti salvi i casi autorizzati e comunque nel rispetto delle normali procedure di acquisto;
- ogni forma di registrazione a siti i cui contenuti non siano strettamente legati all'attività lavorativa;
- partecipazione a forum non professionali, a giochi on-line, l'utilizzo di chat line, di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames).

Al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa, l'Ente con logica preventiva, adotta uno specifico sistema di filtro automatico che impedisce determinate operazioni quali l'upload, download (illeciti o illegali) o l'accesso a determinati siti ludici (black-list). 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 dal Titolare); peer to peer; malware, spyware, hacking, proxy anonimi, bypass proxy, phishing.

Tali limitazioni sono purtroppo talvolta aggirabili con artifici informatici; di conseguenza, la responsabilità sul rispetto del divieto di accesso a tali contenuti è in ogni caso in capo all'utente.

Qualsiasi altra tipologia di contenuti o siti che il Titolare riterrà di non dover rendere accessibile dalla rete aziendale, verrà preventivamente comunicata agli utenti.

La navigazione, ovvero l'accesso ai siti Internet, avviene previa autenticazione dell'Utente su di un Proxy Server. Di conseguenza, viene reso noto che è registrato, ed è consultabile anche da remoto, il tracciato cronologico dei siti frequentati. 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. Gli eventuali controlli per motivi di sicurezza informatica, compiuti esclusivamente dal personale tecnico autorizzato dal Responsabile dei servizi informatici, potranno avvenire mediante un sistema di controllo dinamico dei contenuti o mediante "file di log" della navigazione svolta. Il controllo sui log, i quali sono cancellati periodicamente ed automaticamente, non è sistematico e le informazioni vengono conservate temporaneamente per finalità di sicurezza di questo Ente.

Il prolungamento dei tempi di conservazione dei log potrà aver luogo solo nei seguenti casi:

- Esigenze tecniche o di sicurezza del tutto particolari;
- Indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;
- Su specifica richiesta dell'autorità giudiziaria

L'utilizzo degli strumenti aziendali 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.

Per garantire la manutenzione della sicurezza e della rete, soggetti autorizzati dalla Direzione Aziendale (di norma Amministratori di sistema e aziende esterne autorizzate) possono monitorare gli apparati, i sistemi ed il traffico in rete in ogni momento rispettando la riservatezza degli utilizzatori attraverso analisi aggregata ed anonima dei dati di traffico.

Controlli su base individuale saranno attivati solo in caso di reiterati comportamenti illeciti, anomali o non conformi alla normativa e al presente regolamento, e comunque dopo un avviso "generalizzato" relativo al rilevato utilizzo anomalo degli strumenti aziendali all'intera struttura lavorativa o sue aree.

11. Protezione da virus

Le postazioni di lavoro sono protette da software antivirus aggiornato quotidianamente.

Ogni Utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico. Questa fattispecie può accadere mediante virus o malware, proveniente da dati e/o software importati/installati dall'Utente, che si auto-installano, all'insaputa dell' Utente, all'interno del Pc, infettandolo e diffondendosi nella rete informatica aziendale.

Nel caso in cui il software antivirus rilevi e non disinfetti la presenza di un virus, l'Utente dovrà immediatamente sospendere ogni elaborazione in corso e segnalare l'accaduto al personale tecnico autorizzato dal Responsabile dei servizi informatici.

Ogni dispositivo di memorizzazione esterna dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e nel caso venga rilevato un virus, dovrà essere prontamente consegnato al personale tecnico autorizzato che provvederà ad effettuare le dovute operazioni di disinfezione.

Si considererà comportamento sanzionabile quello dei dipendenti che assoggetteranno il proprio PC alla aggressione di virus per avere RIPETUTAMENTE superato gli alert del sistema antivirus, aprendo comunque i files dei quali veniva rilevata la pericolosità.

12. Salvataggio dati

Ogni Utente é responsabile della corretta conservazione dei dati e dei documenti elettronici che utilizza sul Pc per motivi lavorativi, di qualsiasi tipo, formato e natura essi siano. Per questo motivo la tutela della gestione dei dati sulle postazioni di lavoro (Personal computer e Pc portatili) è demandata all'Utente finale, che avrà l'obbligo di effettuare il salvataggio dei dati memorizzati sui computer in dotazione, con frequenza almeno settimanale e la conservazione degli stessi in luogo idoneo.

Il Responsabile dei servizi informatici metterà a disposizione degli Utenti che ne facessero richiesta, delle partizioni di disco su file server aziendali che l'Utente potrà utilizzare, in maniera esclusiva e riservata, per il salvataggio dei dati aziendali (nb servizio da organizzare).

Costituisce buona regola la pulizia periodica (almeno ogni sei mesi) degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. E' infatti assolutamente da evitare un'archiviazione ridondante.

13. Teleassistenza

Per lo svolgimento di normali attività di assistenza e manutenzione su personal computer connessi alla rete, il personale tecnico autorizzato dal Responsabile dei servizi informatici potrà utilizzare specifici software di connessione remota. Tali programmi sono utilizzati per assistere l'Utente al fine di effettuare interventi di assistenza informatica e di manutenzione su applicativi e hardware in uso. L'attività di assistenza e manutenzione avviene previa autorizzazione da parte dell'Utente e mediante visualizzazione di un indicatore visivo sul monitor che segnala la connessione in remoto del tecnico informatico.

14. Monitoraggio

Il Titolare, attraverso il Responsabile dei servizi informatici, effettuerà monitoraggi periodici su dati anonimi allo scopo di verificare l'attuazione del presente Disciplinare, 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.

15. Controlli

L'Ente si riserva di effettuare controlli per verificare il rispetto del presente politica.

Riguardo a tali controlli la presente Politica costituisce preventiva e completa informativa nei confronti dei dipendenti.

In base al principio di correttezza, l'eventuale trattamento deve essere ispirato ad un canone di ' trasparenza, come prevede anche la disciplina di settore.

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, il Titolare, attraverso il Responsabile dei servizi informatici, potrà adottare le eventuali misure che consentano la verifica di ali 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 aziendali, invitando i destinatari ad attenersi scrupolosamente al 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 e irregolarità, saranno effettuati controlli su base individuale.

n 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;

Oltre a ciò l'Ente si riserva di effettuare specifici controlli sui software caricati sul 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'Ente 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, che ledono diritti di terzi o che, comunque, risultino illegittime.

16. Sanzioni

È fatto obbligo a tutti i Dipendenti ed Utenti del sistema informativo dell'Ente di osservare le disposizioni portate a conoscenza con il presente Regolamento. Il mancato rispetto o la violazione delle regole sopra ricordate é perseguibile con provvedimenti disciplinari e/o risarcitori previsti dalla vigente normativa, nonché con tutte le azioni civili e penali consentite.

17. Aggiornamento e revisione

Il presente Regolamento è stato redatto tenendo conto sia delle Linee guida del Garante della Privacy emanate con delibera n. 13 del 1° marzo 2007 che della direttiva n. 2/2009 del Ministro per la Pubblica Amministrazione e Innovazione.

Per qualsiasi eventuale ulteriore indicazione, valgono oltre al presente regolamento le disposizioni di cui al disciplinare tecnico riportato in allegato "B" al d.lgs 196/2003.

Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni al presente Regolamento. Le proposte vanno esaminate dalla Direzione Aziendale.

Il presente Regolamento è soggetto a revisione con frequenza annuale o qualora se ne ravveda la necessità.

Copia del presente documento verrà consegnata a ciascun dipendente aziendale ovvero messo a disposizione per ogni Utente autorizzato all'utilizzo della rete aziendale.

Con l'entra a in vigore del presente Regolamento, tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi sostituite dalle presenti.