Disciplinare per l’utilizzo degli strumenti informatici

Sommario

Disciplinare per l'utilizzo degli strumenti informatici.....I

1. SCOPO E CAMPO DI APPLICAZIONE.....1

2. DEFINIZIONI E ACRONIMI.....1

3. RESPONSABILITA' DEL DOCUMENTO.....2

4. RESPONSABILITÀ GENERALI DI TUTTI I LAVORATORI.....2

5. REGOLE PER L'USO DEGLI STRUMENTI AZIENDALI.....3

6. POSTAZIONI DI LAVORO.....4

7. CREDENZIALI.....5

8. NAVIGAZIONE INTERNET.....5

9. POSTA ELETTRONICA.....7

10. SOFTWARE AZIENDALE.....8

11. PROFILI PER L'INSTALLAZIONE DEL SOFTWARE.....9

12. SPAZIO DISCO.....10

13. DISPOSITIVI ESTERNI.....10

14. TELEFONI.....11

15. DISPOSITIVI DI FIRMA DIGITALE E DI POSTA ELETTRONICA CERTIFICATA (PEC).....12

16. STRUMENTI AZIENDALI "NON ELETTRONICI".....12

17. PIATTAFORME DI COLLABORATION e VIDEO-CONFERENCE.....13

18. POLICY PER GLI INTERVENTI DI SICUREZZA E I CONTROLLI.....14

19. UTILIZZO DI STRUMENTI AZIENDALI IN AMBITO EXTRALAVORATIVO.....16

20. UTILIZZO DI STRUMENTI PERSONALI IN AMBITO LAVORATIVO (BYOD - Bring Your Own Device).....16

21. MANCATA OSSERVANZA DELLE NORME E DELLE ISTRUZIONI.....17

1. SCOPO E CAMPO DI APPLICAZIONE

Il presente Disciplinare ha lo scopo di fornire a dipendenti e collaboratori della **Città metropolitana di Torino** (di seguito "CmTO") le modalità d'utilizzo degli strumenti aziendali e le istruzioni da seguire durante lo svolgimento delle attività lavorative che comportano un trattamento di dati personali, al fine di evitare che, anche inconsapevolmente, possano minacciare o compromettere la sicurezza del sistema informatico aziendale o la protezione dei dati ivi contenuti o arrecare un qualunque danno all'azienda (economico o di immagine).

Il diffondersi delle nuove tecnologie consente infatti al lavoratore, nell'adempimento delle mansioni assegnate, l'accesso a strumenti e servizi sempre più innovativi e performanti, ma, di riflesso, richiede l'adozione di precise etiche comportamentali, il rispetto delle norme in vigore e in generale dei principi di correttezza, diligenza e buona fede e di una condotta conforme ai civici doveri. Le prescrizioni di seguito indicate vogliono quindi porre l'attenzione sugli aspetti summenzionati e devono essere considerate in funzione e coerentemente con quanto prescritto all'interno del "*Vademecum Privacy – Istruzioni operative per il personale della Città metropolitana di Torino*"[1] cui si rinvia integralmente, disponibile sul canale "**Privacy**" della Intranet.

Il presente disciplinare definisce altresì le regole per il corretto utilizzo degli strumenti aziendali anche con riferimento all'installazione ed utilizzo di programmi ed applicazioni software garantendo al riguardo anche il rispetto delle disposizioni di cui alla *L. 633/41 e s.m.i.* nonché al *D. Lgs. 30/2005*, relativi alla tutela del diritto d'autore, proprietà intellettuale ed industriale.

2. DEFINIZIONI E ACRONIMI

Strumento aziendale: qualsiasi strumento messo a disposizione dalla CMTO al lavoratore ai fini dello svolgimento delle proprie mansioni lavorative. Rientrano in tale ambito, a titolo di esempio non esaustivo, la postazione di lavoro (desktop o notebook), i telefoni, internet, la posta elettronica, il software, i dispositivi di firma digitale, le credenziali di accesso (login);

DLP - Data Loss Prevention: Sistema di sicurezza mirato ad effettuare il controllo della diffusione o movimentazione all'interno e verso l'esterno delle modalità di

[1] https://intranet.cittametropolitana.torino.it/it/documentazione/vademecumprivacypdf-versione-1

accesso alle informazioni identificate come riservate, sensibili o comunque di rilevante interesse per l'azienda, attraverso componenti software installate sulle PdL e configurazioni a livello centralizzato sulle *policy* di movimentazione/accesso delle risorse (file e cartelle);

URL-FILTERING: sistema di blocco o accesso a URL di navigazione basato su categorizzazione dei siti. Può essere collegato a sistemi esterni di notifica di siti pericolosi (*black-list*) per la sicurezza informatica;

CONTENT-FILTERING: Sistema di analisi del contenuto delle pagine di navigazione al fine di prevenire l'attuazione di azioni malevoli, in caso di potenziale o identificato rischio di sicurezza, quali presenza di malware, virus o script dannosi, contenuto non etico, reindirizzamento su siti a rischio, etc.

SOFTWARE CENTER*:* repository accessibile dalla intranet finalizzato a rendere disponibile tutto il software aziendale e quello che può essere autonomamente scaricato ed installato dal lavoratore, in funzione delle *policy* relative.

3. RESPONSABILITA' DEL DOCUMENTO

La Direzione Aziendale di riferimento per le necessità ed informazioni connesse al presente Disciplinare è la **Direzione Performance, Innovazione, ICT – QA1**.

Il documento è soggetto ad una revisione periodica da parte dei responsabili della redazione.

Eventuali modifiche o integrazioni al documento possono essere suggerite da tutto il personale dipendente mediante comunicazione mail all'indirizzo supervisionesit@cittametropolitana.torino.it .

4. RESPONSABILITÀ GENERALI DI TUTTI I LAVORATORI

È responsabilità di tutto il personale che a vario titolo presta attività lavorativa presso la Città metropolitana di Torino, applicare puntualmente le regole contenute nel presente **Disciplinare**, così come tutte le altre regolamentazioni aziendali vigenti, nonché le istruzioni fornite dai propri Responsabili gerarchici e/o funzionali.

In generale, chiunque ravvisi nell'ambito delle proprie mansioni lavorative dubbi o incertezze circa:

- l’applicazione delle istruzioni ricevute;
- il manifestarsi di nuove esigenze tecniche o organizzative che potrebbero migliorare lo svolgimento delle operazioni affidate;
- malfunzionamenti di strumenti elettronici;
- eventuali perdite di dati;
- violazioni di dati personali;
- incidenti che potrebbero compromettere la sicurezza di CmTO
- le corrette modalità di utilizzo degli applicativi software;

deve segnalarlo tempestivamente al Dirigente/Funzionario responsabile, che a sua volta deve informare la Direzione competente, in base alla situazione.

5. REGOLE PER L’USO DEGLI STRUMENTI AZIENDALI

Gli strumenti messi a disposizione dall'azienda sono strumenti di lavoro ed è responsabilità dei singoli assegnatari custodirli in modo appropriato e diligente, al fine di evitare, per quanto possibile, il furto, l'appropriazione o anche solo l'utilizzo da parte di terzi non autorizzati.

In ogni caso, è indispensabile, oltre a quanto già specificato nel par. precedente, segnalare prontamente alla struttura aziendale competente il danneggiamento, lo smarrimento, il furto o anche l’accesso non autorizzato a tali strumenti.

È indispensabile salvaguardare l’integrità e la sicurezza dei dati e documenti trattati o comunque accessibili attraverso gli strumenti aziendali, prestando la massima attenzione per le informazioni a carattere riservato e sensibile o i dati rientranti nella categoria dei dati particolari.

È buona regola la periodica pulizia degli archivi delle unità di rete, dell’hard-disk della propria postazione di lavoro e della casella di posta, con cancellazione di file ed e-mail obsoleti e inutili, ed evitando la duplicazione dei dati archiviati.

Si ricorda che tutti gli strumenti di lavoro sono finalizzati ad un uso professionale e sono quindi destinati all’adempimento delle mansioni assegnate.

Poiché l’azienda autorizza la fruizione di alcuni dispositivi quali Portatile, Smartphone, Tablet, anche in ambito extralavorativo, nel par. 8 sono esplicitate le regole e responsabilità particolari per tale uso.

6. POSTAZIONI DI LAVORO

La Postazione di Lavoro in dotazione (composta da uno o più dei *device* standard quali computer desktop, notebook, tablet, smartphone, modem LTE, ecc.) deve essere custodita con la massima diligenza, sia durante gli spostamenti, sia durante l'utilizzo nel luogo di lavoro, per evitarne il danneggiamento, lo smarrimento o il furto; di conseguenza in caso di allontanamento, anche solo temporaneo, il lavoratore deve aver cura di fare tutto quanto in suo potere per lasciare il computer in modalità protetta da furti o rimozioni (utilizzo della *docking station* con serratura ove prevista, cavo di blocco, posizionamento dei dispositivi in armadi con chiusura, ecc…)

Nell'utilizzo del dispositivo il lavoratore deve evitare l'insorgere di disservizi, di costi di manutenzione non previsti e, soprattutto, evitare di incorrere in minacce alla sicurezza del sistema informatico aziendale. In caso di allontanamento dalla postazione di lavoro o di inattività per almeno 10 minuti, deve sempre essere attivato lo screen-saver (mediante la combinazione di tasti *Win+L* o *CTRL+ALT+CANC* ed *Invio*).

È proibita la modifica manuale, da parte dell'assegnatario, dell'**indirizzo di rete IP** attribuito (qualora sia statico) o del **nome host** della postazione in dotazione. Analogamente è vietata la creazione di sistemi operativi e macchine virtuali coesistenti con quelle assegnate per gli utilizzi non inerenti al contesto lavorativo. Non è permesso disinstallare o manomettere i software caricati sul sistema operativo ed in particolare i software necessari per il monitoraggio e la protezione dello stesso o della rete internet (quali antivirus o firewall).

E' fatto altresì divieto assoluto di modificare autonomamente la configurazione standard della postazione, sia sotto il profilo hardware che sotto il profilo software senza l'esplicita e documentabile autorizzazione della Direzione competente (QA1 – SIT).

Nello svolgimento dell'attività lavorativa in "Modalità Agile" (*smart working*), è obbligatorio utilizzare sempre gli strumenti di accesso sicuro messi a disposizione dall'Ente secondo le indicazioni fornite all'atto della consegna, ad esempio VPN o VPN+RDS - Remote Desktop.

7. CREDENZIALI

L'accesso alla postazione di lavoro, è protetto da un sistema di autenticazione al dominio aziendale denominato **PROVTO** che richiede al lavoratore di inserire - all'accensione della propria postazione di lavoro – il codice identificativo (*login*) ed una parola chiave (*password*). Tutte le credenziali devono essere personali e segrete, pertanto devono essere conservate e gestite in modo accorto al fine di evitare l'accesso a dati ed applicativi da parte di terzi non autorizzati.

Le password devono essere scelte rispettando determinati criteri di robustezza (non banale, lunghezza di otto caratteri, presenza di almeno dei caratteri non alfabetici, non riconducibile al lavoratore, modificata ogni 3 mesi, ecc.).

Le credenziali utente, composte da codice identificativo (*login*) e parola chiave (*password*) consentono l'identificazione univoca di ciascun utente del Sistema Informativo Aziendale mediante *Single Sign On*: questo significa che login e password sono, tendenzialmente, univoci per tutte le applicazioni dell'Ente.

Vi sono alcune specificità: nel caso della casella di posta elettronica e della VPN, l'accesso non è garantito dal login bensì **dall'indirizzo di posta elettronica aziendale**, mentre la password è sempre la medesima in tutti i casi (c.d. password unificata).

L'aggiornamento o il reset della password di dominio avviene attraverso la funzionalità messa a disposizione sulla pagina **Intranet**, alla voce **Cambio password**[2] previo avviso tramite messaggio mail, a partire da una settimana prima della scadenza.

8. NAVIGAZIONE INTERNET

L'uso improprio della navigazione Internet, come anche l'acquisizione, la riproduzione o la condivisione abusive e/o che possano comunque esporre la CmTO a danno/responsabilità (a mero titolo di esempio, attività di cd. "*file sharing*" e/o scambio di opere coperte da copyright) relativamente a file di immagini, di musica, filmati o l'accesso a siti non eticamente corretti è vietato.

È fatto altresì divieto al lavoratore di scaricare programmi o procedure, anche gratuiti, provvedendo ad installarli autonomamente sugli apparati aziendali, fatto

[2] https://idm.cittametropolitana.torino.it/cambiopassword/

salvo quanto previsto nel prosieguo. Manovre errate riconducibili a tali comportamenti possono infatti, oltre che violare la normativa vigente in materia di diritto d'autore (cd. *legge sul copyright*) o condizioni d'uso, causare danni, dovuti alla necessità di provvedere ad interventi tecnici per il ripristino della funzionalità della stazione di lavoro e/o causare la perdita di dati aziendali.

Fra le misure tecniche adottate per prevenire abusi o minacce alla sicurezza aziendale, in CMTO è attivo il tracciamento delle attività sugli applicativi del Sistema Informativo Aziendale, da/per l'esterno della rete aziendale e la conservazione dei log di traffico telematico, per le seguenti finalità: per "*ragioni di sicurezza interna, statistiche, prevenzione dei reati previsti dal modello organizzativo*" ex *D. Lgs. 231/2001*, e trasmissione dei dati all'Autorità Giudiziaria in caso di formale richiesta. I log vengono conservati per il tempo strettamente necessario al perseguimento delle finalità su indicate. CMTO assume come tempo di conservazione per questa tipologia di log in 6 mesi. I log detengono il punto di partenza (indirizzo IP mittente), l'istante di accesso ed il server o url di destinazione della navigazione.

In conformità alle *Linee Guida del Garante Privacy per posta elettronica ed internet del 1.3.2007* e al fine di ridurre gli usi impropri della navigazione in internet e prevenire eventuali controlli difensivi, CMTO adotta – in via preventiva **-** le seguenti misure:

- uso di filtri (URL Filtering e Content Filtering) che tracciano e prevengono determinate operazioni reputate inconferenti con l'attività lavorativa o ritenute a rischio per la sicurezza informatica (accesso a determinati siti inseriti in black list, e/o download di file o software);
- uso di regole Data Loss Prevention (c.d. DLP): al fine di tracciare e bloccare la diffusione di documenti marcati come riservati all'esterno del sistema informativo aziendale.

La navigazione in rete deve avvenire facendo rigorosamente uso dei dispositivi di protezione preposti quali sono i sistemi **proxy**, **firewall, VPN ed RDS**: sono pertanto vietati collegamenti derivanti da configurazioni non approvate che eludano tali sistemi di controllo.

9. POSTA ELETTRONICA

La casella di posta elettronica è uno strumento finalizzato allo scambio di informazioni nell'ambito dell'attività lavorativa; deve quindi considerarsi eccezionale

l'uso della posta elettronica per finalità personali e, di conseguenza, limitato a comunicazioni brevi e a carattere occasionale, ricordando sempre che l'indirizzo non è privato, bensì aziendale.

A tale riguardo, il dipendente è tenuto ad adottare gli accorgimenti di seguito indicati, per garantire da un lato la riservatezza di eventuali comunicazioni personali ma al contempo la continuità aziendale e/o l'eventuale esigenza giudiziaria o aziendale di verifica che renda necessaria l'apertura dello strumento di posta:

- cancellare gli eventuali messaggi a contenuto personale - utilizzare abitualmente le caselle di posta elettronica condivise tra più lavoratori ovvero le caselle di posta di gruppo (eventualmente affiancandole a quelle individuali);

- in caso di assenza programmata, utilizzare le funzionalità del sistema di posta per l'invio automatico di messaggi di risposta recanti le coordinate della casella di gruppo o del responsabile a cui rivolgersi

Nell'ipotesi in cui la email debba essere utilizzata per la trasmissione di categorie particolari di dati, si raccomanda di prestare attenzione a che:

- l'indirizzo del destinatario sia stato correttamente digitato
- l'oggetto del messaggio non contenga direttamente il riferimento a stati, fatti o qualità idonei a rivelare la particolarità del dato
- gli allegati siano protetti con una password di accesso (comunicata con altro canale)

Ai fini della sicurezza della rete aziendale, è necessario valutare l'affidabilità del mittente prima di accedere ai file allegati alla posta elettronica (non eseguire download di file eseguibili o documenti da siti Web o FTP ambigui o comunque non conosciuti il cui indirizzo Internet inserito nel corpo della mail).

Al fine di ridurre il rischio di diffusione di mail contenenti malware vengono applicati alla mail in ingresso **filtri di controllo delle estensioni** di allegati (es .zip, .rar .exe, etc) e **filtri di limitazione** anti-spam.

Eventuali segnalazioni di mail ritenute sospette devono essere inoltrate al gruppo SOC (mediante inoltro della mail sospetta all'indirizzo d-soc@csi.it) e/o al gruppo di gestione della posta elettronica.

Così come per la navigazione Internet, è attivo il tracciamento e conservazione dei log di posta, per le seguenti finalità: per "*ragioni di sicurezza interna, statistiche, prevenzione dei reati previsti dal modello organizzativo*" ex *D. Lgs. 231/2001*, trasmissione dei dati all'Autorità Giudiziaria in caso di formale richiesta. CMTO assume come tempo di conservazione per questa tipologia di log 12 mesi. I Backup delle caselle di posta vengono conservati per un periodo di 3 anni.

Con l'occasione si rammenta che il contenuto dei messaggi inviati deve essere espresso in maniera professionale e corretto e quindi non deve contenere espressioni che possano rivelarsi offensive, razziste, sessiste, discriminatorie o volgari.

10. SOFTWARE AZIENDALE

Sono vietati, se non espressamente autorizzati da CmTO, la duplicazione e qualsiasi forma di estensione d'uso del software aziendale, inteso sia come software prodotto direttamente da CmTO sia come software prodotto da terzi ed utilizzato da CmTO in forza di appositi contratti di licenza d'uso.

Anche il software aziendale infatti è pienamente tutelato dalla normativa vigente in materia di proprietà intellettuale ed una sua duplicazione e/o un suo utilizzo non autorizzato o comunque difforme da quello definito nelle condizioni della licenza è vietato.

È altresì vietata l'installazione di software con modalità diverse da quelle di seguito richiamate o non necessario per le attività lavorative.

È opportuno che le mail siano accompagnate dal disclaimer "*il presente messaggio di posta elettronica, corredato di eventuali allegati, costituisce una comunicazione aziendale e non ha natura personale. Le eventuali risposte potranno essere conosciute anche da altri lavoratori dell'organizzazione della Città Metropolitana di Torino*"

11. PROFILI PER L'INSTALLAZIONE DEL SOFTWARE.

CmTO definisce le dotazioni di software standard e opzionali secondo le esigenze di servizio, e le gestisce centralmente per tutti i dipendenti, ivi inclusi anche gli aggiornamenti.

A tutti i lavoratori delle Direzioni viene assegnato il profilo di "*standard user*", il quale non prevede la possibilità di operare in autonomia sulla propria postazione riguardo ad installazione software e aggiornamenti, salvo eccezioni esaminate singolarmente.

Laddove, per specifiche e puntualmente motivate esigenze di servizio, venga assegnato il profilo di "*Amministratore/Administrator*", che permette di operare in autonomia sulla propria postazione riguardo ad installazione software e aggiornamenti, nei limiti di quanto consentito dalle prescrizioni del presente Disciplinare, non dovrà essere installato o utilizzato software privo di licenza d'uso, ovvero destinato ad utilizzi fraudolenti.

Nel Software Center aziendale viene individuato e reso disponibile, oltre al software già presente nell'immagine base, il software che può essere autonomamente scaricato e installato nella versione acquisita dall'Ente.

Qualora il dipendente necessiti per lo svolgimento dell'attività lavorativa di un software non presente nel Software Center, anche solo in una versione diversa da quella disponibile, dovrà provvedere a segnalare la necessità al proprio Responsabile, il quale procederà a comunicarlo alla **Direzione Performance, Innovazione, ICT – QA1** mediante comunicazione mail all'indirizzo supervisionesit@cittametropolitana.torino.it .

Attività di testing di soluzioni reperibili in rete sono ammissibili al solo scopo di "testare" per un tempo limitato la soluzione e verificarne l'eventuale utilità aziendale, devono essere effettuate nel pieno rispetto delle relative condizioni di licenza (in quanto versione "*trial*", etc.) e per il solo tempo strettamente necessario e vanno quindi disinstallate. L'autorizzazione alla installazione dovrà essere richiesta, in qualunque caso, alla **Direzione Performance, Innovazione, ICT – QA1**.

Tutte le postazioni e le configurazioni dei profili utenti sono censiti centralmente in un apposito registro dedicato.

CmTO attua verifiche riguardo al software installato sui pc in dotazione ai propri dipendenti (puntuali, periodiche e/o a campione), al fine di assicurare la conformità alla normativa in vigore e alle policy aziendali e provvede – come di seguito dettagliato – alla rimozione del software non autorizzato

12. SPAZIO DISCO

Lo spazio disco, disponibile presso appositi server accessibili in rete, rappresenta una risorsa aziendale importante a supporto della condivisione di informazioni professionali aziendali. Vanno, di conseguenza, evitati: lo "spreco" di tale spazio; l'utilizzo per scopi non attinenti ad attività lavorative; l'utilizzo per la comunicazione non protetta di informazioni riservate o tutelate dalla legge sulla privacy.

La cessazione di utilizzo di uno spazio disco (per cambio ruolo o responsabilità o organizzativo) deve essere comunicata tramite il proprio Responsabile all'area di Assistenza Help Desk, tramite comunicazione alla casella mail **hd_pdl_prto@csi.it**.

Per i dati ed i documenti che risiedono sui server gestiti centralmente, come ad esempio cartelle di rete e database vengono eseguiti periodicamente i salvataggi con la possibilità di ripristinare in toto oppure selettivamente eventuali file distrutti, ad esempio per guasti hardware oppure per cancellazioni involontarie.

Sulle postazioni di lavoro o sui dispositivi mobili assegnati non vengono invece effettuate operazioni di salvataggio e non devono pertanto essere salvati file aziendali, soprattutto se contengono dati personali.

In caso di compromissione della postazione di lavoro e/o malfunzionamento quest'ultima potrà essere reinstallata integralmente, con la relativa perdita di tutte le informazioni in essa conservate.

13. DISPOSITIVI ESTERNI

I dispositivi esterni aziendali (dispositivi di archiviazione USB, Schede SD, ecc.) possono essere utilizzati solo in via assolutamente eccezionale, per motivi strettamente connessi ad esigenze lavorative e trattati con particolare cautela, onde evitare che il loro contenuto possa essere trafugato o alterato o distrutto.

I supporti esterni contenenti dati particolari o comunque riservati, devono essere custoditi in armadi muniti di serratura. Tutti i supporti già contenenti dati aziendali, ma destinati all'alienazione o a diverso utilizzo o a differente assegnatario, devono essere trattati in sicurezza, procedendo a seconda del caso con la formattazione o con la distruzione sicura, al fine di evitare che il loro contenuto possa essere recuperato dopo la cancellazione dei file da terzi non autorizzati.

La distruzione sicura viene effettuata a cura della Direzione Performance, Innovazione, ICT – QA1 mediante attività svolta dal personale CSI-Piemonte.

È infine vietato costituire punti di accesso alle reti interne aziendali non controllati e autorizzati dalla Direzione Performance, Innovazione, ICT – QA1 o utilizzare sistemi di *cloud storage*[3] per interscambio dati diversi da quelli definiti dall'azienda. Per specifiche ed eccezionali esigenze di servizio, e previa comunicazione alla Direzione Performance, Innovazione, ICT – QA1, possono essere autorizzati sistemi esterni di condivisione dei dati.

14. TELEFONI

I telefoni fissi o mobili assegnati, devono essere utilizzati, nell'ambito delle mansioni assegnate, per lo svolgimento dell'attività lavorativa.

Per assicurare la sicurezza degli smartphone aziendali è previsto l'obbligo dell'autenticazione per l'accesso al dispositivo.

All'accensione verrà richiesto obbligatoriamente l'inserimento di un codice, lasciando al dipendente la scelta di inserire una password, un PIN, un segno o il riconoscimento dell'impronta digitale o del viso.

Gli smartphone e tablet aziendali sono configurati mediante una piattaforma di gestione integrata denominata VmWare AirWatch, e prevedono la separazione della componente "*Lavoro*" da quella "*Personale*". Le applicazioni aziendali devono essere utilizzate all'interno della partizione "*Lavoro*", all'interno della quale i dati sono crittografati e non accessibili se non mediante l'inserimento del PIN di sicurezza a 6 cifre.

L'uso del telefono fisso per finalità personali deve considerarsi eccezionale e/o per urgenza e, di conseguenza, limitato a comunicazioni brevi ed a carattere puramente occasionale.

[3] I.e. Google Drive, DropBox, WeTrasfer,

15. DISPOSITIVI DI FIRMA DIGITALE E DI POSTA ELETTRONICA CERTIFICATA (PEC)

I dipendenti, ad oggi, in base all'attuale normativa, sono tenuti all'utilizzo degli eventuali dispositivi di firma digitale e posta elettronica certificata in assegnazione, esclusivamente per lo svolgimento dell'attività lavorativa.

16. STRUMENTI AZIENDALI "NON ELETTRONICI"

Per "*non elettronici*" si intendono sia documenti cartacei sia documenti di altro tipo come ad esempio **microfilm, microfiches, lavagne** e **lucidi**.

Per proteggere i dati personali o in genere riservati contenuti nei documenti è opportuno che essi non siano lasciati negli ambienti di transito o pubblici (corridoi o sale riunioni), o sulla scrivania ma siano riposti, quando non utilizzati e comunque al termine dell'attività lavorativa negli appositi archivi.

Le stampe devono essere immediatamente ritirate dalle stampanti comuni.

Eventuali supporti utilizzati in riunioni o corsi di formazione su cui siano stati riportati dati personali o riservati (es. lavagne) devono essere cancellati al termine dell'uso.

I documenti contenenti categorie particolari di dati devono essere custoditi in appositi armadi dotati di chiavi. I locali ove sono presenti i documenti contenenti i dati personali (ed in particolare quelli di natura sensibile o confidenziale), devono essere soggetti a controllo e a verifica, al fine di evitare che durante l'orario di lavoro o al termine dello stesso possano essere conosciuti o accessibili da parte di soggetti non autorizzati. Si raccomanda, in caso di allontanamento dal proprio ufficio, di adottare tutte le accortezze e precauzioni al fine di impedire l'accesso fisico a chi non sia legittimato, soprattutto se esterno all'organizzazione di appartenenza.

Pertanto, le porte degli uffici ed almeno un armadio per ufficio devono essere dotati di serratura con chiave. Al termine dell'orario lavorativo, ove la dinamica delle attività ed il numero di occupanti lo consentano, è necessario chiudere sempre a chiave gli uffici nei quali vengono svolti trattamenti di dati personali. I documenti cartacei ed i supporti removibili che contengono dati personali devono essere conservati esclusivamente per il tempo previsto nel piano di conservazione aziendale

trascorso il quale devono essere distrutti (es. con un **trita-documenti**) e non gettati nei cestini.

17. PIATTAFORME DI COLLABORATION e VIDEO-CONFERENCE

Le piattaforme di *collaboration* offrono strumenti per un supporto dell'attività lavorativa a distanza sia in tempo reale (es video conferenza, condivisione e modifica di documenti tra più persone nello stesso momento) che in modalità asincrona (es. uno spazio cloud per memorizzare condividere file).

CmTO dispone della piattaforma **Cisco Webex**, che mette a disposizione uno strumento di videoconferenza e di condivisione in tempo reale di documenti.

Gli strumenti di *collaboration*, quando vengono impiegati per condividere documenti, video o immagini, devono essere utilizzati nel rispetto delle regole di comportamento suindicate al fine di garantire la riservatezza e in generale la sicurezza delle informazioni che possono transitare sulle stesse ma anche la tutela del segreto professionale, di marchi e del *know-how* aziendale. In particolare, in relazione alla funzionalità di collaborazione in tempo reale è vietato effettuare snapshot o attivare la registrazione delle call al di fuori dei casi necessari ed espressamente autorizzati dai partecipanti (es. eventi di formazione).

È vietata la conservazione permanente, all'interno degli strumenti di collaboration, attraverso le funzioni di chat o in modalità asincrona (es. funzionalità di salvataggio file in OneDrive) di documenti contenenti dati personali per i quali è previsto esclusivamente l'utilizzo i dischi di rete aziendali o dei database applicativi. Nell'ambito di attività temporanee di trattamento che richiedano l'interazione tra autorizzati tramite strumenti di *collaboration*, i dati personali devono essere crittografati ed eliminati al termine della sessione di lavoro.

È consentito, durante l'esecuzione delle *call*, l'uso della funzione di offuscamento dello sfondo o la disattivazione della telecamera.

Le regole suindicate si applicano anche nel caso in cui vengano utilizzati strumenti di collaboration non aziendali come *Skype, Zoom, Google Meet*.

18. POLICY PER GLI INTERVENTI DI SICUREZZA E I CONTROLLI

Il personale di CmTO e del CSI incaricato che opera con funzioni di monitoraggio della sicurezza aziendale e di assistenza è autorizzato a compiere, nel sistema informatico aziendale, interventi tecnici e/o manutentivi diretti a garantire la sicurezza e la salvaguardia del sistema (es. attività di controllo, amministrazione e backup, ecc).

Tali interventi, realizzati unicamente ai fini di garanzia della sicurezza ed estranei a qualsiasi finalità di controllo dell'attività lavorativa, possono anche comportare l'accesso ai dati trattati da ciascun lavoratore, ivi compresi: le mail di posta elettronica, i siti internet acceduti, i files dei dischi di rete e locali presenti negli archivi, file personali o programmi presenti sulla postazione di lavoro.

Il personale sistemistico può in qualunque momento procedere alla rimozione di file, applicazioni, software o altro che riterrà essere pericoloso per la sicurezza aziendale o in contrasto alle regole aziendali.

Il collegamento o la visualizzazione da remoto del desktop della singola postazione di lavoro, può avvenire solo previa esplicita segnalazione all'interessato. È inoltre prevista l'effettuazione di controlli atti a limitare la diffusione di malware all'interno della rete aziendale o altri problemi di sicurezza informatica.

Per tali fini, in caso di evidenza di anomalia, vengono effettuate attività di verifica su alcune tipologie di log, tracciati dai sistemi di protezione, quali:

- dati rilevati dalle console dei sistemi antivirus (numero infezioni, tipologia, pc infettati, user di appartenenza, etc)
- log di posta e log derivanti dalla applicazione dei mail filtering (caselle di destinazione/arrivo messaggi, ora/minuti invio/ricezione, tipologia di file allegato, user, ad esclusione dei contenuti della posta)
- log dei sistemi di URL Filtering e Content Filtering (tracciatura delle URL permesse/bloccate dalle policy aziendali, tracciatura della connessione proveniente dagli IP/user, ora/minuto/secondo, server acceduto, pagina visitata, dimensioni file scaricato, numero di accessi continuativo)
- log DLP: (analisi delle tracciature dei documenti riservati acceduti; ora/minuto/secondo, tipologia di regola di controllo, IP/user che ha effettuato l'azione)
- log di accesso ai database od ai server aziendali.

A titolo meramente esemplificativo rientrano nella tipologia i controlli necessari a verificare:

- le segnalazioni di frequenti e ripetuti tentativi di connessione provenienti dalle postazioni di lavoro verso siti identificati come malevoli e pertanto bloccati, a partire da 20 connessioni/die
- le segnalazioni di tentativi continuativi provenienti dalla postazione conseguenti all'attuazione di blocchi della navigazione verso pagine di siti ritenuti a rischio per il loro contenuto, a partire da 20 connessioni/die
- gli accessi anomali (per frequenza o orario) da parte degli utenti, anche se autorizzati, a risorse di rete o documenti catalogati come riservati, a partire dalla singola connessione

Le anomalie riscontrate vengono verificate, quando possibile, con l'utente assegnatario della postazione al fine di identificare nel minor tempo possibile le cause che hanno portato alla generazione degli eventi potenzialmente malevoli e di intervenire per rimuoverne l'origine e bloccarne la diffusione. Al fine di limitare e mitigare diffusione di virus e/o malware all'interno dell'azienda, sono presenti dei filtri di analisi di rete che sono in grado di analizzare eventuali connessioni o traffico di rete anomalo tra dispositivi interni o flussi sospetti dall'interno verso l'esterno.

È inoltre possibile che per verificare il corretto utilizzo degli strumenti in dotazione vengano svolti controlli a campione mediante la raccolta e l'analisi di dati aggregati e anonimi. Nel caso di provato o constatato uso illecito o non consentito degli strumenti aziendali risultante dalla verifica delle informazioni in modalità aggregata e anonima, può essere necessario procedere alla verifica di mirate registrazioni delle sessioni di lavoro, al fine di verificare la correttezza dei comportamenti anche a fini disciplinari e al fine di fornire un riscontro all'eventuale richiesta dell'autorità giudiziaria, senza alcuna ulteriore informativa all'interessato. Il periodo di conservazione dei log generati dagli strumenti di sicurezza sopra elencati non è superiore ai 6 mesi.

Oltre alle finalità di sicurezza interna, i log vengono conservati per le seguenti finalità: statistiche, prevenzione dei reati previsti dal modello organizzativo *ex D. Lgs. 231/2001*, trasmissione dei dati all'Autorità Giudiziaria in caso di formale richiesta.

19. UTILIZZO DI STRUMENTI AZIENDALI IN AMBITO EXTRALAVORATIVO

Pur nel rispetto integrale di quanto sopra indicato (incluso il divieto di installazione di software non necessario per le attività lavorative e/o con modalità diverse da quelle ivi contemplate), CmTO ammette la fruizione di alcuni dispositivi quali PC notebook, Smartphone e Tablet in ambito extra-lavorativo a condizione che l'uso dello strumento non comporti da parte del lavoratore violazioni di norme di legge, regolamentazioni aziendali, danni economici e di sicurezza per l'azienda.

20. UTILIZZO DI STRUMENTI PERSONALI IN AMBITO LAVORATIVO (BYOD- Bring Your Own Device)

Non è generalmente consentito l'utilizzo di dispositivi personali quali notebook, tablet, o altro per le attività lavorative salvo le eccezioni necessarie e contingenti, *debitamente autorizzate* dal Dirigente/Funzionario responsabile e dalla Direzione Performance, Innovazione, ICT – QA1; trova autorizzazione (a seguito *comunicazione* alla Direzione Performance, Innovazione, ICT – QA1) l'utilizzo della propria postazione personale domestica per le esigenze legate al Lavoro Agile, laddove non sia temporaneamente disponibile una PdL aziendale, mediante comunicazione mail all'indirizzo supervisionesit@cittametropolitana.torino.it .

Analogamente, è ammesso a condizione che l'uso del dispositivo personale non comporti da parte del lavoratore violazioni di norme di legge, regolamentazioni aziendali, danni economici e di sicurezza per l'azienda, per i quali sarà ritenuto il diretto responsabile.

Non è consentito in alcun caso l'utilizzo della VPN su dispositivi personali, a meno di espressa autorizzazione della Direzione Performance, Innovazione, ICT – QA1.

21. MANCATA OSSERVANZA DELLE NORME E DELLE ISTRUZIONI

Qualora dalle attività tecniche, manutentive o di analisi, descritte nei paragrafi precedenti, dovessero essere riscontrati abusi o utilizzi degli strumenti aziendali non conformi o in violazione delle prescrizioni contenute nel presente documento così come nelle altre fonti regolamentari aziendali (ad. es. Codice Etico, Codice

Disciplinare, ecc), questi saranno segnalati alla **Direzione Risorse Umane - QA4**, per valutare l'eventuale adozione di azioni anche di tipo disciplinare.