Città
metropolitana
di Milano

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

Approvato con decreto del sindaco RG n. 230/2024 del 24 settembre 2024

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'osservanza 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);

- D.lgs. 101 del 10 agosto 2018 (Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679);
- 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. 90 del 28 giugno 2024 (Legge sulla Cybersicurezza)
- Piano Triennale per l'informatica nella Pubblica Amministrazione 2024-2026;

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 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 viene utilizzato il meccanismo di Multi-Factor Authentication (MFA). L'utente è infatti tenuto ad autenticarsi utilizzando un codice identificativo (userid) e una parola chiave segreta (password) che sono rilasciati dal Dipartimento Transizione digitale e successivamente procedere con l'autenticazione utilizzando gli strumenti messi a disposizione dall'Amministrazione.

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:

- 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. Il dipendente dovrà posizionare i file di lavoro nella cartella "Documenti" del proprio computer che dovrà essere sincronizzata su un sistema condiviso di archiviazione messo a disposizione dall'Ente (OneDrive). Inoltre, nel caso di dati estremamente sensibili, sarà necessario cifrare i documenti contenenti tali dati utilizzando gli strumenti di criptazione già in uso presso l'Ente.
- Procedere con la protocollazione di documentazione a valore legale secondo le regole previste dal Manuale di Gestione dell'Ente.
- 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

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.

L'utilizzo dell'indirizzo di posta elettronica fornito dall'Ente a ciascun dipendente deve essere utilizzato esclusivamente per attività lavorative e non per scopi personali.

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:

- 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;
- 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;
- È 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 sei 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:

- 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.
- Non è consentito scaricare e 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. 4.3 Wi-Fi

Rete Wi-Fi pubblica

All'interno delle sedi di Città Metropolitana di Milano è disponibile una rete Wi-Fi pubblica per consentire la navigazione internet agli utenti esterni all'Ente (ospiti, cittadini, turisti etc.). Per accedere a tale rete, sarà necessario registrarsi inserendo il proprio numero di cellulare.

Rete Wi-Fi privata

In alcune zone delle sedi principali della Città Metropolitana di Milano è presente una rete WiFi privata destinata agli utenti dell'Amministrazione. Tale rete consente ai dispositivi portatili forniti dall'Ente ed opportunamente configurati dal Dipartimento Transizione digitale, di accedere alle risorse della rete come se fossero connessi via cavo.

Tale rete Wi-Fi è protetta ed è ad uso esclusivo dei dispositivi forniti dall'Ente. Non è pertanto consentito collegare qualsiasi dispositivo, diverso da quelli assegnati, alla rete Wi-Fi dell'Ente.

Art. 4.4 Intranet

Il portale Intranet è un portale web interno alla rete di Città Metropolitana di Milano ed è utilizzato da tutti i dipendenti dell'Ente. Dal portale Intranet è possibile accedere ai software istituzionali e ai link dei principali portali informativi dell'Ente.

Il portale intranet inoltre è utilizzato come bacheca elettronica per le comunicazioni interne ai dipendenti e per la diffusione di informazioni e documenti di interesse generale dell'ente.

Art. 5 – Smartworking

I dipendenti di Città Metropolitana di Milano che usufruiscono dello smart working, devono disporre di una dotazione informatica minima adeguata alle mansioni svolte, che comprende un personal computer e una connessione ad Internet.

Dispositivi di proprietà dell'Ente

Il dipendente potrà essere dotato dall'Amministrazione di un personal computer portatile ed eventualmente di un cellulare, da utilizzarsi nel totale rispetto delle regole determinate dalla regolamentazione e in conformità con le indicazioni che gli saranno fornite, nonché con quanto trattato nell'Allegato tecnico a questo documento.

Gli strumenti di lavoro affidati al dipendente devono essere usati esclusivamente per lo svolgimento dell'attività lavorativa, nel rispetto di quanto previsto dai regolamenti dell'Amministrazione, e non per scopi personali o non connessi all'attività lavorativa. Il dipendente ha l'obbligo di utilizzare e custodire gli strumenti di lavoro affidatigli con la massima cura e diligenza.

I dispositivi mobili di proprietà dell'Amministrazione, utilizzati dai dipendenti per svolgere

attività lavorativa da remoto, sono utilizzati anche durante l'espletamento dell'attività lavorativa presso l'ordinaria sede di servizio.

Dispositivi di proprietà del dipendente

L'utente potrà utilizzare, nel caso in cui non possa disporre di strumentazione fornita dall'Ente, apparecchiature di proprietà per svolgere attività lavorativa in smartworking. L'uso di strumentazione propria dovrà essere autorizzato dal personale del Dipartimento Transizione digitale, che ne valuterà la compatibilità con i sistemi utilizzati dall'Ente e verificherà che dispongano dei requisiti di sicurezza necessari. In questo caso verrà richiesto all'utente, che confermerà di svolgere l'attività con una autodichiarazione, di installare alcuni programmi necessari per accedere ai servizi informatici e di mantenere i sistemi e l'antivirus aggiornati. In particolare, il dipendente deve seguire le Linee Guida fornite dal Dipartimento transizione digitale per installare il software di Remote Desktop, che garantisce il collegamento remoto al dispositivo presente presso l'ordinaria sede di servizio.

Nel caso di utilizzo di sistemi di proprietà del dipendente verrà fornita assistenza solo sulle componenti software che saranno fornite dall'Ente. In particolare, si richiama la necessità di verificare la presenza e il regolare funzionamento del software antivirus e anti-malware installato sul proprio computer.

Per minimizzare il rischio potenziale di danni, il dipendente che si avvale di strumenti propri per effettuare le attività di smartworking, almeno durante l'esercizio di tali attività, deve tenere i comportamenti descritti nel presente disciplinare anche durante l'utilizzo di dispositivi personali.

Norme di utilizzo degli strumenti laptop, desktop e mobili

I dipendenti che usufruiscono dello smartworking devono rispettare le seguenti indicazioni:

- sia che vengano utilizzati dispositivi personali oppure di proprietà dell'Ente, accedere alla rete dell'Ente utilizzando la VPN e nel caso di dispositivi personali è necessario collegarsi tramite Accesso Remoto (Remote Desktop) al computer presente nella propria sede di lavoro e operare come se si fosse davanti allo stesso: il monitor della postazione in sede risulterà disattivato in modalità CTRL-ALT-CANC e non sarà possibile visualizzare l'attività dell'utente;
- nel caso di dispositivi di proprietà del dipendente, creare un account separato per le attività lavorative, le cui credenziali siano note unicamente al dipendente medesimo (è esclusa pertanto la condivisione di tali credenziali con i familiari);
- nel caso di dispositivi forniti dall'Amministrazione, utilizzare solo l'account creato per il dipendente dal Dipartimento Transizione digitale e solo per scopi di lavoro; è vietata la creazione di ulteriori account, se non su specifica e motivata autorizzazione del responsabile della struttura di appartenenza; è altresì vietata la condivisione delle credenziali, anche con i familiari;
- i dati trattati durante l'attività lavorativa devono essere accessibili unicamente al dipendente;
- una volta terminato il servizio, utilizzare le funzioni di gestione degli appunti di Windows per eliminare la cronologia appunti, evitando così di mantenere anche solo

temporaneamente salvate password o dati sensibili;

- configurare la modalità di blocco automatico dell'accesso al sistema dopo un breve periodo di inattività o bloccare manualmente l'accesso al sistema quando il dispositivo non è in uso;
- custodire adeguatamente le credenziali di accesso e non condividerle con terzi;
- effettuare sempre il logout dai servizi Web, programmi e piattaforme di lavoro una volta terminata la sessione lavorativa;
- custodire con le debite cautele i dispositivi in uso;
- utilizzare esclusivamente dispositivi removibili (chiavette usb, hard-disk esterni, ecc.) di cui si conosce la provenienza ed effettuare sempre la scansione di tali dispositivi provenienti dall'esterno;
- utilizzare, sia nel caso di attività lavorativa in sede sia durante lo smart working, la funzione di stampa riservata per evitare di lasciare a lungo nel vassoio della stampante documenti. Utilizzare tale funzione soprattutto nel caso di stampa di documenti contenenti dati sensibili;
- non tentare di aggirare i meccanismi di controllo degli accessi di qualsiasi risorsa informatica protetta;
- comunicare tempestivamente al Dipartimento Transizione digitale qualsiasi incidente da cui potrebbe derivare una violazione di dati personali.

Tutte le indicazioni contenute nel presente Disciplinare (es. gestione della posta elettronica, creazione e conservazione di password etc.), valide per l'attività in presenza, sono da considerarsi valide e applicabili anche nel caso di attività svolta da remoto.

Norme di utilizzo di smartphone e router Wi-Fi

I dispositivi smartphone e router Wi-Fi (con SIM dati) assegnati dall'Amministrazione sono strumenti di lavoro utilizzabili unicamente a tale scopo. Non possono essere ceduti, condivisi con terzi o utilizzati per scopi personali.

Entrambe le tipologie di dispositivo possono essere utilizzate per la connessione ad Internet in mobilità. Il relativo traffico dati può essere consumato solo per finalità connesse con l'attività lavorativa. Il dipendente è responsabile dell'uso corretto e lecito della connessione ad Internet.

Connessione ad Internet

Il dipendente che effettua attività di smartworking potrà utilizzare la propria rete Wi-Fi, e quindi connettere a tale rete i dispositivi forniti dall'Ente, per finalità istituzionali connesse alle attività lavorative svolte e nel rispetto del presente Disciplinare.

Nel caso in cui ci sia necessità di connettersi a rete wireless diverse da quella della propria abitazione si raccomanda, al fine di prevenire l'esposizione a cyber attacchi, di evitare il collegamento a reti non sicure o sulle quali non si siano presenti adeguati sistemi di protezione e sicurezza.

Art. 6 - 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.

Il Dipartimento Transizione Digitale imposta la propria azione di monitoraggio e controllo sui sistemi informatici dell'Ente messi a disposizione per lo svolgimento dell'attività lavorativa nel rispetto della normativa vigente e sul presupposto di un utilizzo responsabile degli stessi da parte degli Utenti, adottando in ogni caso le soluzioni tecnologiche idonee a garantire i profili di sicurezza dei sistemi informativi e dei dati gestiti.

Tutte le attività sotto riportate sono svolte nel rispetto dei principi di gradualità, pertinenza e non eccedenza stabiliti dal Garante per la protezione dei dati personali nonché dei diritti e delle libertà fondamentali dei lavoratori, sempre mediante funzionalità consentite dalla normativa vigente.

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.

L'amministratore di sistema, nel caso in cui rilevi anomalie o configurazioni non corrette delle PdL, può provvedere a isolare immediatamente l'origine dell'anomalia o del malfunzionamento anche senza preavvisare l'Utente, per salvaguardare la sicurezza e l'integrità dei sistemi informativi dell'Ente. In tal caso, verrà data successiva informativa all'Utente sui motivi dell'avvenuto intervento sulla PdL da parte dell'amministratore di sistema. 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.

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.

Il Dipartimento utilizza sistemi automatizzati per la gestione centralizzata dei cosiddetti "file di log", che consentono di tracciare eventuali anomalie o minacce informatiche che potrebbero colpire i sistemi, compromettendo la funzionalità e la sicurezza degli apparati informatici dell'Ente e delle informazioni ivi contenute.

I file di log relativi alla navigazione in Internet sono registrati e conservati per le suddette finalità di funzionalità e sicurezza, in conformità alla normativa vigente. Nel caso di eventi anomali e/o pregiudizievoli per la sicurezza informatica, i file di log relativi alla navigazione possono essere

esaminati dagli amministratori di sistema per l'individuazione del problema tecnico e l'adozione delle necessarie misure conseguenziali. In ogni caso, tutti i controlli di funzionalità e monitoraggio avvengono nel rispetto di quanto previsto dal CAD, dalle norme in materia di tutela della libertà e dignità dei lavoratori, della normativa unionale e nazionale in materia di protezione dei dati personali.

La conservazione dei log di navigazione Internet è di sei mesi.

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.

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 tracking e monitoraggio che consentono di rilevare minacce per la sicurezza dell'Ente e analizzare il flusso di traffico o di carico dei sistemi di posta elettronica.

Tali strumenti hanno l'esclusiva finalità di garantire la piena funzionalità, la sicurezza e l'efficienza del sistema di posta e sono utilizzati esclusivamente da personale autorizzato del Dipartimento.

Art. 7 - Modifica o cessazione del rapporto di lavoro

Di norma l'assegnazione della strumentazione che costituisce la postazione di lavoro non decade in caso di spostamento ad altro settore dell'Ente.

In caso di cessazione del rapporto di lavoro con l'Ente o pensionamento, prima della restituzione della postazione di lavoro si è tenuti a:

- comunicare tutte le informazioni relative all'ubicazione nei sistemi centralizzati di tutti i dati concernenti l'attività lavorativa al proprio responsabile o al soggetto che, in accordo alla normativa, è deputato a trattarli, cancellando le eventuali copie presenti nella postazione stessa;
- cancellare eventuali altri dati personali propri o di terzi e non personali che dovessero risultare ancora presenti.

In assenza di richieste specifiche, il Dipartimento provvederà al ritiro della postazione di lavoro e alla formattazione/cancellazione dei dati presenti per procedere alla riassegnazione.

In caso di decesso, è possibile da parte degli eredi inoltrare richiesta di copia delle comunicazioni email al Dipartimento Transizione digitale al fine di raccogliere eventuale documentazione personale ancora presente sui dispositivi di proprietà dell'Ente.

In tutti i casi in cui si verifichi un trasferimento interno alla struttura o cessazione del rapporto con l'Ente, il Dipartimento Risorse Umane e Organizzazione, lo comunica formalmente al Dipartimento Transizione digitale secondo le modalità stabilite.

Il Dipartimento Transizione digitale procede, quindi, secondo le seguenti modalità:

- nel caso di assegnazione ad altro Settore verranno disattivate tutte le abilitazioni dell'utente relative ai servizi utilizzati dal Settore di provenienza, comprese quelle relative ai portali e alle banche dati esterne. Resteranno valide le abilitazioni ai "servizi orizzontali" (es. utente di dominio e posta elettronica). Nel caso di assegnazione ad altro settore sarà competenza e responsabilità del Dirigente, di una P.O. o del Responsabile di Settore di procedere alla richiesta delle specifiche abilitazioni necessarie per lo svolgimento dell'attività lavorativa ovvero per gli ulteriori "servizi orizzontali" (es. navigazione internet, cloud, ecc.) e i necessari "servizi verticali" (es. protocollo, gestione atti, finanziaria, risorse condivise ecc.);
- nel caso di cessazione del rapporto tutti gli account relativi all'utente verranno disabilitati e/o eliminati.

Resta in capo al Responsabile del proprio Settore di ogni cartella di rete o risorsa condivisa, a cui l'utente per il quale è sopraggiunta la modifica o la cessazione del rapporto è abilitato, richiedere la modifica o eliminazione dei permessi di accesso.

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 Dipartimento transizione digitale.

Per evitare problemi durante la migrazione dei dati, utilizzare esclusivamente la cartella "Documenti", da sincronizzare in OneDrive laddove possibile, 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 in settimana 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 nel fine settimana, 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, attraverso l'apertura di un ticket all'indirizzo: https://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 e-mail.
- 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 o link sospetti

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

Nel caso in cui siano stati aperti/scaricati allegati o sia stato cliccato un link non sicuro, il dipendente dovrà seguire i seguenti passaggi:

- scollegare immediatamente il dispositivo da Internet e da qualsiasi altra rete interna, scollegando sia Wi-Fi che i cavi Ethernet utilizzati per una connessione di rete interna o esterna;
- avvisare il servizio di Helpdesk per richiedere un controllo accurato del dispositivo;
- effettuare tempestivamente una scansione antivirus e ripetere tale procedura anche qualche giorno dopo;
- eliminare il messaggio e qualsiasi eventuale copia scaricata dell'allegato;
- modificare le credenziali di accesso degli account salvati sul dispositivo;
- cancellare tutti i dati del browser, inclusi cookie e cronologia.

Inoltre, il dipendente dovrà contattare il Dipartimento Transizione digitale, e nello specifico il DPO dell'Ente, per ricevere supporto nella gestione delle situazioni di possibili compromissioni del proprio computer. Nello specifico, il dipendente dovrà:

- comunicare al Direttore del Dipartimento Transizione Digitale la situazione di compromissione del proprio computer;
- se ritenuto necessario, procedere con la denuncia alle Autorità;
- valutare, insieme al Dipartimento Transizione digitale e DPO, se inoltrare una comunicazione ufficiale anche al Garante per la protezione dei dati personali.

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 cliccare, 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.

Template di firme e disclaimer

Per garantire la coerenza della comunicazione, i dipendenti sono tenuti ad utilizzare un template per le firme e i disclaimer inseriti nei messaggi di posta elettronica. In particolare, il template della firma deve contenere, nell'ordine riportato, le seguenti informazioni:

- Nome e Cognome
- Ruolo all'interno dell'Ente
- Nome dell'Ente [Città Metropolitana di Milano]
- Dipartimento/Settore/Area
- Indirizzo [Via/Viale …, numero civico (Milano)]
- Numero di telefono

La firma dovrà essere impostata secondo le direttive definite dall'Ente.

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 tendenze 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.

Crittografia dei dati

Così come descritto all’Art. 3 del presente disciplinare, sarà necessario crittografare i dati estremamente sensibili utilizzando gli strumenti di criptazione in uso presso l’Ente. In particolare, i dipendenti potranno utilizzare la funzionalità “Cifra” di GoSign Desktop per proteggere i dati con una password di accesso, scegliendo tra diverse tipologie di “chiavi” per criptare il documento contenente i dati sensibili.

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

La Città metropolitana, al fine di non avere vincoli tecnologici, promuove lo sviluppo e l'acquisto di prodotti applicativi multi browser. A seguito dell'adozione di M365 da parte dell'Ente, Il browser che si consiglia 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.

Edge permette l'uso di applicativi progettati per Internet Explorer, residuali presso l'Ente, 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 salvataggi 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.

Utilizzo dei dispositivi di telefonia mobile e smartphone

I dispositivi di telefonia mobile o smartphone e relativa SIM sono di proprietà dell'Ente e fanno parte della dotazione informatica messa a disposizione esclusivamente per l'attività lavorativa, nel rispetto delle seguenti regole.

Il dipendente assegnatario di tali dispositivi è responsabile di tenere con cura il dispositivo e di intraprendere ogni azione in suo potere per impedire deterioramenti o danneggiamenti dello stesso.

I dispositivi mobili assegnati non possono essere ceduti a terzi a nessun titolo.

Tutte le attività non espressamente previste nei relativi contratti di fornitura di beni e servizi (es. aggiornamento software, backup, ripresa dati, configurazioni varie ecc.) sono a carico e sotto la responsabilità dell'assegnatario.

Gli assegnatari possono utilizzare il telefono di servizio per telefonate personali solo avvalendosi della fatturazione separata a proprio carico delle telefonate private (Dual billing) da parte dell'operatore di telefonia mobile. Il servizio Dual billing è attivabile mediante la sottoscrizione di un apposito contratto contenente i dati necessari per la fatturazione delle telefonate private.

L'assegnazione, la consegna iniziale e la restituzione, in caso di modifica o cessazione del rapporto con l'amministrazione, dei dispositivi avverrà secondo le modalità stabilita dal Dipartimento Transizione Digitale.

Utilizzo della firma digitale

La firma digitale è il risultato di una procedura informatica che, applicata a un documento elettronico, ne garantisce l'autenticità. La firma digitale è l'equivalente elettronico della firma autografa su carta e ha valore legale in quanto è strettamente legata al suo titolare.

Città Metropolitana di Milano ha acquistato un numero considerevole di firme digitali InfoCert con l'obiettivo di distribuirle a tutti i dipendenti dell'Ente.

Il Dipartimento Transizione digitale gestisce il registro delle firme digitali concesse e provvede al rinnovo di quelle in scadenza ove ne sussistano le condizioni. Il Dipartimento, a seguito di comunicazione dell'organo competente, provvede alla revoca della firma nei casi previsti dalla legge o qualora non sussistano più i presupposti di fatto e di diritto che ne hanno determinato il rilascio.

La firma digitale è utilizzata per la sottoscrizione di documenti nel rispetto dei poteri di firma derivanti dalla legge o dai regolamenti interni dell'Amministrazione.

Per procedere con la firma digitale, il dipendente deve scaricare uno dei software messo a disposizione dai distributori di firme digitali certificati AgID (es. Go Sign Desktop) attraverso cui confermare la propria identità, utilizzando il codice OTP ricevuto tramite SMS o notifica tramite app. Al termine del processo, si suggerisce di controllare puntualmente che la firma sia stata correttamente apposta attraverso l'utilizzo della componente "Verifica" disponibile sul software scaricato.

In futuro, si prevede di dismettere l'utilizzo di app/software specifici, per utilizzare invece le versioni web di tali strumenti.

Identità digitale

L'identità digitale è oggi necessaria per accedere a moltissimi servizi online. I dipendenti di Città Metropolitana devono rispettare alcune indicazioni di utilizzo dell'identità digitale al fine di non ledere all'immagine dell'Ente, soprattutto nel caso in cui accedano ai servizi digitali con delega ad operare per conto dell'Amministrazione.

Tale delega, rilasciata dall'Amministrazione, prova infatti l'appartenenza del dipendente all'Ente Città Metropolitana. Pertanto, l'accesso ai servizi digitali con delega ad operare per conto di Città Metropolitana di Milano deve essere effettuato soltanto per scopi correlati all'attività lavorativa.

Nel caso in cui un dipendente non sia stato precedentemente delegato ad operare per conto dell'Ente, ma si trova comunque ad accedere a servizi digitali che permettono al dipendente di raccoglie dati e informazioni inerenti all'attività lavorativa, questo è tenuto ad utilizzare tali informazioni soltanto nell'ambito dell'attività professionale, senza divulgare informazioni sensibili.

Social media policy

Sulla base delle Linee Guida del Vademecum "Pubblica Amministrazione e Social Media" realizzato dal Formez, sono qui definite le principali regole e le modalità di gestione dei profili dell'Ente sui social media (LinkedIn, Facebook, Instagram, X, YouTube).

Utilizzo degli account istituzionali dell'Ente

Se il dipendente accede ai social network dell'Ente con un account istituzionale, egli agisce in nome e per conto dell'Ente, pertanto dovrà utilizzare un linguaggio consono e in nessun modo pubblicare contenuti che possano ledere l'immagine dell'Ente.

Abilitato a gestire i vari social network è l'Ufficio Stampa. In particolare, l'Ufficio Stampa si occupa del monitoraggio, dell'aggiornamento e del corretto funzionamento del social network.

Ogni argomento ed il contenuto delle varie tematiche che si vuole pubblicare su un profilo social istituzionale deve essere, a seconda della complessità, discusso e condiviso con il vertice politico-istituzionale di riferimento, il relativo dirigente per competenza e il dirigente dell'Ufficio Stampa. Nel caso in cui il contenuto da pubblicare fosse inerente a richieste derivanti dagli utenti tramite commenti, le risposte devono essere preventivamente verificate con gli uffici di competenza, se necessitano di integrazioni con contenuti tecnici.

Il linguaggio da usare sui social network deve essere semplice e diretto, non confidenziale né burocratico, valorizzando, per tipologia di contenuti e stili comunicativi, le potenzialità del canale e del mezzo utilizzato (ad esempio audio video, visual, etc.). Inoltre, il dipendente che pubblica contenuti sui profili social istituzionali deve sempre mantenere un tono adeguato al contesto di comunicazione pubblica e istituzionale dell'Ente verso il cittadino.

I dipendenti possono utilizzare gli account istituzionali dell'Ente per:

- comunicare attività istituzionali;
- promuovere iniziative di vario genere (progetti, informazioni sui bandi, servizi, eventi e messaggi di pubblica utilità…). Si precisa che Si precisa che la pubblicazione di atti o avvisi pubblici sui profili social ha validità di pubblicità-notizia e non di pubblicità legale.
- rilanciare e condividere contenuti e messaggi di pubblico interesse ed utilità provenienti da terzi, enti pubblici, associazioni e gruppi presenti nel territorio.

I dipendenti non possono utilizzare i profili social istituzionali per finalità politiche di parte, per scopi personali e commerciali.

Utilizzo degli account personali

Anche nel caso in cui il dipendente acceda ai social network con account personali, egli è sempre considerato un dipendente pubblico anche fuori dal luogo e dall'orario di lavoro. Pertanto, anche in questo caso, il suo comportamento deve essere decoroso, dignitoso e improntato alla correttezza verso l'Amministrazione.

Ai dipendenti è severamente vietato trattare sui social media argomenti di lavoro o condividere informazioni riservate relative all'Amministrazione, nonché pubblicare contenuti che possano ledere l'immagine dell'Ente. È però consentito condividere liberamente sui propri profili privati i contenuti diffusi dai canali social della Città Metropolitana.

I dipendenti non possono trasmettere e/o diffondere messaggi minatori ovvero ingiuriosi, commenti e dichiarazioni pubbliche offensive nei confronti dell'Amministrazione, riferiti alle attività istituzionali dell'Ente e, più in generale, al suo operato, che per le forme e i contenuti possano comunque nuocere all'Amministrazione, ledendone l'immagine o il prestigio o compromettendone l'efficienza.

Ad eccezione di eventi pubblici che si svolgono presso la sede di lavoro i dipendenti non possono divulgare foto, video o altro materiale multimediale, che riprenda locali e personale dell'Ente senza l'esplicita autorizzazione delle strutture e delle persone coinvolte.

I dipendenti non possono aprire canali social a nome della Città Metropolitana di Milano o che trattino argomenti riferiti all'attività istituzionale dell'Ente, senza preventiva autorizzazione.

L'utilizzo improprio dei social network dell'Amministrazione e la diffusione di notizie e comunicazioni varie inerenti all'attività lavorativa, costituisce violazione del Codice di Comportamento nazionale e della Città Metropolitana e determina l'applicazione delle sanzioni disciplinari previste dalla normativa vigente e dal Contratto collettivo nazionale e decentrato di Lavoro.

Microsoft Office 365

Dal 2023, Città Metropolitana di Milano fornisce ai propri dipendenti gli strumenti di Microsoft Office 365 per lo svolgimento delle loro attività lavorative. Gli strumenti di Microsoft Office 365 rappresentano oggi gli strumenti ufficiali utilizzati dall'Amministrazione.

L'Ente fornisce licenze che permettono l'utilizzo degli strumenti di Microsoft 365 anche in locale. I dipendenti che non dispongono di tali licenze sono tenuti ad accedervi tramite web utilizzando il proprio account Microsoft.

Tutti gli strumenti devono essere utilizzati nel rispetto delle indicazioni contenute in questo Disciplinare e soltanto ai fini delle attività lavorative.

Microsoft Teams

Messaggistica istantanea

Il dipendente può utilizzare le chat di **messaggistica istantanea** di Microsoft Teams per comunicare sia con i colleghi dell'Amministrazione sia con utenti esterni all'Ente tramite chat disponibile per le videoconferenze.

La messaggistica istantanea è consigliata per comunicazioni brevi e immediate inerenti all'attività lavorativa che richiedono risposte rapide. Si consiglia infatti di non utilizzare questo strumento per discutere di temi personali. La messaggistica istantanea non è adatta per discussioni complesse o per condividere qualsiasi comunicazione che richiede una validazione ufficiale o la condivisione di informazioni e/o documenti altamente riservate o sensibili, che vanno invece trasmessi tramite canali ufficiali e che garantiscano il rispetto delle norme GDPR.

Videoconferenze

Il dipendente utilizza Microsoft Teams anche per organizzare videoconferenze sia con gli altri dipendenti dell'Ente, sia con utenti esterni all'Amministrazione. I sistemi di videoconferenza sono strumenti di lavoro da utilizzare in alternativa a riunioni in presenza o come alternativa alla chiamata telefonica.

Sono riportati di seguito alcuni accorgimenti per la buona riuscita di una videoconferenza:

- Assicurarsi che la connessione internet sia stabile. Utilizzare cuffie con microfono per migliorare la qualità dell'audio e ridurre il rumore di fondo;

- Spegnere il proprio microfono quando non utilizzato per evitare di introdurre rumori, brusii o interferenze e utilizzare la funzione "alzare la mano" di Teams per segnalare la volontà di intervenire;
- Verificare che la webcam sia posizionata correttamente per catturare un'immagine chiara e centrata del viso e assicurarsi che l'illuminazione sia adeguata, preferibilmente con luce frontale;
- Nel caso ci si connetta dalla propria abitazione è bene utilizzare uno sfondo neutro o le funzioni di sfondo sfocato o sfondi virtuali di Teams nel caso in cui non si disponga di una zona riservata e per minimizzare le distrazioni visive;
- Nel caso in cui non si disponga di banda sufficiente a garantire un adeguato segnale audio-video è conveniente spegnere la videocamera;
- Condividere lo schermo solo quando necessario e chiudere tutte le altre applicazioni o schede che non sono pertinenti alla riunione per evitare condivisioni accidentali;
- Qualora sia necessario registrare la videoconferenza, informare i partecipanti e ottenere il loro consenso prima di registrare qualsiasi sessione al fine di rispettare la privacy e la conformità alle normative vigenti;
- Scollegarsi sempre al termine della videoconferenza, soprattutto se si utilizzano stanze virtuali condivide che potrebbero essere utilizzate successivamente per altre riunioni.

Outlook

Per accedere ad Outlook Web, il dipendente deve collegarsi al sito Outlook.com ed effettuare l'accesso al proprio account Microsoft. Tramite Outlook web, il dipendente dell'Ente avrà accesso alla propria casella di posta elettronica, nonché al riquadro di navigazione con il calendario, i contatti e le attività.

Per un utilizzo corretto e sicuro di Outlook web il dipendente è tenuto a rispettare tutte le indicazioni inerenti alla posta elettronica riportate in questo Disciplinare.

OneDrive

OneDrive è utilizzato dai dipendenti come soluzione di archiviazione cloud dei propri file inerenti l'attività lavorativa. Il dipendente è infatti tenuto a salvare i propri file su OneDrive e non in locale sui propri dispositivi così da evitare perdite di dati e documenti.

In particolare, tale strumento viene utilizzato per effettuare backup periodici, così come indicato all'Art. 3 del presente disciplinare.

È vietato al dipendente l'utilizzo di OneDrive per salvare documentazione di carattere personale.

Integrazione tra OneDrive e SharePoint

Per permettere la collaborazione sui file all'interno dell'Ente, il Dipartimento Transizione digitale sta valutando la possibilità di integrare lo strumento di OneDrive con quello di SharePoint, utilizzato come piattaforma per siti di team collaborativi e intranet dell'Ente dove i documenti e i file sono destinati alla condivisione e alla collaborazione di gruppo.

I file memorizzati in SharePoint potranno essere sincronizzati sul computer locale di un utente tramite il client di sincronizzazione di OneDrive. Questo permetterà agli utenti di lavorare offline sui file e poi sincronizzarli automaticamente con SharePoint.

I file creati o modificati in OneDrive potranno essere automaticamente trasferiti o sincronizzati con SharePoint per iniziare processi di workflow, come approvazioni o revisioni, che sono configurati su SharePoint.

Le impostazioni di sicurezza e i permessi assegnati ai file in SharePoint influenzano come i file sono accessibili e gestiti quando vengono sincronizzati o aperti tramite OneDrive.

Per garantire l'accesso a documentazione lavorativa anche a seguito di pensionamento oppure cambio del datore di lavoro, il dipendente dovrà condividere l'accesso a tutti i documenti salvati su SharePoint al Direttore/Responsabile del proprio Settore e ad almeno un altro collega, individuato in accordo con il Direttore/Responsabile del proprio Settore stesso.