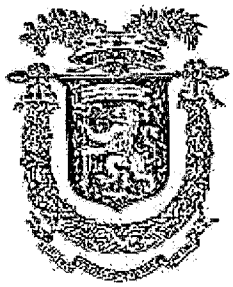
CITTÀ METROPOLITANA DI MESSINA



Regolamento per l'utilizzo dei servizi e delle attrezzature informatiche

a cura dei Servizi Informatici

1

Art.1 - Oggetto e ambito di applicazione

Il presente Regolamento contiene le disposizioni riguardanti il corretto modo d'uso della rete informatica della Città Metropolitana di Messina e di tutte le risorse informatiche, in conformità e nel rispetto di quanto previsto dalla specifica normativa di settore e dalle ulteriori disposizioni previste dall'Ente.

Esso attiene tutti i servizi e gli apparati di proprietà dell'Ente concessi nella disponibilità degli utenti per l'ordinario svolgimento delle proprie prestazioni lavorative, identificabili prevalentemente nelle seguenti unità: computer, stampanti, apparati mobili, apparati rimovibili, sistemi d'identificazione e autenticazione informatica, Internet, Intranet, strumenti di scambio file, posta elettronica e qualsiasi altro programma/apparecchiatura informatica destinata a memorizzare o a trasmettere dati e informazioni.

L'applicazione e il rispetto puntuale delle disposizioni contenute nel presente Regolamento rientra nelle responsabilità di tutti i soggetti che utilizzano gli strumenti informatici messi a disposizione dall'Ente. Ferme restando le disposizioni normative in materia e tutte le prescrizioni previste per il trattamento dei dati sensibili, il suo contenuto costituisce disposizione di servizio ed è indirizzato a tutti gli utilizzatori del sistema informatico dell'Ente, senza distinzione di ruolo o livello, ivi compresi gli amministratori.

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

Art. 2 – Assegnazione e Gestione delle credenziali di autenticazione

Le credenziali necessarie all'autenticazione degli utenti per l'accesso alla rete dell'Ente sono attribuite dagli Amministratori di Sistema, e sono costituite da un codice di identificazione utente (username) associato a una password che dovrà essere personalizzata al primo accesso. Quest'ultima dovrà essere custodita con la massima diligenza, preservata dalla conoscibilità di colleghi o soggetti esterni all'Ente e modificata periodicamente. E' consigliabile utilizzare password lunghe almeno 8 caratteri, formate da combinazioni di lettere maiuscole, minuscole, cifre numeriche e anche segni speciali, ed evitare di annotarle in chiaro sia su supporti cartacei che informatici.

Art. 3 – Utilizzo delle risorse di sistema

L'accesso alla rete dell'Ente avviene per mezzo delle credenziali di cui al precedente articolo. E' fatto assoluto divieto utilizzare credenziali diverse dalle proprie.

Nei server del sistema dell'Ente sono allocate anche aree di dati (cartelle) create per essere condivise dagli utenti che ne fanno richiesta. Queste sono soggette a operazioni di controllo, amministrazione e back up da parte del personale dei Servizi Informatici. Tali aree, pertanto, devono essere utilizzate per memorizzare informazioni inerenti esclusivamente attività d'ufficio, per cui non è consentito, nemmeno per brevi periodi di tempo, memorizzare dati personali ovvero non legati a competenze istituzionali. E' opportuno, infine, che periodicamente gli utenti provvedano a razionalizzare gli archivi, cancellando i file inutili e/o obsoleti, prestando attenzione nel contempo alla duplicazione dei dati per evitarne inutile ridondanza e magari difformità di versione dei file stessi.

Il personale dei Sistemi Informatici può in qualunque momento procedere alla cancellazione di file e applicazioni sia sui PC che sulle altre unità di rete, ritenuti pericolosi ai fini della sicurezza del sistema.

Art. 4 – Utilizzo del Personal Computer

Il Personal Computer affidato all'utente è uno strumento di lavoro. Ogni utilizzo estraneo all'attività lavorativa può contribuire a innescare disservizi, guasti con conseguenti costi di assistenza e, soprattutto minacce alla sicurezza dell'intera rete. Il Personal Computer deve essere quindi custodito con la massima cura evitando ogni possibile forma di danneggiamento.

Il personale dei Servizi Informatici, su richiesta dell'utente, o in caso di oggettiva necessità derivante dal monitoraggio automatico della rete, può collegarsi in modalità remota per garantire interventi di assistenza operativa, nonché interventi relativi alla sicurezza per scongiurare i danni derivanti da intrusioni di virus, spyware, malware, ecc.

Non è consentito installare e/o utilizzare programmi diversi da quelli ufficialmente forniti, sussistendo il grave pericolo di introdurre virus, ovvero alterare funzionalità del software installato. Inoltre si ritiene utile ricordare che l'utilizzo di software non licenziato o comunque protetto da diritti d'autore viola la normativa a tutela dei diritti d'autore, esponendo l'utente a responsabilità sanzionate anche penalmente.

Non è inoltre consentito, salvo preventiva autorizzazione da parte dei Servizi Informatici, modificare la configurazione del Personal Computer, né installare dispositivi esterni di memorizzazione e/o comunicazione (hard disk, router, modem, internet key, ecc.) .

E' necessario prestare la massima attenzione ai supporti di origine esterna (pendrive), avvertendo immediatamente i Servizi Informatici nel caso in cui vengano rilevati virus.

Infine il Personal Computer deve essere sempre spento alla fine dell'orario di lavoro o in casi di prolungata assenza dal posto di lavoro, al fine di evitare che possa essere utilizzato da terzi senza che vi sia la possibilità di provarne, nel caso, l'indebito uso.

Art. 5 – Utilizzo di Internet

E' fatto divieto memorizzare (download) dalla rete documenti, file o dati comunque non pertinenti lo svolgimento delle attività istituzionali, e in particolare:

a) non è consentito navigare in siti non attinenti allo svolgimento delle mansioni assegnate;

b) non è consentita l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti online e simili.

c) è vietata ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa;

d) non è permessa la partecipazione, per motivi non professionali, a Forum, l'utilizzo di chat line, bacheche elettroniche e le registrazioni in guest book, utilizzando anche pseudonimi (nicknames), onde evitare di esporre a rischi di sicurezza la rete dell'Ente.

Si rende noto che il sistema dell'Ente è dotato di filtri idonei a evitare navigazioni in siti non correlati all'attività lavorativa, per cui esistono black-list create in relazione ai parametri ritenuti più idonei, soggette a continuo aggiornamento.

Inoltre a ciò si affiancano sistemi attivi di monitoraggio della navigazione, che effettuano un monitoraggio generalizzato e anonimo dei log di connessione.

Gli archivi di log risultanti da questo monitoraggio contengono traccia di ogni operazione di collegamento effettuata dall'interno della rete dell'Ente verso Internet, sempre a disposizione per eventuali richieste da parte dell'Autorità Giudiziaria.

Eventuali attivazioni di controlli specifici saranno preventivamente notificate.

Art. 6 – Utilizzo della posta elettronica

Le caselle di posta elettronica date in uso al dipendente sono destinate esclusivamente all'uso d'ufficio.

Si rammenta che:

a) non è consentito inviare o memorizzare messaggi (interni ed esterni) di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica, o che costituiscano comunque condotta illecita;

b) non è consentito l'utilizzo dell'indirizzo di posta elettronica aziendale per la partecipazione a dibattiti, Forum, newsletter o mail-list, non attinenti l'attività lavorativa;

c) è fatto divieto di divulgare le notizie, i dati e qualsiasi altra informazione appresa in occasione della ricezione o invio di posta elettronica, in quanto coperte dal segreto professionale cui sono tenuti i dipendenti in ottemperanza agli obblighi di fedeltà e correttezza;

d) la posta elettronica diretta all'esterno della rete informatica aziendale può essere intercettata da estranei e, dunque, è preferibile non usarla per inviare documenti di lavoro "Strettamente Riservati".

Infine si raccomanda di non fornire mai le proprie credenziali e soprattutto la password in risposta a eventuali messaggi apparentemente innocui o comunque falsamente attribuibili a siti di istituzioni bancarie, governative, ecc. perché quasi sicuramente sono da annettersi a tentativi di *phishing,* che potrebbero innescare intrusioni di virus, malware o produrre enormi quantitativi di *spamming,* tali da procurare gravi danni o addirittura blocco del sistema.

Sanzioni

Gli utenti sono direttamente responsabili sia civilmente, sia penalmente, a norma delle leggi vigenti, per l'uso improprio fatto dei servizi di rete e della posta elettronica.

L'Amministrazione si riserva la facoltà di denunciare l'utente alle autorità competenti per le attività illecite compiute durante l'attività lavorativa o con i mezzi messi a disposizione dall'Amministrazione.

Per comportamenti non conformi al presente regolamento, l'Amministrazione può richiedere al Responsabile dei Sistemi Informativi di limitare o annullare i privilegi concessi al singolo utente.

L'utente è tenuto a risarcire l'Amministrazione per danni prodotti alle apparecchiature o alla rete in violazione alle norme vigenti e/o in violazione al presente regolamento.

Applicazione e interpretazione del presente regolamento

Per qualsiasi dubbio relativo all'applicazione pratica o all'interpretazione del presente regolamento, tutti gli utenti possono rivolgersi al Responsabile del Servizio Sistemi Informativi della Città Metropolitana di Messina.