Città
metropolitana
di Milano

Disciplinare per l'utilizzo dei servizi informatici e di comunicazione telematica

Milano, 15 dicembre 2023

PREMESSA

Il Sistema Informativo rappresenta una componente vitale per l'operatività della Città Metropolitana di Milano, che promuove attivamente tutti gli interventi tecnologici, procedurali e organizzativi atti a mantenere un adeguato livello di sicurezza dell'infrastruttura e dei servizi nel costante rispetto delle normative in materia.

Le complesse attività volte al raggiungimento di tale obiettivo richiedono una continua evoluzione tecnologica e la collaborazione di tutti i soggetti coinvolti.

Un utilizzo consapevole degli strumenti informatici rappresenta una condizione imprescindibile e un obiettivo prioritario da perseguire.

A tal fine, viene individuato l'insieme di regole atte a definire il corretto comportamento da tenere nell'utilizzo dei dispositivi e dei servizi messi a disposizione degli utenti dalla Città Metropolitana di Milano, garantendo la conformità dei sistemi informativi ai requisiti di sicurezza ed alle vigenti normative sulla tutela della privacy.

Art. 1 - Oggetto

Il presente disciplinare ha per oggetto i criteri e le modalità operative di accesso e di utilizzo dei servizi informatici e telematici (servizio Intranet, Internet e posta elettronica) da parte degli utenti che utilizzano tali servizi.

Destinatari del presente disciplinare sono i dipendenti, collaboratori e tutti gli utilizzatori che, a vario titolo, nello svolgimento della propria attività, ricorrono ai servizi informatici e telematici forniti dalla Città Metropolitana di Milano.

Il presente disciplinare non disciplina strumenti e servizi che la Città Metropolitana di Milano mette a disposizione dell'utenza esterna. In tali casi il settore richiedente è responsabile dell'osservazione delle norme di legge in materia.

Art. 2 - Riferimenti normativi, adozione e pubblicità

Il presente disciplinare è adottato ai sensi del:

- D.lgs. 196 del 30 giugno 2003 (Codice in materia di protezione dei dati personali - Allegato B);
- D.lgs. 82 del 7 marzo 2005 (Codice dell'amministrazione digitale);
- Provvedimento 1° marzo 2007 del Garante per la protezione dei dati personali (Linee Guida sull'uso di posta elettronica e internet nei rapporti di lavoro). In particolare, questo Provvedimento costituisce il disciplinare d'uso di internet e della posta elettronica nei rapporti di lavoro ed è adottato dalla Città Metropolitana con le modalità prescritte per i regolamenti sull'ordinamento degli uffici e dei servizi.
- Regolamento (UE) 2016/679 (*General Data Protection Regulation*)
- Circolare n. 1 del 17 marzo 2017 (Misure minime di sicurezza ICT per le pubbliche amministrazioni; Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015);

- Piano Triennale per l'informatica nella Pubblica Amministrazione 2022-2024;
- DPR nr. 81 del 13.06.2023 (Codice di comportamento dei dipendenti della Pubblica Amministrazione, con specifico riferimento alle nuove norme riguardanti l'utilizzo delle tecnologie informatiche, dei mezzi di informazione e dei social media).

L'allegato tecnico al presente disciplinare, limitandosi a descrivere aspetti tecnici relativi ai sistemi informatici e di comunicazione telematica, viene aggiornato dal Dipartimento Transizione digitale mediante atto dirigenziale.

Di tale disciplinare, dell'allegato tecnico e relativi aggiornamenti si dà adeguata diffusione tra i destinatari, anche attraverso la rete intranet.

Art. 3 - Uso degli strumenti e dei servizi informatici - modalità di accesso e norme di comportamento

L'uso degli strumenti e dei servizi informatici è indispensabile per assicurare l'efficienza e l'efficacia della Pubblica Amministrazione.

Gli strumenti ed i servizi sono in continua evoluzione ed adeguamento e fanno parte delle risorse che l'Ente mette a disposizione per fornire un adeguato livello di servizi al cittadino.

Gli utenti sono tenuti a mantenere in buono stato gli strumenti e ad osservare le seguenti norme di utilizzo dei servizi. Il Dipartimento Transizione digitale, al fine di garantire la sicurezza del sistema, si riserva di sospendere temporaneamente i servizi informatici per effettuare accertamenti e controlli.

Per accedere ai servizi informatici da una postazione di lavoro l'utente è tenuto ad autenticarsi utilizzando un codice identificativo (userid) e una parola chiave segreta (password) che sono rilasciati dal Dipartimento Transizione digitale.

Poiché la conoscenza della password può consentire indebitamente a terzi l'accesso alla rete della Città Metropolitana in nome dell'utente titolare e l'accesso ai dati cui il medesimo è abilitato (ad es. visualizzazione di informazioni riservate, distruzione o modifica dei dati, lettura della posta elettronica, ecc.), ogni utente è tenuto ad attenersi alle seguenti indicazioni:

Buone norme

- Conservare la propria password con riservatezza e diligenza non cedendola a terzi;
- Cambiare con periodicità la propria password (ogni sei mesi o tre mesi nel caso si gestiscano dati sensibili e/o giudiziari);
- Non utilizzare credenziali (userid e password) di altri utenti, nemmeno se fornite volontariamente o di cui si ha casualmente conoscenza;
- Non cedere, una volta superata la fase di autenticazione, l'uso della propria postazione ad altre persone senza la propria supervisione;
- Non lasciare incustodita ed accessibile la propria postazione una volta connesso al sistema con le proprie credenziali di autenticazione;
- Utilizzare per il proprio lavoro soltanto componenti hardware e software autorizzati dall'Ente e/o di proprietà dell'Ente;

- Prendere tutte le precauzioni necessarie a prevenire l'accesso ai dati salvati in locale sulla postazione di lavoro da parte di persone non autorizzate. L'utente è infatti responsabile di tali dati;
- Salvare periodicamente i dati importanti residenti sul proprio personal computer per evitare spiacevoli inconvenienti, come la perdita dei file causata da guasti hardware o da cancellazione involontaria.

Divieti

- Non è consentito l'utilizzo degli strumenti e dei servizi informatici per attività non connesse allo svolgimento delle mansioni lavorative assegnate;
- Non è consentito dalla propria postazione di lavoro disinstallare o disattivare sistemi di protezione o aggirare politiche di sicurezza distribuite dal Dipartimento Transizione digitale.

Art. 4 - Uso dei servizi di comunicazione telematica

Internet, intranet, posta elettronica, ecc. sono strumenti di comunicazione telematica fondamentali per assicurare l'efficienza e l'efficacia della Pubblica Amministrazione. L'impegno della Città Metropolitana di Milano è di svilupparne l'uso per migliorare la qualità e la tempestività della comunicazione sia all'interno dell'Ente che con gli interlocutori esterni.

A questo scopo la Città Metropolitana di Milano provvede a dotare tutti i dipendenti di un'utenza per l'accesso ai servizi di posta elettronica ed alla intranet.

L'accesso alla rete Internet deve invece essere richiesto dal direttore al quale l'utente è assegnato. Lo stesso direttore è tenuto a comunicare il trasferimento o la cessazione del rapporto dell'utente con la Città Metropolitana di Milano. Tale comunicazione determina la disabilitazione dai servizi.

L'accesso alla rete Internet è attivato automaticamente ai direttori.

L'accesso ai servizi di comunicazione telematica è revocato su richiesta – *motivata ed inviata per conoscenza al lavoratore, che entro 3 giorni può presentare le sue controdeduzioni al Direttore del Personale* - del direttore di riferimento o in caso di accertate violazioni della legge o del presente disciplinare.

Art 4.1 - Posta elettronica

L'uso della posta elettronica, strumento fondamentale nello svolgimento dell'attività lavorativa, deve essere adottato per quanto possibile in sostituzione delle comunicazioni cartacee per tutte le comunicazioni interne al fine di rendere più efficienti le procedure e realizzare consistenti risparmi di risorse.

Responsabilità

L'uso dell'indirizzo di posta elettronica assegnato dalla Città Metropolitana di Milano comporta la spendita del nome dell'Ente. Il materiale e i contenuti inviati sono diretta responsabilità dell'utente che deve evitare che propri comportamenti in rete possano ledere l'immagine esterna dell'Ente o ne possano comportare la responsabilità.

Occorre inoltre osservare alcune precauzioni per evitare che le mail scambiate arrechino rischi ai servizi informativi della Città Metropolitana o contribuiscano a diffondere informazioni riservate. A tale scopo ogni utente è tenuto ad attenersi alle seguenti norme:

Buone norme

- Controllare con attenzione le mail ricevute: l'ambiente di posta è in grado di identificare ed eliminare i principali virus nascosti negli allegati. Tuttavia, è possibile che qualche virus non venga intercettato ed è compito di ogni utente vigilare e cancellare ogni e-mail con mittenti, link o allegati sospetti specialmente se non se ne conosce la provenienza;

Effettuare la manutenzione della casella di posta eliminando i messaggi non più attuali e contenenti allegati di grandi dimensioni e archiviando i messaggi di posta dalla casella alla propria postazione di lavoro; ciò eviterà rischi di sovraccarichi che limitano le prestazioni del sistema di posta elettronica;

- In caso di assenze prolungate attivare un messaggio automatico che indichi il periodo di assenza ed eventualmente un altro riferimento al quale inviare i messaggi di lavoro urgenti;
- l'utente evita che, nei messaggi inviati a destinatari esterni all'Ente, siano visibili in chiaro liste di indirizzi mail di utenti della Città Metropolitana di Milano
- Impostare la firma delle mail, utilizzando format di firma e disclaimer standard definiti dall'Ente

Divieti

- Sono vietate pratiche di "spamming", cioè di invio e diffusione di grandi quantità di messaggi indesiderati (messaggi a catena, inserimento di utente e password nei messaggi, ecc.). L'inoltro di messaggi non sollecitati (ad esempio informazioni, avvisi, notizie etc.) deve essere attentamente valutato;
- E' vietato l'invio di e-mail con allegati di grosse dimensioni o a un numero elevato di destinatari perché ciò può compromettere il corretto funzionamento del servizio.

Art. 4.2 - Internet

La Città Metropolitana di Milano fornisce accesso alla rete Internet per lo svolgimento dell'attività lavorativa. L'accesso è fornito dal Dipartimento Transizione digitale previa richiesta del direttore di riferimento di ogni utente ed è subordinato all'autenticazione dell'utente presso la rete della Città Metropolitana di Milano.

La navigazione in Internet comporta numerosi rischi che possono minacciare la sicurezza della rete della Città Metropolitana, dei dati e della postazione di lavoro. Per evitare tali rischi, l'accesso ad Internet è filtrato e controllato da adeguati apparati di sicurezza, che si aggiornano automaticamente con liste di indirizzi di siti considerati pericolosi o non correlati con la prestazione lavorativa.

Modalità di conservazione dei dati

I dati di log del servizio internet, specificati nell'allegato tecnico, sono conservati per ragioni connesse alla gestione del servizio e alla sicurezza del sistema per 12 mesi.

Un eventuale prolungamento dei tempi di conservazione è limitato ai seguenti casi:

- Per indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria. In questo caso il Dipartimento Transizione digitale si atterrà alle indicazioni della Direzione Generale;
- Per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria;
- Per eccezionali esigenze tecniche e di sicurezza che il Dipartimento Transizione digitale documenterà indicando nello specifico le ragioni del prolungamento e la sua durata.

Responsabilità

L'uso di internet, sia rispetto alla navigazione che all'utilizzo dei servizi disponibili in rete, rientra nella piena responsabilità dell'utente che, a propria tutela, tiene rigorosamente riservate le sue credenziali di accesso.

Tenendo conto che l'uso di internet è consentito per lo svolgimento della propria attività lavorativa, l'utente è tenuto al rispetto delle seguenti norme di comportamento:

Buone norme

- Per evitare problemi di efficienza e sicurezza della rete, verificare le dimensioni e la provenienza degli eventuali file (immagini, video, documenti etc.) che si intendano scaricare;
- Valutare con attenzione l'opportunità di compilare, fornendo dati personali propri e della Città Metropolitana, form o moduli disponibili in rete;
- Valutare con attenzione l'opportunità di partecipare a forum, aree di dibattito, *virtual community* presenti in rete;
- Valutare con attenzione l'opportunità di effettuare l'upload o comunque la condivisione in rete di materiale di cui si disponga per l'esercizio della propria attività lavorativa.

Divieti

- Non è consentito scaricare ed installare programmi non autorizzati che potrebbero danneggiare il sistema ricevente o carpire informazioni riservate;
- Non è consentito l'accesso e la navigazione se non a mezzo della rete della Città Metropolitana. È pertanto vietato l'utilizzo di modem personali e di Internet provider diversi, salvo i casi autorizzati dal direttore di riferimento;
- Non è consentita l'effettuazione di transazioni finanziarie (*remote Banking*, acquisti on-line, ecc.), salvo i casi autorizzati dal direttore di riferimento;
- Non è consentito scaricare/scambiare materiale informatico privo di licenza o in violazione del diritto d'autore o altri diritti tutelati dalla normativa vigente;
- È inoltre vietato compiere qualsiasi azione tesa ad aggirare o compromettere i meccanismi di protezione dei sistemi informatici (ad esempio effettuare operazioni non autorizzate di scansione di porte e protocolli dall'interno della rete dell'Ente, falsificare la propria identità, falsificare il contenuto degli *header* dei protocolli di comunicazione, trasmettere software che alteri il normale funzionamento del sistema informatico del destinatario).

Art. 5 - Monitoraggi e controlli

Al fine di garantire la sicurezza degli strumenti e dei servizi informatici e di comunicazione telematica, per effettuare statistiche e prevenire usi impropri, il Dipartimento Transizione digitale si avvale di sistemi di monitoraggio e controllo, nel rispetto dei principi di pertinenza e non eccedenza.

Postazione di lavoro

Il Dipartimento Transizione digitale verifica che le postazioni di lavoro mantengano lo standard di sicurezza definito. Il riscontro di eventuali anomalie consente al Dipartimento Transizione digitale di adottare tutte le misure necessarie, compreso l'isolamento della postazione di lavoro dalla rete della Città Metropolitana. Nel perdurare di tali anomalie il comportamento verrà segnalato al responsabile della struttura di appartenenza del dipendente e al Direttore del Personale.

Nel caso l'utilizzo anomalo sia riconducibile ad un utente non dipendente, il comportamento andrà segnalato alla Direzione Generale per l'adozione degli atti di competenza.

Posta elettronica

I contenuti dei messaggi di posta elettronica, compresi i file allegati, sono riservati. L'accesso ai messaggi e ai file allegati è ammesso solo per eccezionali e documentati problemi di sicurezza del sistema su richiesta dell'utente o previa comunicazione all'utente stesso.

Il Dipartimento Transizione digitale utilizza strumenti di monitoraggio del traffico che mettono in evidenza situazioni anomale di traffico o di carico dei sistemi che ne possano compromettere il funzionamento.

Internet

Il Dipartimento Transizione digitale verifica il corretto utilizzo della rete ai fini della sicurezza e l'attività sull'uso della rete Internet.

Su richiesta esplicita dell'utente, per lo svolgimento di attività diagnostica, può essere temporaneamente memorizzato e controllato il contenuto di una pagina consultata. Una volta effettuata la verifica, la pagina viene cancellata.

I controlli vengono effettuati su dati aggregati anche relativi a singole direzioni o settori. Qualora il controllo anonimo rilevi un utilizzo anomalo degli strumenti informatici, il Dipartimento Transizione digitale effettuerà un avviso generalizzato inerente all'utilizzo anomalo rilevato, con l'invito ad attenersi scrupolosamente alle istruzioni impartite. Nel perdurare delle anomalie si procederà a controlli su base individuale o per postazioni di lavoro segnalando il comportamento al responsabile della struttura di appartenenza del dipendente e al Direttore del Personale il quale, se necessario, attiverà il procedimento disciplinare nelle forme e con le modalità previste dal C.C.N.L.

Nel caso l'utilizzo anomalo sia riconducibile ad un utente non dipendente, il comportamento andrà segnalato alla Direzione Generale per l'adozione degli atti di competenza.

Verranno comunicati alle organizzazioni sindacali ogni anno i report e le statistiche delle modifiche/revoche degli accessi, intervenute a seguito di violazione delle norme definite nel Disciplinare di accesso relativo alla rete Internet e all'utilizzo della posta elettronica.

Allegato tecnico

Standard di sicurezza e principali misure di protezione

Dotazione informatica

Gli strumenti forniti sono di proprietà dell'Ente e devono essere utilizzati esclusivamente per svolgere la propria attività lavorativa.

Il computer assegnato contiene tutti i software necessari a svolgere le attività. Per evitare rischi di sicurezza o danni accidentali non è consentita l'installazione di programmi o la modifica di configurazioni (software e hardware) che non siano state preventivamente richieste e autorizzate dal Servizio IT.

Per evitare problemi durante la migrazione dei dati, utilizzare esclusivamente la cartella "Documenti" per salvare e organizzare i file in sottocartelle, evitare d'immagazzinare documenti personali come foto/video/musica ed effettuare pulizie periodiche eliminando file non più necessari.

Aggiornamenti e patch di sicurezza

Una delle principali cause che rendono i sistemi informatici vulnerabili agli attacchi è la mancanza di aggiornamenti che correggono importanti falle di sicurezza.

Le Postazioni di Lavoro prevedono un sistema centralizzato e automatico per la distribuzione degli aggiornamenti del sistema operativo e dei software installati.

Gli aggiornamenti del sistema operativo sono distribuiti mensilmente tramite Windows Update:

- Sui **pc portatili** l'installazione è programmata il mercoledì in pausa pranzo. L'utente è tenuto a **riavviare** il pc per completare l'aggiornamento dopo che appare la notifica di riavvio, oppure scegliere "Aggiorna e arresta" al termine dell'attività lavorativa (attenzione che in quest'ultimo caso il pc impiegherà un po' più tempo a spegnersi).
- Sui **pc fissi** gli aggiornamenti sono programmati il sabato notte, in modo completamente automatico. Per i pc spenti in tale orario l'utente è tenuto ad **avviare** manualmente l'installazione cliccando sulla notifica che indica la disponibilità di aggiornamenti e a **riavviare** poi il pc per completare l'aggiornamento una volta che appare la notifica di riavvio.

Interventi di assistenza

Ogni malfunzionamento hardware o software della dotazione informatica assegnata deve essere segnalato al servizio di Helpdesk attraverso il sistema di ticketing e l'indicazione dettagliata del problema riscontrato, seguendo una delle due procedure elencate di seguito:

- L'apertura di un ticket all'indirizzo: https://assistenza.cittametropolitana.mi.it
- L'invio di una mail all'indirizzo assistenza@cittametropolitana.mi.it

Gli interventi di assistenza possono richiedere l'accesso da remoto alla postazione di lavoro. Tale accesso può avvenire unicamente con il consenso dell'assegnatario che sta utilizzando la postazione.

Password

Indicazioni per creare una password più sicura

- Utilizzare **minimo 8 caratteri**
- Utilizzare almeno una lettera **maiuscola**, un **numero** e un **carattere speciale** ($!@&?.-#)
- Più la password è **lunga** e **complessa**, più è sicura.
- Evitare l'uso di **parole ovvie e banali** o **facilmente indovinabili** (es. il proprio nome)
- Evitare l'uso d'**informazioni personali** facilmente rintracciabili (data di nascita, nomi dei figli, nome dell'animale domestico, etc.)
- Sostituire alcune lettere di una parola con numeri o caratteri speciali graficamente riconducibili alla lettera sostituita (ad esempio la "**a**" con "**4**" o "**@**", la "**e**" con "**3**" o "**&**", la "**s**" con "**5**" o "**$**", la "**i**" con "**1**" o "**!**", la "**o**" con "**0**", etc.)

  Es. CittàMetropolitana ► *C1tt4M3tr0p0l!t4n@*
- Usare una frase facile da ricordare (come un motto, un titolo di una canzone, etc.)

  Es. LavoroInCittàMetropolitanaDiMilano
- Oppure usare in alternativa solo le iniziali della frase, seguita da numeri e caratteri speciali, in modo da avere una password non troppo lunga, ma comunque sicura perché non forma una parola di senso compiuto

  Es. Licmdm97!

Indicazioni per gestire al meglio la propria password

- **Non condividere** mai la propria password per email.
- Negare eventuali richieste di **salvataggio password** dell'utenza di Città Metropolitana (ad esempio nel browser).
- Non inserirla mai in portali che non siano quelli **ufficiali** dell'ente o tramite collegamenti contenuti in mail di dubbia provenienza (phishing).
- **Non riutilizzare** la password dell'utenza di Città Metropolitana per altri servizi e portali (es. corsi online, servizi di storage, etc.), o per account privati (es. posta personale, banca, etc.); usare sempre **password diverse** per **utenze diverse**.
- Effettuare sempre il **logout** da servizi e portali dopo aver concluso l'attività.
- **Bloccare** sempre il pc quando ci si allontana dalla postazione (CTRL+ALT+CANC ► Blocca)
- **Non scrivere** mai la propria password su foglietti, agende o in file sul pc.
- Per ricordarsi le varie password si può ricorrere a un **gestore delle password** gratuito come **KeePass**, che permette di salvare e categorizzare le proprie password tramite una sola password di accesso.
- Registrarsi sul portale **Cambio Password** per poter facilmente cambiare la propria password in caso di scadenza o dimenticanza, seguendo la semplice guida passo per passo sul portale E-learning.

Posta elettronica

Controlli automatici sullo spam

Il servizio di posta elettronica prevede specifiche misure di protezione, che, attraverso l'analisi automatica del contenuto della e-mail, identificano e-mail malevole (che contengono virus o altre tipologie di minacce). Le e-mail riconosciute dal sistema di posta come pericolose vengono automaticamente spostate nella casella "Posta indesiderata" dell'utente o vengono bloccate prima dell'ingresso in casella.

Qualsiasi sistema di posta non è però in grado di riconoscere tutte le e-mail malevole che, talvolta, vengono recapitate all'utente.

È fondamentale che ogni utente controlli con attenzione le e-mail ricevute, esaminando il mittente e allertandosi nel caso una e-mail abbia contenuti dubbi e chiedendo eventualmente supporto all'assistenza informatica.

Di seguito alcuni elementi che caratterizzano mail malevole:

1. Il mittente è un indirizzo di posta elettronica pubblico

Guardare l'indirizzo del mittente aiuta a capire se la persona che ha inviato l'e-mail è veramente colei che afferma di essere. Spesso, i criminali informatici usano un indirizzo di posta elettronica pubblico, come @gmail.com. Se si hanno dubbi sulla veridicità del messaggio, prima di aprire la e-mail o cliccare su qualsiasi link in essa contenuto, è meglio contattare direttamente il destinatario e chiedere informazioni sulla e-mail ricevuta.

2. Allegati strani

In caso di e-mail inaspettate o derivanti da qualcuno di non conosciuto, in cui si è invitati ad aprire e/o scaricare allegati apparentemente non sicuri, non aprire e/o scaricare mai l'allegato. Questo potrebbe contenere malware che infetteranno il computer, o peggio ancora, ransomware che bloccheranno il computer e i dati, prendendoli in ostaggio.

3. Senso di urgenza

Le e-mail di phishing spesso creano un falso senso di urgenza e pericolo che spinge l'ignara vittima a seguire le indicazioni contenute nel messaggio. Controllare attentamente la veridicità del messaggio prima di cliccare sui link invitati che, in caso di e-mail di phishing, non rimandano al sito autentico, ma ad uno creato ad-hoc per la truffa.

4. Errori di ortografia in un dominio conosciuto

Senza cliccarlo, passare il mouse sopra il link per visualizzare il vero URL nascosto. Spesso, le truffe replicano siti web famosi in tutto e per tutto. Non potendo però duplicare il dominio, cercano di crearne uno il più simile possibile all'originale: se si riceve una e-mail che invita a cliccare un link che cita siti web famosi (es. amazon.it o intessasanpaolo.it), probabilmente l'e-mail ricevuta è fraudolenta; pertanto, si invita a non cliccare sul link contenuto nell'e-mail.

5. Messaggio sgrammaticato

Spesso è possibile capire che si tratta di una e-mail di phishing dal modo in cui è scritto il messaggio. Lo stile potrebbe essere diverso da quello che ci si aspetta di solito dal mittente, oppure il messaggio potrebbe contenere errori grammaticali e ortografici.

Limiti di spazio delle caselle

Ogni provider di posta definisce un limite massimo di spazio per casella di posta. Lo spazio è vincolante e non può essere incrementato. Per questo motivo ogni utente deve provvedere alla cancellazione di mail non necessarie per non portare la casella a saturazione.

Sistema Antivirus

Tutte le postazioni di lavoro che hanno accesso alla rete (dominio "provmi") sono dotate di sistema antivirus per il rilevamento, segnalazione, blocco e rimozione di virus, worm, Trojan, malware e altre applicazioni pericolose o indesiderate.

La distribuzione degli aggiornamenti avviene quotidianamente ed è gestita centralmente da un server.

Una consolle centralizzata permette di monitorare tutte le attività di aggiornamento in atto e verificarne il completamento e raccoglie le segnalazioni di infezione permettendo di identificare particolari trend di crescita ed intervenire eventualmente in maniera remota su interi rami di rete.

Ogni utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico dell'Ente, evitando di compiere navigazione su siti non sicuri, download di software e file non autorizzati, etc.

Internet

Filtri

L'accesso ad Internet è regolamentato da un sistema di controllo delle pagine web visitate che permette di bloccare l'accesso a siti Web e ai file potenzialmente pericolosi e specificati mediante appositi filtri.

Accertarsi comunque sempre dell'affidabilità di qualsiasi sito prima di visitarlo e della genuinità di qualsiasi file prima di eseguirlo.

Registrazione dei dati

I sistemi di controllo e filtraggio dei siti navigati, registrano le seguenti informazioni (Log) che possono essere utilizzate dal personale IT per attività di monitoraggio:

- Nome account dell'utente
- Indirizzo IP della stazione di lavoro
- URL richiesta
- Indirizzo IP del server remoto
- Quantità dei dati trasferiti

Browser

Il browser che si raccomanda di utilizzare è **Microsoft Edge** che, oltre ad essere un browser moderno e sicuro con **aggiornamenti** automatici regolari, contiene nei preferiti una cartella "Città Metropolitana" con i **siti più utili** dell'Ente.

Inoltre, è l'unico browser che permette l'uso di applicativi progettati per Internet Explorer, grazie alla **modalità di compatibilità** già configurata.

Utilizzo delle condivisioni di rete

L'utente può accedere alle cartelle di rete del proprio settore di appartenenza, per le quali ha ricevuto le opportune **autorizzazioni**.

La **richiesta** di accesso a cartelle già esistenti o la creazione di nuove avviene tramite un **modulo** di richiesta presente sulla Intranet, firmato digitalmente dal proprio responsabile.

Tutte le cartelle di rete servono per immagazzinare esclusivamente documenti inerenti l'attività **lavorativa** in condivisione con i colleghi; pertanto, non è consentito il salvataggio di documenti personali come foto/video/musica.

Ogni cartella ha uno **spazio limitato**: è quindi importante porre attenzione all'uso dello spazio, evitando sprechi e organizzando una manutenzione periodica, eliminando dati duplicati o non più necessari.

Tutte le cartelle di rete sono soggette a **backup** giornalieri.

Nominare file e cartelle

Non creare file e cartelle con nomi **troppo lunghi** o con caratteri particolari, per evitare poi problemi nella gestione dei percorsi e nella compatibilità tra i vari sistemi e applicazioni.

Usare piuttosto nomi **corti e semplificati**, usare eventuali parole solo in forma abbreviata, evitare articoli, preposizioni, accenti, apostrofi e spazi, utilizzare il trattino "-" o il trattino basso "_" per distanziare le parole.

Utilizzo dei portatili

Il portatile assegnato è di proprietà dell'Ente e fa parte della dotazione informatica messa a disposizione esclusivamente per l'attività lavorativa, nel rispetto delle seguenti regole e nel divieto di utilizzo per scopi personali non connessi all'attività lavorativa.

Un portatile va maneggiato con cura poiché è molto più delicato di una postazione fissa e necessita di maggiore attenzione nel suo utilizzo quotidiano.

I danni causati da incuria non sono coperti dalla garanzia del fornitore e gli interventi fuori garanzia danno luogo ad addebiti extra, a carico di chi ha causato il danno.

Per evitare che si verifichino la maggior parte dei guasti e/o incidenti occorre seguire alcune semplici regole:

Prevenire i possibili incidenti

- Evitare di mangiare o bere mentre si lavora al computer per evitare danni irreversibili (ad esempio nel rovesciare bevande sul pc);
- Usare il portatile solo in condizioni sicure, al riparo da luce del sole e altri fonti di calore, liquidi, polveri e altro materiale dannoso;
- Posizionare il computer in punti non raggiungibili dai bambini o dagli animali domestici;
- Evitare di appoggiare oggetti sopra il portatile: la pressione eccessiva sullo schermo LCD e sulla tastiera potrebbe danneggiarli;
- Impugnare e sollevare il computer solo dalla base, non afferrandolo dallo schermo per evitare di danneggiare il display o i connettori che lo collegano alla scheda madre inserita nella base del portatile;
- Prima di richiudere lo schermo del portatile assicurarsi sempre che non ci sia nulla tra la tastiera e lo schermo;
- Non smontare per nessun motivo il coperchio posteriore del portatile, per non invalidare la garanzia e per evitare danni accidentali alle parti interne.

Custodia

- Quando non in uso, il PC dev'essere custodito in luogo sicuro, adottando tutte le opportune precauzioni contro furti e danneggiamenti accidentali;
- Durante il trasporto, utilizzare la custodia assegnata assicurandosi che non vi siano all'interno alimenti o sostanze che possano danneggiarlo;
- Posizionare il portatile nel vano interno della borsa, isolandolo da altri materiali;
- Prestare attenzione agli urti durante il trasporto o lo spostamento;
- Non lasciare il pc in sospensione per lungo tempo, piuttosto usare l'ibernazione o meglio ancora spegnerlo quando in custodia;
- Quando è spento, non lasciare l'alimentatore collegato se la batteria è già carica al 100%.

Usare il portatile in condizioni ideali

- Assicurarsi di avere le mani pulite prima di usare il portatile;
- Posizionare il portatile su una superficie piana, pulita e priva di polvere;
- Usare il portatile in una posizione areata in modo tale che ci sia spazio attorno al dispositivo per favorirne l'aerazione e prevenirne il surriscaldamento;
- Non appoggiare fogli di carta o altro materiale sul portatile acceso che ne impedirebbe la dissipazione del calore.

Pulizia

- Spegnere il computer e scollegarlo dall'alimentazione elettrica prima di procedere alla pulizia;
- Mantenere pulito il portatile rimuovendo i residui di polvere e sporcizia con un panno in microfibra;

- Per non danneggiarlo, pulire lo schermo delicatamente senza fare troppa pressione;
- Non spruzzare mai dell'acqua o altre soluzioni detergenti direttamente sul portatile e sullo schermo, ma su un panno morbido;
- Non utilizzare fazzoletti o simili tipi di carta per non graffiare le superfici lucide;
- Non applicare adesivi, calamite o altre "personalizzazioni "sul telaio del portatile.

Collegamento delle periferiche (chiavette usb, cuffie, adattatori di rete e cavo di alimentazione)

- Prestare attenzione all'inserimento di prese USB e di rete: gli ingressi sono molto delicati e vanno maneggiati con cura;
- Fare attenzione alle dimensioni e alla forma dei relativi connettori prima di stabilire il collegamento in modo da individuare la porta corretta;
- Non forzare l'inserimento della periferica: se si sente resistenza nell'inserimento controllare bene e non forzare.

Non abbandonare il portatile in macchina

- Le alte temperature raggiunte nell'abitacolo dell'auto potrebbero causare danni molto gravi;
- Inoltre, rappresenterebbe un invitante obiettivo per malintenzionati di passaggio.

In caso di qualsiasi problema hardware o software, si è pregati di darne comunicazione al servizio competente o all'assistenza tecnica di Città Metropolitana.