PROVINCIA REGIONALE DI CATANIA

denominata "Libero Consorzio Comunale" ai sensi della L.R. n. 8/2014

REGOLAMENTO sull'utilizzo della Rete informatica e dei Servizi di telefonia

Redatto ai sensi del D.Lgs. 196/2003

(Testo unico sulla Privacy)

Allegato della Deliberazione del Commissario Straordinario con i poteri della Giunta n. 108 del 20/08/2014

PREMESSA

La diffusione delle nuove tecnologie dell'informazione e della comunicazione nelle Pubbliche Amministrazioni ha determinato notevoli vantaggi, innalzando gradualmente i livelli di economicità ed efficienza dell'azione amministrativa, ma ha anche generato una considerevole esposizione dell'Ente e degli utenti (dipendenti e collaboratori dello stesso) a rischi di natura tecnica e patrimoniale, oltre alle responsabilità penali conseguenti alla violazione di specifiche disposizioni di legge (diritto d'autore, privacy, ecc.), con possibili evidenti problemi alla sicurezza ed all'immagine dell'Ente, e con eventuali implicazioni relative alla tutela della riservatezza e dei dati personali.

La Provincia Regionale di Catania denominata "Libero Consorzio Comunale" ai sensi della L.R. n. 8/2014, e da qui in avanti chiamata "Ente", in qualità di datore di lavoro, in un'ottica di trasparenza, diligenza e correttezza, adotta il presente regolamento sulle modalità di utilizzo della posta elettronica, della navigazione nella rete Internet, intranet e dei servizi di telefonia VoIP, che contiene, oltre ai richiami previsti nel provvedimento del Garante della Privacy n. 13 del 1° marzo 2007, "Linee guida del Garante per posta elettronica e internet" e nella direttiva n. 2 del 26 maggio 2009 "Utilizzo di Internet e della casella di posta elettronica istituzionale sul luogo di lavoro" della Presidenza del Consiglio dei Ministri - Dipartimento della Funzione Pubblica, le necessarie integrazioni normative correlate alle dinamiche interne dell'Ente.

Questo regolamento è rivolto a tutti gli utilizzatori di Intranet, Internet, della posta elettronica e dei servizi di telefonia VoIP, al fine di responsabilizzarli nei confronti di eventuali utilizzi non coerenti con la prestazione lavorativa e non conformi alle norme che disciplinano il lavoro alle dipendenze delle Pubbliche Amministrazioni, e per evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla sicurezza nel trattamento dei dati.

Considerato inoltre che l'Ente, nell'ottica di uno svolgimento proficuo e più agevole della propria attività, mette a disposizione dei propri dipendenti e collaboratori apparecchiature informatiche e mezzi di comunicazione efficienti (Personal Computer, Notebook, casella di posta elettronica, accesso alla rete Internet, etc.), sono stati inseriti nel regolamento alcuni articoli relativi alle modalità ed alle regole che ciascun utente deve osservare nell'utilizzo delle apparecchiature informatiche.

FIGURE COINVOLTE:

Provincia Regionale di Catania denominata "Libero Consorzio Comunale" ai sensi della L.R. n. 8/2014: Datore di Lavoro e "Titolare";

Segretario Generale: Responsabile della Trasparenza ed Anticorruzione e detentore della "Chiave Crittografata";

Dirigente del Servizio Informatica: Responsabile del trattamento dei dati dei file di log e responsabile della nomina degli Amministratori di Sistema e di Dominio;

Amministratore di Sistema, con il compito della "gestione" della rete Lan sovrintendendo alle risorse dei Sistemi Operativi degli elaboratori (Sala Ced) e dei Sistemi di DataBase. Può accedere in modo privilegiato alle risorse del sistema telematico/informativo per lo svolgimento della propria mansione;

Amministratori di Dominio PRVCT*,* con il compito di:

- accedere alle risorse di rete (P.C.) sia in locale che da "remoto" ai fini di assistenza tecnica;
- accedere a tutti i dati degli Utenti, sia a quelli delle cartelle condivise di ogni Servizio, ubicati nell'*Areadir* dello Storage, sia a quelli all'interno delle cartelle personali collocati sulla *Homedir* di ogni singolo Utente;
- attivare nuovi Utenti di Dominio;

- annettere a Dominio nuovi PC e nuove stampanti di rete;
- installare software applicati sui p.c. della Rete annessi a Dominio;

Utenti del Dominio sono tutti gli utenti della rete (Dipendenti, Amministratori, etc…) che hanno diritto di accesso ai servizi di rete;

INDICE

ART. 1 - FINALITA'

1. Il presente regolamento è diretto a definire i criteri e le modalità operative di accesso ed utilizzo della posta elettronica, della navigazione nella rete Intranet e Internet e dei servizi di telefonia VoIP, al fine di assicurare un uso corretto e razionale delle stesse da parte degli utenti.
2. Il Servizio Sistemi Informativi propone la programmazione, gestione e manutenzione delle risorse informatiche e adotta idonee misure organizzative, tecnologiche e di sicurezza, volte a prevenire il rischio di utilizzo improprio delle risorse informatiche ed il contenzioso con gli utenti.

ART. 2 - CAMPO DI APPLICAZIONE

1. Il campo di applicazione riguarda i seguenti servizi: Intranet, Internet, posta elettronica e telefonia VoIP.
2. Il regolamento si applica a tutti gli utenti. Per "utenti" si intendono gli amministratori, i dirigenti, i dipendenti a tempo indeterminato e determinato, i lavoratori interinali, i collaboratori coordinati e continuativi, i collaboratori, i tirocinanti e comunque, chiunque, a prescindere dal rapporto contrattuale intrattenuto con l'Amministrazione, sia in possesso di specifiche credenziali di autenticazione per l'accesso al sistema informatico, alla navigazione internet, all'uso della posta elettronica e dei servizi di telefonia VoIP, rilasciate dal Servizio Sistemi Informativi a seguito di richiesta di autorizzazione del Dirigente del Servizio competente.

ART. 3 - PRINCIPI GENERALI

1. L'Ente promuove l'utilizzo di Intranet, Internet, della posta elettronica e dei servizi di telefonia VoIP, quali risorse necessarie a perseguire con efficienza le proprie finalità.
2. Ogni utente è responsabile, civilmente e penalmente, del corretto uso delle risorse informatiche e dei servizi di telefonia VoIP. E' altresì responsabile del contenuto delle comunicazioni effettuate e ricevute a fini istituzionali anche per quanto attiene la riservatezza dei dati contenuti, la cui diffusione impropria potrebbe configurare violazione del segreto d'ufficio e della normativa per la tutela dei dati personali.

ART. 4 - FILE DI LOG

1. I file di log sono archivi nei quali sono registrate le attività che l'utente compie durante la navigazione nella rete Internet, l'utilizzo della posta elettronica e dei servizi telefonici.
2. Il responsabile del trattamento dei dati dei file di log è il Dirigente del Servizio Sistemi Informativi.
3. Gli incaricati del trattamento dei dati sono nominati dal Dirigente del Servizio Sistemi Informativi con atto scritto.
4. Le informazioni trattate possono contenere dati personali, anche sensibili, riguardanti gli utenti, identificati o identificabili.

ART. 5 - UTILIZZO DEL PERSONAL COMPUTER

1. Il Personal Computer affidato al dipendente è uno strumento di lavoro. Ogni utilizzo non inerente all'attività lavorativa può contribuire a innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.
2. L'utilizzo del computer è protetto da credenziali di accesso (*username e password*) che devono essere custodite dall'incaricato e non divulgate. Anche il collegamento alla rete Intranet, Internet, posta elettronica e applicativi vari è protetto da credenziali di accesso. Non è consentita l'attivazione della password di accensione (*bios*).
3. L'Amministratore del Sistema, se ne ricorrono le condizioni previste dalla legge, su richiesta dei vari Dirigenti responsabili dei Servizi, per reperire informazioni d'ufficio, può accedere agli archivi e ai documenti presenti nel Personal Computer affidato al dipendente.
4. Non è consentito l'uso di programmi diversi da quelli distribuiti ufficialmente dal Servizio Sistemi Informativi dell'Ente(*D.Lgs. 518/92 sulla Tutela giuridica del software e L. 248/2000 nuove norme di tutela del diritto d'autore*).
5. Non è consentito installare autonomamente programmi provenienti dall'esterno perché sussiste il grave pericolo di portare virus informatici e di alterare la stabilità delle applicazioni del computer, salvo casi particolari in cui può essere richiesta l'installazione di programmi per scopi lavorativi all'Amministratore del Sistema.
6. Non è consentito all'utente modificare le caratteristiche impostate sul proprio PC, salvo previa autorizzazione esplicita dell'Amministratore del Sistema.
7. Il Personal Computer deve essere spento prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio. In ogni caso deve essere attivato lo *screen saver* con la relativa password.
8. Non è consentita la memorizzazione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.
9. In presenza di ospiti o di personale di servizio occorre:
   - Fare attendere gli ospiti in luoghi in cui non siano presenti informazioni riservate o dati personali.
   - Se è necessario allontanarsi dalla scrivania in presenza di ospiti, riporre i documenti e attivare il salvaschermo (*screen saver*) del PC premendo *ctrl-alt-canc* e selezionando il pulsante "*Blocca Computer*".
   - Non rivelare o fare digitare le password dal personale di assistenza tecnica.
   - Non rivelare mai le password.
   - Segnalare qualsiasi anomalia o stranezza telefonicamente al Servizio Helpdesk (n. Tel. 4444).

ART. 6 - UTILIZZO DELLA RETE

1. Le unità di rete *storage-areadir* sono aree di condivisione di informazioni relative al Servzio/Ufficio di appartenenza e non devono essere utilizzate per scopi diversi, mentre le unità di rete *storage-homedir* sono aree di utilizzo personale attinenti ad attività d'ufficio. Tali unità di rete sono sottoposte a backup giornaliero con riciclo settimanale su unità DAT conservate in un armadio ignifugo.
2. Le password d'ingresso alla rete e ai programmi sono segrete e vanno gestite secondo le

procedure impartite. È assolutamente proibito entrare nella rete e nei programmi con nomi utente di altri.

3. Costituisce buona regola la periodica (almeno ogni sei mesi) pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. É infatti assolutamente da evitare un 'archiviazione ridondante.
4. É cura dell'utente effettuare la stampa dei dati solo se strettamente necessaria e di ritirarla prontamente dai vassoi delle stampanti condivise. É buona regola evitare di stampare documenti molto lunghi su stampanti condivise. In caso di necessità la stampa in corso può essere cancellata.

ART. 7 - GESTIONE DELLE CREDENZIALI DI AUTENTICAZIONE

1. Il codice per l'identificazione dell'incaricato (*username*) e la relativa *password* di ingresso alla rete Intranet e Internet, di accesso ai programmi e dello *screen saver*, sono previste ed attribuite dall'Amministratore del Sistema. Il codice per l'identificazione dell'incaricato non potrà essere assegnato ad altri incaricati, neppure in tempi diversi. É consentita comunque l'autonoma sostituzione della *password* da parte degli incaricati al trattamento.
2. La *password* è composta da almeno otto caratteri; essa non deve contenere riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni **90 giorni**.
3. Nella gestione delle password si devono rispettare le seguenti regole:
   - Non utilizzare i nomi di personaggi dello spettacolo e non fare alcun riferimento ai dati personali propri (nomi, indirizzi, date di nascita….), dei propri parenti, amici, colleghi o comunque conoscenti;
   - Non sceglierla uguale alla matricola o alla *username*;
   - Non possono essere uguali alle 10 password precedentemente utilizzate dall'utente;
   - Custodirla sempre in un luogo sicuro e non accessibile a terzi;
   - Non divulgarla a terzi;
   - Non condividerla con altri utenti.
4. Le credenziali di autenticazione non utilizzate da almeno **sei mesi** vengono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica. Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.
5. Alla credenziali di autenticazione è associato un profilo di autorizzazione, allo scopo di limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento. Periodicamente, e comunque almeno **annualmente**, è verificata la sussistenza delle condizioni per la conservazione del profilo di autorizzazione assegnato.

ART. 8 - UTILIZZO DEI SUPPORTI RIMOVIBILI

1. I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.
2. I supporti rimovibili contenenti dati sensibili devono essere custoditi in archivi chiusi a chiave.
3. Non è consentito scaricare nel PC dell'ufficio *file* contenuti in supporti rimovibili non aventi alcuna attinenza con la propria prestazione lavorativa.

4. Tutti i *file* di provenienza incerta od esterna, ancorché attinenti all'attività lavorativa, sono sottoposti automaticamente al controllo preventivo dell'antivirus installato sul PC.
5. I *file* che contengono dati sensibili, che non vengono conservati per ragioni di legge, di documentazione o di lavoro, devono essere rimossi in modo appropriato e sicuro.

ART. 9 - UTILIZZO DI PC PORTATILI

1. L'utente è responsabile del PC portatile assegnatogli dall'Amministrazione e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.
2. Ai PC portatili si applicano le regole di utilizzo previste per i PC connessi in rete, con particolare attenzione alla rimozione di eventuali *file* elaborati sullo stesso prima della riconsegna.
3. I PC portatili utilizzati all'esterno (convegni, visite in azienda), in caso di allontanamento, devono essere custoditi in un luogo protetto. Devono essere prese particolari precauzioni quando si opera da posti pubblici, nelle stanza dove si tengono riunioni ed in altre zone non protette fuori dei locali dell'Ente.

ART. 10 - USO DELLA POSTA ELETTRONICA

1. La casella di posta elettronica, sia convenzionale che certificata, è uno strumento di lavoro sempre più utilizzato nella comunicazione tra i cittadini, le imprese e la Pubblica Amministrazione e tra le Pubbliche Amministrazioni; costituisce, per l'Ente lo strumento privilegiato per tutte le comunicazioni, sia interne che esterne allo stesso.
2. Per gli assegnatari di casella di posta elettronica convenzionale, con dominio del tipo "nome.cognome@provincia.ct.it", se ne raccomanda la consultazione quotidiana e le risposte in tempi ragionevoli alle e-mail ricevute;
3. Per gli assegnatari di casella di Posta Elettronica Certificata, essendo la PEC equivalente alla raccomandata A/R tradizionale, avendone lo stesso valore legale, ovvero l'opponibilità a terzi della spedizione e ricezione di un documento, è obbligatoria la consultazione tempestiva in modo da evitare pregiudizi o comunque danni all'Ente.
4. Per entrambe le tipologie di caselle è necessario archiviare/scaricare periodicamente il contenuto in modo da evitare che tali caselle si possano riempire, rendendo impossibile l'invio e la ricezione di nuovi messaggi.
5. La casella di posta elettronica, convenzionale e certificata, deve essere utilizzata dall'utente esclusivamente per ragioni d'ufficio e non per fini personali privati. Ciò al fine di prevenire inutili intrusioni nella sfera personale dei lavoratori e/o violazioni della segretezza della corrispondenza.
6. É vietato utilizzare tecniche di "mail spamming".
7. Per le comunicazioni di eventi o di iniziative istituzionali è consentito l'invio di comunicazioni a liste di utenti. Per tipologie di comunicazioni preventivamente autorizzate dall'Amministrazione, lo strumento pubblicitario interno è la bacheca dell'Area Intranet, quello esterno è il sito Internet dell'Ente (www.provincia.ct.it).
8. É vietato allegare al testo delle comunicazioni materiale potenzialmente insicuro (ad esempio file eseguibili di cui non sia certa la provenienza o contenenti macro, ecc);

9. Ogni Servizio dell'Ente, su richiesta del proprio Dirigente, potrà chiedere al Servizio Sistemi Informativi l'attivazione di un indirizzo di posta elettronica, individuale o condiviso, funzionale all'espletamento delle relative attività;
10. Sull'home page del sito della Provincia dovrà essere istituita apposita bacheca virtuale finalizzata alla pubblicizzazione delle informative sindacali.

ART. 11 - USO DELLA RETE INTERNET E DEI RELATIVI SERVIZI

1. Il PC abilitato alla navigazione in Internet costituisce uno strumento aziendale necessario allo svolgimento della propria attività lavorativa. É fatto divieto all'utente lo scarico di software gratuito (*freeware*) e *shareware* prelevato da siti Internet, se non espressamente autorizzato dall'Amministratore del Sistema.
2. É vietata ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.
3. É vietata la partecipazione a *forum* non professionali, l'utilizzo di *chat line* (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in *guest books* anche utilizzando pseudonimi (o *nicknames*).
4. É vietato accedere a siti pornografici, pedofili e di simile natura.
5. La rete internet è una risorsa messa a disposizione degli utenti quale fonte di lavoro, informazione, documentazione, ricerca e studio. La normativa vigente pone in capo all'Amministrazione l'onere di predisporre misure tecnologiche ed organizzative per ridurre il rischio di utilizzi impropri di internet consistenti in attività non correlate alla prestazione lavorativa, quali la visione di siti non pertinenti, l'upload e il download di file per finalità ludiche o comunque estranee all'attività lavorativa.
6. Tutti gli utenti ai quali sono state assegnate le credenziali di autenticazione utilizzano la rete internet secondo le limitazioni e le *policies* stabilite dall'Amministrazione.
7. Al fine di prevenire il rischio di utilizzi impropri della rete, reputati non compatibili con l'attività lavorativa, il Servizio Sistemi Informativi implementa un sistema di filtri che impedisce l'accesso diretto ad alcuni siti e il download di file o software aventi particolari caratteristiche (vedere l'elenco allegato "*Proxy Common Access Control List - ACL*"). Per motivate esigenze lavorative, su richiesta del competente Dirigente, potrà essere richiesta al Servizio Sistemi Informativi l'autorizzazione alla navigazione su risorse che risultassero non accessibili.
8. Ciascun dipendente è direttamente e personalmente responsabile dell'uso del servizio di accesso a Internet, dei contenuti che vi ricerca, dei siti che contatta, delle informazioni che vi immette e delle modalità con cui opera.
9. Per favorire la dematerializzazione dei processi produttivi è consentito assolvere incombenze amministrative e burocratiche senza allontanarsi dal luogo di lavoro (es. effettuare adempimenti on line nei confronti di Pubbliche Amministrazioni e di concessionari di servizi pubblici, ovvero per tenere rapporti con istituti bancari ed assicurativi) purché contenute nei tempi strettamente necessari allo svolgimento delle transazioni (punto 3 "Utilizzo della rete Internet" della Direttiva n. 2/2009 della Presidenza del Consiglio dei Ministri, Dipartimento della funzione pubblica.).
10. Le credenziali di accesso al servizio (USERNAME e PASSWORD) sono personali e segrete. Qualunque azione o attività esercitata mediante l'utilizzo del codice identificativo e della password assegnati è ascritta in via esclusiva all'utente assegnatario delle credenziali di autenticazione che sarà chiamato a rispondere delle attività svolte. L'utente

è civilmente responsabile di qualsiasi danno arrecato all'Ente e/o a terzi in violazione di quanto espressamente previsto dalle norme e di quanto indicato nel presente regolamento. L'utente può essere chiamato a rispondere, oltre che per i propri fatti illeciti, anche per quelli commessi da chiunque utilizzi il suo codice identificativo e la sua parola chiave con il suo consenso o comunque in seguito ad un suo negligente comportamento sulla custodia delle credenziali di accesso. La violazione delle presenti disposizioni può comportare infine l'applicazione delle sanzioni disciplinari previste dai vigenti Contratti Collettivi di Lavoro, rimanendo ferma ogni ulteriore forma di responsabilità civile e penale.

ART. 12 - PROTEZIONE ANTIVIRUS

1. L'Ente è dotato di sistemi di protezione contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale.
2. Sulla base dell'analisi dei casi, degli incidenti, delle diverse tipologie di virus e worm Trojan Horse e altri tipi di programmi nocivi, delle modalità con cui si propaga un'infezione all'interno di un contesto lavorativo, si elencano una serie di raccomandazioni utili per la prevenzione e la protezione dei dati che ogni utente dovrà osservare:
   - nella posta elettronica, quando si introducono allegati è bene usare formati aperti (es. .pdf, .txt, .kml, .xml, .csv, .rtf), facilmente leggibili da chiunque e possibilmente non contenenti macro;
   - fare attenzione quando si utilizzano file contenenti macro sopratutto quando la fonte non è conosciuta o comunque poco attendibile;
   - fare attenzione agli allegati che contengono un'estensione doppia;
   - in caso di ricezione di una e-mail con oggetto insolito, effettuare un controllo con il mittente prima di aprire l'eventuale allegato;
   - non considerare le icone mostrate dagli allegati come garanzia dell'integrità del software;
   - in caso di ricezione di e-mail non richieste o con oggetti insoliti, o con collegamenti ad indirizzi web presenti nel testo, non aprirle senza aver preventivamente valutato l'opportunità;
   - controllare che i supporti di memorizzazione utilizzati e scambiati siano immuni da virus;
   - non tentare di avviare il computer da supporti esterni;
   - evitare di prelevare ed eseguire software da sorgenti poco affidabili;
   - non utilizzare programmi non autorizzati, con particolare riferimento ai videogiochi, spesso veicoli di virus.

ART. 13 - MONITORAGGI E CONTROLLI

1. Gli eventuali controlli sull'utilizzo della rete internet, compiuti dal personale incaricato della sicurezza informatica interna, potranno avvenire mediante analisi dei "file di log". L'utilizzo di tali informazioni (file di log) è ispirato ai principi di pertinenza e non eccedenza ed avverrà nel rispetto delle "*Linee guida del Garante per posta elettronica e internet*" (G. U. n. 58 del 10 marzo 2007).
2. Nell'effettuare controlli sull'uso di internet e della posta elettronica sarà evitata un'interferenza ingiustificata sui diritti e le libertà fondamentali dei lavoratori, come pure

di soggetti esterni che ricevono o inviano comunicazioni elettroniche di natura personale o privata.

3. Non saranno utilizzati sistemi hardware e software che mirano al controllo a distanza dei lavoratori, svolti mediante:
   - la lettura e la registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio di email;
   - la riproduzione e la memorizzazione sistematica delle pagine web visualizzate dagli utenti;
   - l'analisi occulta dei computer portatili affidati in uso;
   - la lettura e la registrazione dei caratteri inseriti tramite tastiera o analogo dispositivo.

4. L'attività di controllo e monitoraggio è svolta dal Servizio Sistemi Informativi e deve essere mirata all'area di rischio, tenendo conto del Codice della Privacy, dello Statuto dei lavoratori e del principio della segretezza.

5. Le attività di navigazione nella rete Internet e della posta elettronica vengono automaticamente registrate in forma elettronica attraverso i log file di sistema. Il trattamento dei dati contenuti nei log avviene secondo le prescrizioni di legge.

6. In caso di un uso non corretto o anomalo delle risorse assegnate ai dipendenti (personal computer, e-mail, telefono), tali da arrecare disservizi o danni alla rete informatica (fonia/dati) dell'Ente o danni (fisici o morali) all'Ente o ad altre persone, il Servizio Sistemi Informativi potrà effettuare un controllo preliminare e anonimo, su dati aggregati riferiti all'intero Ente o a sue articolazioni (servizi/uffici) in modo da individuare la causa dell'anomalia. Il controllo anonimo potrà concludersi con un avviso generalizzato relativo all'utilizzo anomalo delle risorse dell'Ente e con l'invito ad attenersi scrupolosamente ai compiti assegnati ed alle istruzioni impartite. L'avviso potrà essere circoscritto agli utenti afferenti al servizio/ufficio in cui sia stata rilevata l'anomalia. In presenza di successive anomalie verranno eseguiti controlli su base individuale. Non sono ammissibili controlli prolungati, costanti e indiscriminati.
   Al fine di specificare meglio cosa si intende per uso anomalo o non corretto delle risorse informatiche si enuncia di seguito a titolo esemplificativo, ma non esaustivo, il seguente elenco di attività vietate:
   - creare, trasmettere o scaricare volontariamente, e-mail contenenti messaggi, immagini, dati o materiale offensivo, diffamatorio, osceno, discriminante o che comunque violino i diritti assoluti della persona e della dignità umana;
   - installare sulla stazione di lavoro software, anche se gratuiti (freeware o shareware) non espressamente autorizzati dall'Ente;
   - usare dispositivi removibili (CD, dvd, hard disk, floppy etc.) per alterare la procedura di avvio del dispositivo ed in particolare per effettuare l'avvio di un sistema operativo diverso da quello fornito dall'Ente;
   - scaricare e/o usare materiale informatico il cui contenuto (software, testo, audio e video) sia coperto da diritto di autore;
   - navigare in internet su siti contrari a norme di legge;
   - utilizzare qualunque tipo di sistema informatico o elettronico per controllare le attività di altri utenti, per leggere, copiare o cancellare file e software di altri utenti;

- utilizzare software visualizzatori di pacchetti TCP/IP (sniffer), software di intercettazione di tastiera (keygrabber o keylogger), software di decodifica password (cracker) e più in generale software rivolti alla violazione della sicurezza del sistema e della privacy;
- usare l'anonimato o servirsi di risorse che consentano di restare anonimi o alterare la propria identità;
- qualunque attività (installazione di software, navigazione su internet, collegamento con dispositivi removibili, etc.) che possano introdurre, all'interno della rete informatica dell'Ente, virus, malware, spyware e/o qualunque altro tipo di software dannoso per la sicurezza informatica della rete;
- utilizzo del telefono per usi offensivi, diffamatori, osceni, o che comunque violino le norme di legge.

7. I dati elementari contenuti nei file di log relativi alla navigazione nella rete Internet, alla posta elettronica e ai sistemi telefonici, in ottemperanza a quanto previsto nel provvedimento del 24/07/2008 del Garante per la protezione dei dati personali, vengono conservati per un periodo di 6 mesi esclusivamente per il perseguimento di finalità organizzative, produttive, statistiche e di sicurezza. Al trascorrere dei suddetti 6 mesi, tali informazioni verranno automaticamente cancellate dal sistema stesso attraverso procedure di sovraregistrazione (es. rotazione dei *file di log*).
   La deroga al prolungamento dei tempi di conservazione dei dati (ventiquattro mesi per il traffico telefonico e dodici mesi per quello telematico, ex art. 132 del Codice privacy), è consentita solo per finalità giudiziarie segnalate dalle stesse autorità entro i tempi normali di conservazione (6 mesi).
   L'accesso ai dati relativi al traffico deve essere obbligatoriamente blindato con adeguate misure di sicurezza *(strong authentication)* e sarà registrato automaticamente su un apposito registro telematico degli accessi.
   E' prevista la monitorizzazione degli accessi dei controlli da parte degli amministratori di sistema su apposito registro che a richiesta delle OO.SS. e delle RSU può essere visionato, previa autorizzazione del Segretario/Direttore Generale".La conservazione dei *file di log* di accesso a Internet è garantita in formato crittografato. La chiave di decrittazione è custodita dal Segretario Generale.

ART. 14 - CESSAZIONE DEL SERVIZIO DI ACCESSO ALLA RETE INTRANET E INTERNET

1. Ai sensi del presente regolamento, l'utilizzo del servizio di accesso alla rete Intranet e Internet cessa nei seguenti casi:
   - se non sussiste più la condizione di dipendente o di collaboratore autorizzato all'uso;
   - se è accertato un uso non corretto del servizio da parte dell'utente:
   - in caso di manomissioni e/o interventi sull'hardware e/o sul software in uso all'utente e impiegati per la connessione;
   - in caso di accesso dell'utente a siti e/o servizi vietati;
   - in caso di concessione di accesso ad internet a qualsiasi titolo da parte dell'utente a terzi;
   - su richiesta motivata del dirigente;
   - in caso di procedimento disciplinare e/o penale;
   - in ogni altro caso in cui sussistono ragionevoli evidenze di una violazione degli obblighi dell'utente o comunque problematiche di sicurezza del sistema informatico.

ART. 15 - UTILIZZO DEI SERVIZI E DEGLI APPARECCHI TELEFONICI

1. Fermo restando il rispetto dei principi e dei doveri di cui all'art. 3, l'utilizzo delle utenze telefoniche di servizio per scopi personali è consentito solo in caso di improrogabili esigenze private (vedi anche norme deontologiche Deliberazione Commissariale n. 171 del 09/12/2013).
2. Al fine di garantire un corretto utilizzo dei servizi di telefonia VoIP l'Ente predispone, ove tecnicamente possibile, adeguate profilazioni che consentano l'effettuazione o meno delle diverse tipologie di chiamata (es. chiamate su telefonini, internazionali etc.).
3. Nella categoria dei telefoni "fissi" di cui al comma 1 sono compresi anche i dispositivi "voice over IP" (ad esempio gli "IP telefoni").
4. Accesso ai dati trattati dall'utente.
   Per motivi di sicurezza del sistema telefonico, per motivi tecnici e/o manutentivi (ad esempio, aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, etc.) o per finalità di controllo e programmazione dei costi aziendali (ad esempio, verifica costi di traffico telefonico, tipologia di consumi, statistiche, etc.), comunque estranei a qualsiasi finalità di controllo dell'attività lavorativa, è facoltà del Segretario Generale, tramite l'Amministratore del Sistema, accedere direttamente, nel rispetto della normativa sulla privacy, a tutti gli strumenti di telecomunicazione aziendali, nonché ai tabulati del traffico telefonico. Per motivi di privacy le ultime tre cifre delle numerazioni sono oscurate.
5. Modalità dei controlli sull'utilizzo delle strumentazioni telefoniche.
   Il controllo sull'utilizzo delle strumentazioni telefoniche è di tre tipologie e viene effettuato, in forma anonima, come di seguito indicato:

   a) Controllo puntuale.

      Il controllo puntuale è effettuato su utenze telefoniche determinate, a seguito di specifica segnalazione effettuata da un soggetto terzo e su autorizzazione specifica del titolare del trattamento dei dati. Si considera terzo anche l'operatore telefonico, e l'utilizzatore nominale (prevalente) della linea o del singolo numero interno in questione. Nel caso in cui la segnalazione del soggetto terzo si riferisca a una persona nominativamente individuata, la struttura competente all'effettuazione dei controlli deve dare informazione del controllo in corso al soggetto cui si riferisce la segnalazione, specificando che può essere presentata richiesta di accesso ai relativi documenti amministrativi a norma della Legge n. 241/1990 e ss. mod. e int.

   b) Controllo a seguito di reportistica di utilizzo e spesa.

      Le anomalie che possono emergere sono, per ciascuna aggregazione di utenti:

      - scostamenti significativi, in percentuale, sulla durata e tipologia di traffico fra differenti aggregazioni;
      - scostamenti significativi, in percentuale, sulla durata e tipologia di traffico fra periodi differenti, a fronte della medesima aggregazione;
      - tipologia di servizi telefonici fruiti difformi dai servizi previsti per il normale svolgimento dell'attività lavorativa.

   c) Controllo a seguito di "*screening generale*" dei dati aggregati in presenza di evidenti anomalie.

      Suddetta tipologia di controllo viene attivata a seguito di un esame di carattere generale, in corrispondenza del processo di copiatura dei dati aggregati forniti dall'operatore telefonico tramite portale web o supporto cartaceo nel computer degli

incaricati del trattamento dei dati, o in fase di verifica fattura, e in cui emerga una palese e immediata anomalia nei volumi o costi complessivi del traffico telefonico. Le anomalie che possono emergere, per ciascuna linea singola o impianto di centralino, sono:

- tipologia di chiamate o di servizi utilizzati palesemente anomale;
- costi aggiuntivi, noleggi o servizi non corrispondenti agli ordinativi concordati;
- durata delle telefonate a direttrice fisso-mobile superiore al 30% della durata complessiva a direttrice fisso-fisso (locali + interurbane);
- variazioni inattese di tipologia e volume di traffico delle utenze utilizzate per strumentazione, fax e altri strumenti di connettività, rispetto alla tipologia di servizio previsto e ai valori medi dei 6 bimestri precedenti.

ART. 16 - DISPOSIZIONI AGGIUNTIVE PER LA TELEFONIA MOBILE

1. Fermo restando il rispetto dei principi e dei doveri di cui all'art. 3, l'utilizzo delle utenze di telefonia mobile per scopi personali è consentito solo in caso di urgenza, a fronte di occasionali ed improrogabili esigenze private.
2. E' fatto assoluto divieto di cessione ai terzi degli apparecchi e delle SIM.
3. Se le condizioni tecniche lo consentono, i cellulari di servizio assegnati agli utenti devono risultare attivi e raggiungibili quando essi sono in attività di servizio.

ART. 17 - SANZIONI

1. Il mancato rispetto o la violazione delle regole contenute nel presente regolamento è perseguibile con provvedimenti disciplinari nonché con le azioni civili e penali consentite.
2. Il presente regolamento sarà adeguatamente pubblicizzato, attraverso la rete interna, nei confronti di ciascun utilizzatore.
3. L'utente, nell'utilizzo delle risorse informatiche, deve attenersi, oltre alle disposizioni del Codice disciplinare contenuto nei contratti collettivi di comparto, anche ai principi e ai doveri stabiliti nel "Codice di comportamento dei dipendenti delle pubbliche amministrazioni".
4. La non osservanza dei principi e delle norme contenute nel presente regolamento costituisce violazione degli obblighi e dei doveri del dipendente pubblico e, pertanto, in relazione alla gravità dell'infrazione, l'Ente potrà attivare il procedimento disciplinare secondo la normativa vigente per il personale o per l'area dirigenza del comparto Regioni ed Autonomie Locali , nonché tutte le azioni civili e penali previste per legge.

ART. 18 - MODIFICHE ED INTEGRAZIONI

1. Il presente regolamento potrà essere soggetto a revisioni periodiche, anche su eventuale proposta delle organizzazioni di rappresentanza dei lavoratori e dalle RSU.

ART. 19 - ENTRATA IN VIGORE E PUBBLICITA'

1. Il regolamento entra in vigore con l'avvenuta esecutività della Deliberazione di approvazione e dopo la pubblicazione all'Albo Pretorio;
2. Con l'entrata in vigore del presente regolamento tutte le eventuali disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi abrogate e sostituite dalle presenti;
3. Copia del regolamento è pubblicata sul sito ufficiale dell'Ente, nelle sezioni "Albo Pretorio" e "Regolamenti" e nella rete Intranet per la massima diffusione;

NOTA INFORMATIVA AI SENSI DELL'ART. 13 DEL D.LGS N. 196 DEL 30/06/2003

Ai sensi dell'art. 13 del D.lgs n. 196 del 30 giugno 2003 si informa che, con riferimento al presente regolamento relativo all'utilizzo della rete internet, dei servizi telefonici e della posta elettronica nel rapporto di lavoro, il trattamento dei dati avverrà nel rispetto delle seguenti disposizioni:

a) Oggetto del trattamento: informazioni relative all'utilizzo della rete Internet, della posta elettronica e dei servizi telefonici, contenute nei file di log;

b) Finalità del trattamento: verifica del corretto utilizzo di Internet, della posta elettronica e dei servizi telefonici, a garanzia della disponibilità ed integrità dei sistemi informativi nonché della sicurezza sul lavoro;

c) Modalità del trattamento: informatizzato, effettuato da soggetti autorizzati all'assolvimento di tali compiti, edotti dei vincoli imposti dal decreto legislativo n. 196/2003 e con misure atte a garantire la riservatezza dei dati ed evitare l'accesso ai dati stessi da parte di soggetti terzi non autorizzati;

d) Obbligatorietà del conferimento dati: in quanto indispensabile per l'assolvimento degli obblighi di cui sopra; pertanto, l'opposizione al trattamento potrebbe comportare l'impossibilità di prosecuzione del rapporto;

e) E' Suo diritto (art. 9, comma 2. D.lgs. 196/2003), anche mediante terza persona fisica, ente, associazione od organismo cui abbia conferito delega o procura, conoscere i dati che La riguardano ed intervenire circa il loro trattamento ai sensi di quanto previsto dall'articolo 7 del citato decreto legislativo. L'unità organizzativa alla quale rivolgersi per esercitare i propri diritti è il Servizio Sistemi Informativi;

f) TITOLARE del trattamento è il Legale Rappresentante dell'Ente;

g) RESPONSABILE del trattamento dei dati è il Dirigente del Servizio Sistemi Informativi;

h) INCARICATO/I del trattamento il/i dipendente/i o eventuali collaboratori esterni del Servizio Sistemi Informativi, autorizzato/i dal responsabile a compiere le operazioni di trattamento di dati, attenendosi alle istruzioni impartite dal titolare e dal responsabile. La designazione è effettuata per iscritto e individua puntualmente l'ambito del trattamento consentito;

i) La pubblicazione delle condizioni contenute nel presente regolamento costituiscono l'informativa da parte dell'utente alla raccolta ed al trattamento dei dati;

j) I dati personali inerenti i dipendenti non possono essere portati a conoscenza di terzi non autorizzati. I colleghi di lavoro della persona interessata sono considerati terzi.

FIGURE COINVOLTE:

Provincia Regionale di Catania denominata "Libero Consorzio Comunale" ai sensi della L.R. n. 8/2014: Datore di Lavoro e "Titolare";

Segretario Generale: Responsabile della Trasparenza ed Anticorruzione e detentore della "Chiave Crittografata";

Dirigente del Servizio Informatica: Responsabile del trattamento dei dati dei file di log e responsabile della nomina degli Amministratori di Sistema e di Dominio;

Amministratore di Sistema, con il compito della "gestione" della rete Lan sovrintendendo alle risorse dei Sistemi Operativi degli elaboratori (Sala Ced) e dei Sistemi di DataBase. Può accedere in modo privilegiato alle risorse del sistema telematico/informativo per lo svolgimento della propria mansione;

***Amministratori di Dominio PRVCT**,* con il compito di:

- accedere alle risorse di rete (P.C.) sia in locale che da "remoto" ai fini di assistenza tecnica;
- accedere a tutti i dati degli Utenti, sia a quelli delle cartelle condivise di ogni Servizio, ubicati nell'*Areadir* dello Storage, sia a quelli all'interno delle cartelle personali collocati sulla *Homedir* di ogni singolo Utente;
- attivare nuovi Utenti di Dominio;
- annettere a Dominio nuovi PC e nuove stampanti di rete;
- installare software applicati sui p.c. della Rete annessi a Dominio;

Utenti del Dominio sono tutti gli utenti della rete (Dipendenti, Amministratori, etc…) che hanno diritto di accesso ai servizi di rete;

Proxy Common Access Control List (ACL)

Target Categories

[CustomWhitelist]	access	whitelist
[CustomBlacklist]	access	deny
[blk_BL_adv]	access	allow
[blk_BL_aggressive]	access	deny
[blk_BL_alcohol]	access	deny
[blk_BL_anonvpn]	access	deny
[blk_BL_automobile_bikes]	access	allow
[blk_BL_automobile_boats]	access	allow
[blk_BL_automobile_cars]	access	allow
[blk_BL_automobile_planes]	access	allow
[blk_BL_chat]	access	deny
[blk_BL_costtraps]	access	deny
[blk_BL_dating]	access	deny
[blk_BL_downloads]	access	deny
[blk_BL_drugs]	access	deny
[blk_BL_dynamic]	access	allow
[blk_BL_education_schools]	access	allow
[blk_BL_finance_banking]	access	allow
[blk_BL_finance_insurance]	access	allow
[blk_BL_finance_moneylending]	access	allow
[blk_BL_finance_other]	access	allow
[blk_BL_finance_realestate]	access	allow
[blk_BL_finance_trading]	access	allow
[blk_BL_fortunetelling]	access	deny
[blk_BL_forum]	access	allow
[blk_BL_gamble]	access	deny
[blk_BL_government]	access	allow
[blk_BL_hacking]	access	deny
[blk_BL_hobby_cooking]	access	allow
[blk_BL_hobby_games-misc]	access	deny
[blk_BL_hobby_games-online]	access	deny
[blk_BL_hobby_gardening]	access	allow
[blk_BL_hobby_pets]	access	allow
[blk_BL_homestyle]	access	allow
[blk_BL_hospitals]	access	allow
[blk_BL_imagehosting]	access	allow
[blk_BL_isp]	access	allow
[blk_BL_jobsearch]	access	allow
[blk_BL_library]	access	allow
[blk_BL_military]	access	deny
[blk_BL_models]	access	allow
[blk_BL_movies]	access	deny
[blk_BL_music]	access	allow
[blk_BL_news]	access	allow
[blk_BL_podcasts]	access	allow
[blk_BL_politics]	access	allow
[blk_BL_porn]	access	deny
[blk_BL_radiotv]	access	allow
[blk_BL_recreation_humor]	access	allow
[blk_BL_recreation_martialarts]	access	deny
[blk_BL_recreation_restaurants]	access	allow
[blk_BL_recreation_sports]	access	allow
[blk_BL_recreation_travel]	access	allow

Proxy Common Access Control List (ACL)

Target Categories

[blk_BL_recreation_wellness]	access	allow
[blk_BL_redirector]	access	allow
[blk_BL_religion]	access	allow
[blk_BL_remotecontrol]	access	deny
[blk_BL_ringtones]	access	deny
[blk_BL_science_astronomy]	access	allow
[blk_BL_science_chemistry]	access	allow
[blk_BL_searchengines]	access	allow
[blk_BL_sex_education]	access	deny
[blk_BL_sex_lingerie]	access	deny
[blk_BL_shopping]	access	allow
[blk_BL_socialnet]	access	deny
[blk_BL_spyware]	access	deny
[blk_BL_tracker]	access	allow
[blk_BL_updatesites]	access	allow
[blk_BL_urlshortener]	access	allow
[blk_BL_weapons]	access	deny
[blk_BL_webmail]	access	allow
[blk_BL_webphone]	access	deny
[blk_BL_webradio]	access	allow
[blk_BL_webtv]	access	allow
Default access [all]	access	allow