Comune di Villafranca Padovana
Provincia di Padova

REGOLAMENTO UTILIZZO STRUMENTI INFORMATICI

Approvato con la delibera di Giunta n. 152 del 29/11/2022

Comune di
Villafranca Padovana

REGOLAMENTO PER L'UTILIZZO DELLA STRUMENTAZIONE INFORMATICA DELL'ENTE E DELLA RETE INTERNET

ARGOMENTI TRATTATI

- Utilizzo del personal computer
- Gestione ed assegnazione delle credenziali di autenticazione
- Utilizzo della rete dell'ente
- Utilizzo e conservazione dei supporti removibili
- Gestione e utilizzo della posta elettronica
- Navigazione in Internet
- Protezione antivirus
- Utilizzo di fax, fotocopiatrici, scanner e stampanti dell'ente
- Utilizzo di strumenti di telefonia mobile e/o connettività
- Partecipazione a social media
- Osservanza delle disposizioni in materia di privacy
- Mancata osservanza delle presenti regole: controlli e sanzioni
- Comunicazioni

PREMESSA

La progressiva diffusione delle tecnologie, ed il necessario utilizzo della rete informatica, rappresentanti, ormai, il principale strumento di lavoro a disposizione dei dipendenti delle pubbliche amministrazioni, potrebbe esporre l'Ente e gli utenti (meglio specificati in seguito) a rischi di carattere patrimoniale oltre a responsabilità penali conseguenti alla violazione di specifiche disposizioni di legge, con ricadute negative sia in termini di sicurezza che di immagine dell'Ente stesso.

CONSIDERAZIONI

Le risorse informatiche e telematiche dell'Ente devono ispirarsi ai principi di diligenza, correttezza e buona fede (principi questi che sono comunque sottesi al rapporto di lavoro).
La stesura del presente disciplinare è stata formulata in ottemperanza a quanto previsto:

- dal Regolamento Europeo 2016/679,
- dal D.Lgs 196/2003 e s.m.i. "Codice in materia di protezione dei dati personali",

- dalle **Linee Guida emanate dall'Autorità Garante** per la Protezione dei Dati Personali, con propria **deliberazione n. 13 del 1 marzo 2007**, sulla disciplina della navigazione in internet, sulla gestione della posta elettronica nei luoghi di lavoro e
- dalla Direttiva n. 2/09 del 26/05/2009 della Presidenza del Consiglio dei Ministri "*Utilizzo di internet e della casella di posta elettronica istituzionale sul luogo di lavoro*", ***nelle quali sono fornite indicazioni in merito al corretto uso degli strumenti informatici da parte dei lavoratori e alle modalità di controllo da parte dei datori di lavoro, al fine di evitare abusi, pur mantenendo il diritto del lavoratore ad una sfera di riservatezza anche nelle relazioni professionali.***

OBIETTIVO

Il presente Disciplinare si propone di definire l'ambito di applicazione, le modalità e le norme sull'utilizzo della strumentazione informatica, telematica e telefonica da parte degli utenti assegnatari al fine di tutelare i beni istituzionali ed evitare condotte inconsapevoli o scorrette che potrebbero esporre l'Ente a problematiche di sicurezza, di immagine e patrimoniali per eventuali danni cagionati anche a terzi.

Si precisa che le presenti regole devono essere osservate da tutti i dipendenti, senza distinzione di ruolo e/o livello, nonché da tutti i collaboratori dell'Ente, a prescindere dal rapporto contrattuale con lo stesso intrattenuto (lavoratori somministrati, tirocinanti, stagisti, volontari ecc…).

PRINCIPIO GUIDA

La regolamentazione degli strumenti e delle risorse informatiche-telematiche-telefoniche deve garantire il diritto del datore di lavoro di proteggere la propria organizzazione, salvaguardando il diritto del lavoratore a non vedere invasa la propria sfera personale.

CONTROLLI

L'insieme delle norme comportamentali da adottare è ispirato ai principi di diligenza, informazione, correttezza nell'ambito dei rapporti di lavoro e inoltre finalizzato a prevenire eventuali comportamenti illeciti dei dipendenti, pur nel rispetto dei diritti a essi attribuiti dall'ordinamento giuridico italiano.

A tale proposito, si rileva che eventuali controlli escludono finalità di monitoraggio diretto ed intenzionale dell'attività lavorativa e sono disposti sulla base della vigente normativa, con particolare riferimento alla Legge n. 300/1970 (c.d. Statuto dei Lavoratori) ed ai provvedimenti appositamente emanati dall'Autorità Garante. L'Ente esclude la configurabilità di forme di controllo istituzionali aventi direttamente ad oggetto l'attività lavorativa dell'Utente.
Non si esclude però che, per ragioni organizzative e produttive, di protezione dei dati ovvero per esigenze dettate dalla sicurezza del lavoro, si utilizzino sistemi informatici, impianti o apparecchiature dai quali derivi la possibilità di controllo dell'attività lavorativa.

L'ente, nel riservarsi il diritto di procedere a tali controlli sull'effettivo adempimento della prestazione lavorativa nonché sull'utilizzo da parte degli utenti dei beni e dei servizi informatici istituzionali (artt. 2086, 2087 e 2104 c.c.), agirà in base al principio della "*gradualità*", quindi:

- i controlli saranno effettuati inizialmente solo su dati aggregati riferiti all'intera struttura istituzionale o a specifiche aree lavorative;
- nel caso in cui si dovessero riscontrare anomalie, indizi di commissione di gravi abusi o illeciti o attività contrarie ai doveri di fedeltà e diligenza, verrà diffuso un avviso generalizzato, o circoscritto all'area o struttura lavorativa interessata, con conseguente invito ad attenersi scrupolosamente alle istruzioni impartite;
- in caso siano rilevate ulteriori violazioni, si potrà procedere con verifiche più specifiche e puntuali, anche su base individuale.

Le specifiche procedure di controllo sono riportate nel capitolo finale dei controlli di questo stesso documento.

UTILIZZO DEL PERSONAL COMPUTER

Il Personal Computer, sia fisso che portatile, affidato all'utente è uno strumento di lavoro istituzionale e non personale. Ogni utilizzo non inerente all'attività lavorativa è vietato perché può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. Il personal computer deve essere custodito con cura evitando ogni possibile forma di danneggiamento.
Il personal computer dato in affidamento all'utente permette l'accesso alla rete solo attraverso specifiche credenziali di autenticazione.

L'ente rende noto che il personale incaricato (Amministratore di sistema e/o tecnico informatico) è autorizzato a compiere interventi nel sistema informatico diretti a garantire la sicurezza e la salvaguardia del sistema stesso, nonché per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento/ sostituzione/implementazione di programmi, manutenzione hardware).
Detti interventi potranno anche comportare l'accesso in qualunque momento ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica, nonché alla verifica sui siti acceduti dagli utenti abilitati alla navigazione esterna. La stessa facoltà, sempre ai fini della sicurezza del sistema e per garantire la normale operatività dell'ente, si applica anche in caso di assenza prolungata od impedimento dell'utente.

Si prevede che l'attività su internet dei singoli utenti venga registrata in appositi *log* mantenuti dai Sistemi Informativi e regolata da appositi filtri di navigazione. Questi ultimi sono implementati mediante uno specifico software, che opera congiuntamente a un sistema proxy/web gateway, per finalità di tutela e per poter eventualmente riferire all'Autorità Giudiziaria comportamenti anomali registrati dai sistemi. In tal modo l'Ente intende prevenire il libero accesso ai siti presenti in rete da parte della generalità dei lavoratori, confinandolo ai soli siti web ritenuti conferenti con lo svolgimento delle attività lavorative (salva diversa valutazione da effettuarsi caso per caso).

La gestione dei Log è in carico all'Ente che li tratterà secondo le normative vigenti. Il personale incaricato del servizio IT ha la facoltà di collegarsi e visualizzare in remoto il desktop delle singole postazioni PC al fine di garantire l'assistenza tecnica e la normale attività operativa, nonché la massima sicurezza contro virus, spyware, malware, ecc... L'intervento viene effettuato esclusivamente su chiamata dell'utente o, in caso di oggettiva necessità, a seguito della rilevazione tecnica di problemi nel sistema informatico. In quest'ultimo caso, sempre che non si pregiudichi la necessaria tempestività ed efficacia dell'intervento, verrà data comunicazione della necessità dell'intervento stesso.

Non è consentito l'uso di programmi diversi da quelli ufficialmente installati, né viene consentito agli utenti di installare autonomamente programmi provenienti dall'esterno, sussistendo infatti il grave pericolo di introdurre virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti.

Si evidenzia che le violazioni della normativa a tutela dei diritti d'autore sul software che impone la presenza nel sistema di software regolarmente licenziato, o comunque libero e quindi non protetto dal diritto d'autore, sono sanzionabili anche penalmente.

E' presente nel sistema un software per la gestione degli applicativi sui client, con la possibilità di generare un report puntuale, contenente i software installati su ogni singolo client a scopo di controllo anonimo/difensivo.
Salvo preventiva espressa autorizzazione, non è consentito all'utente modificare le caratteristiche impostate sul proprio PC, né procedere ad installare dispositivi di memorizzazione, comunicazione o altro (come ad esempio: masterizzatori, chiavette wi-fi o bluetooth, altro).

In ogni caso, ogni utente deve prestare la massima attenzione ai supporti di origine esterna (come ad esempio: chiavette usb, hard disk esterni, ecc…), preventivamente autorizzati, avvertendo immediatamente il personale del Servizio IT nel caso in cui siano stai rilevati virus ed adottando quanto previsto nelle procedure di protezione antivirus.

Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio o in caso di suo inutilizzo. L'utente è tenuto a scollegarsi dal sistema/rete ogniqualvolta sia costretto ad assentarsi dal locale nel quale è ubicata la stazione di lavoro o nel caso ritenga di non essere in grado di presidiare l'accesso alla medesima (es. blocco del PC, screen-saver con password), al fine di evitare che persone estranee effettuino accessi non permessi. Lasciare un elaboratore incustodito connesso alla rete, può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso.

GESTIONE ED ASSEGNAZIONE DELLE CREDENZIALI DI AUTENTICAZIONE

Le credenziali di autenticazione per l'accesso alla rete vengono assegnate dal personale del Servizio IT, previa formale richiesta del Responsabile dell'ufficio/area nell'ambito del quale verrà inserito ed andrà ad operare il nuovo utente.

Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (user id), associato ad una parola chiave riservata (cloud stoan) che dovrà essere custodita dall'incaricato con la massima diligenza e non divulgata. Non è consentita l'attivazione della password di accensione (bios).

La parola chiave, per buona norma, deve essere formata:
- da lettere (maiuscole o minuscole);
- caratteri speciali e/o numeri, anche in combinazione fra loro;

Quindi, è composta da almeno otto caratteri e non deve contenere riferimenti agevolmente riconducibili all'incaricato.

È necessario procedere alla modifica della parola chiave a cura dell'utente, incaricato del trattamento; al primo utilizzo e, successivamente, ogni tre mesi, o quando abbia perduto la propria riservatezza.

UTILIZZO DELLA RETE DELL'ENTE

Per l'accesso alla rete dell'Ente ciascun utente deve essere in possesso della specifica credenziale di autenticazione. È assolutamente proibito entrare nella rete e nei programmi con un codice d'identificazione utente diverso da quello assegnato.

Le credenziali d'ingresso alla rete ed ai programmi ***sono segrete*** e vanno comunicate e gestite secondo le procedure impartite.

Le cartelle utenti presenti nei server sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto, qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità.
In particolare, nelle cartelle di rete sarà controllata la presenza di:

- categorie di file non permessi,
- file di grandi dimensioni
- file non pertinenti.

Risulta opportuno che, con regolare periodicità (almeno ogni tre mesi), ciascun utente provveda alla pulizia degli archivi, con cancellazione dei file obsoleti o inutili.
Particolare attenzione deve essere prestata alla duplicazione dei dati, essendo, infatti, necessario evitare un'archiviazione ridondante.

Si fa obbligo di salvataggio nei corretti percorsi di rete a seconda della tipologia di dato/file

UTILIZZO E CONSERVAZIONE DEI SUPPORTI REMOVIBILI

Tutti i supporti rimovibili autorizzati (CD e DVD riscrivibili, supporti USB, hard disk esterni, memorie flash, ecc.) contenenti dati riservati nonché informazioni costituenti know-how istituzionale, devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato, alterato, distrutto o, successivamente alla cancellazione, recuperato.

In ogni caso, i supporti magnetici contenenti dati riservati devono essere adeguatamente custoditi in armadi chiusi dagli utenti.

E' vietato l'utilizzo di supporti rimovibili personali. L'utente è responsabile della custodia dei supporti e dei dati aziendali in essi contenuti.

GESTIONE E UTILIZZO DELLA POSTA ELETTRONICA

La casella di posta elettronica assegnata all'utente è uno strumento di lavoro ed è quindi destinata esclusivamente all'utilizzo professionale per fini aziendali.

Si ricorda, infatti, che ***attraverso l'e-mail, gli utenti rappresentano pubblicamente l'Ente*** e per questo motivo viene richiesto loro di utilizzare tale strumento in modo lecito, professionale e comunque tale da riflettere l'immagine dell'Ente medesimo.

Tanto premesso, si rammenta che i dati e le informazioni contenute nella casella di posta elettronica istituzionale saranno inevitabilmente oggetto di salvataggio sul server dell'Ente e su altri sistemi di backup.

Al fine di garantire la riservatezza del lavoratore, è opportuno evitare che la corrispondenza personale sia oggetto del possibile e/o incidentale controllo datoriale.
In particolare:

- non è consentito inviare o memorizzare messaggi (interni ed esterni) di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica, o che costituiscano comunque condotta illecita;
- non è consentito l'utilizzo dell'indirizzo di posta elettronica per la partecipazione a dibattiti, Forum, newsletter o mail-list, non attinenti all'attività lavorativa;

Inoltre:

- in caso di assenza, al dipendente sono poste a disposizione apposite funzioni di sistema che consentano di inviare automaticamente messaggi di risposta contenenti i riferimenti di contatto di un altro soggetto o altre modalità di contatto della struttura;
- in caso di eventuali assenze non programmate (ad es. per malattia), qualora il lavoratore non possa attivare la predetta funzionalità, il Titolare

del trattamento, perdurando l'assenza oltre un determinato limite temporale pari a 2 giorni, disporrà lecitamente, sempre che sia necessario e mediante personale appositamente incaricato (ad es. l'amministratore di sistema o un incaricato istituzionale per la protezione dei dati), all'attivazione di un analogo accorgimento, avvertendo gli interessati;
- in caso di assenza improvvisa o prolungata, qualora per improrogabili necessità legate all'attività lavorativa si debba conoscere il contenuto dei messaggi di posta elettronica, l'interessato potrà delegare un altro lavoratore (c.d. fiduciario) a verificare il contenuto dei messaggi e a inoltrare al Titolare del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. Di tale attività verrà redatto apposito verbale e informato il lavoratore alla prima occasione utile.

Si fa presente, inoltre, che è fatto divieto di divulgare le notizie, i dati e qualsiasi altra informazione appresa in occasione della ricezione o invio di posta elettronica, in quanto coperte dal segreto professionale cui sono tenuti i dipendenti in ottemperanza agli obblighi di fedeltà e correttezza; è buona norma rispondere ad e-mail pervenute solo da mittenti conosciuti e cancellare preventivamente le altre; non è consigliabile collegarsi a siti internet contenuti all'interno di messaggi; è necessario mantenere in ordine la casella di posta, secondo le istruzioni ricevute.

Come previsto dall'European Data Protection Board nelle Linee Guida 1/2021 "*On examples regarding Data Breach notification*" nell'integrare le informazioni sulle violazioni dei dati già fornite dal WP 29 nelle "*Guidelines on Personal data breach notification under Regulation 2016/679, WP250"*, si raccomanda di adottare, altresì, i seguenti accorgimenti:

- utilizzare il campo "ccn" per impostazione predefinita per l'invio di e-mail a più destinatari;
- utilizzare l'impostazione per posticipare il recapito dei messaggi (in modo che il messaggio possa essere cancellato / modificato per un certo periodo di tempo dopo aver disposto l'invio);
- disabilitare il completamento automatico durante la digitazione di indirizzi di posta elettronica;
- utilizzare la posta certificata ogniqualvolta sia possibile (ad esempio se l'interessato ha una casella pec in quanto iscritto ad un ordine professionale regolamentato);
- per l'invio di comunicazioni aventi ad oggetto categorie particolari di dati, si raccomanda di trasmettere l'informazione tramite posta elettronica, eventualmente inserendo i dati particolari (es dati sulla salute) in un

allegato protetto con password (e avendo cura di non inserire nel testo/oggetto nessun riferimento ad essi);
- partecipare alle sessioni formative organizzate dall'Ente atte, altresì, a sensibilizzare il personale sugli errori più comuni che portano a una violazione dei dati personali.

In questi casi a garanzia della riservatezza del dipendente, i messaggi di posta elettronica dovranno contenere un avvertimento ai destinatari in cui si dichiara "l'eventuale natura non personale dei messaggi", precisando se le risposte potranno essere conosciute nell'organizzazione di appartenenza del mittente, con rinvio alle presenti policy.

Si raccomanda di prestare attenzione al fenomeno di "social engineering" (ingegneria sociale), utilizzato per carpire informazioni in maniera illecita. Un esempio tipico è il "phishing", ossia una pratica in cui si viene indotti a comunicare informazioni ed effettuare operazioni a seguito di e-mail o "profili fake" (spoofing).

Pertanto, a seguito di comunicazioni (email, sms, etc.) di dubbia provenienza e sospette si raccomanda di non inserire e/o inviare credenziali, non scaricare file/documenti e non aprire i link. È buona norma rispondere ad e-mail pervenute solo da mittenti conosciuti e cancellare preventivamente le altre.

Cessazione indirizzo di posta elettronica

In caso di interruzione del rapporto di lavoro con l'Utente, l'accesso all'indirizzo di posta elettronica verrà disabilitato alla data di fine rapporto di lavoro; per la posta in entrata, verrà impostato un messaggio automatico che informa che da quel momento le comunicazioni lavorative indirizzate all'account potranno essere inviate a un nuovo indirizzo; nei 6 mesi successivi alla cessazione del rapporto di lavoro, il Titolare del trattamento potrà accedere all'account se necessario per lo svolgimento dell'attività lavorativa e a mezzo di personale appositamente incaricato; decorsi i suddetti 6 mesi, si disporrà la definitiva e totale cancellazione dello stesso.

L'ente si riserva il diritto di conservare i messaggi di posta elettronica che riterrà rilevanti.

NAVIGAZIONE IN INTERNET

Il PC assegnato al singolo utente ed abilitato alla navigazione in Internet costituisce uno strumento utilizzabile esclusivamente per lo svolgimento della propria attività lavorativa. Non è, quindi, consentita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa.

In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare Internet per:

- L'upload o il download di software gratuiti (freeware) e shareware, nonché l'utilizzo di documenti provenienti da siti web o http, se non strettamente attinenti all'attività lavorativa (filmati e musica) e previa verifica dell'attendibilità dei siti in questione;
- L'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, e comunque nel rispetto delle normali procedure di acquisto; ogni forma di registrazione a siti i cui contenuti non siano strettamente legati all'attività lavorativa;
- La partecipazione a Forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames) se non espressamente autorizzati dal Responsabile d'ufficio;
- L'accesso, tramite internet, a caselle webmail di posta elettronica personale, partecipare a forum non professionali, a Social Network, ecc...

Il collegamento ad Internet da Pc istituzionali dovrà avvenire esclusivamente tramite la rete istituzionale. Non possono essere utilizzati modem privati per il collegamento alla rete.

Al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa, è stato attivato uno specifico sistema di filtraggio e blocco (firewall) che con le sue policy di sicurezza debitamente implementate ed aggiornate, impedisce determinate operazioni quali lo scarico di programmi o l'accesso a determinati siti internet inseriti in una black-list.

Si precisa che, come previsto al par. 3 "Utilizzo della Rete Internet" della Direttiva n. 2/2009 della Presidenza del Consiglio dei Ministri, l'utilizzo di internet per svolgere attività che non rientrano tra i compiti istituzionali potrebbe essere regolamentato e, quindi, consentito ai dipendenti per assolvere incombenze amministrative e burocratiche senza allontanarsi dal luogo di lavoro (ad esempio, per effettuare adempimenti on line nei confronti di pubbliche amministrazioni e di concessionari di servizi pubblici, ovvero per tenere rapporti con istituti bancari e assicurativi).

Tale modalità, purché contenuta nei tempi strettamente necessari allo svolgimento delle transazioni, avrebbe, inoltre, il vantaggio di contribuire a ridurre gli spostamenti delle persone e gli oneri logistici e di personale per l'amministrazione che eroga il servizio, favorendo, altresì, la dematerializzazione dei processi produttivi.
Tale modalità di utilizzazione di Internet deve essere contenuta nei tempi strettamente necessari allo svolgimento delle transazioni/comunicazioni e privilegiando, quando possibile, l'utilizzo delle pause di lavoro.

L'accesso alle risorse del sistema intranet dall'esterno è consentito esclusivamente tramite un collegamento che necessita di autenticazione VPN (Virtual Private network) e solo da parte di utenti autorizzati.

L'abilitazione e le credenziali di accesso vengono fornite dal personale del Servizio IT, previa richiesta formale del Responsabile dell'Ufficio/Area, verificati i requisiti di sicurezza.

PROTEZIONE ANTIVIRUS

Il sistema informatico è protetto da ***software antivirus aggiornato quotidianamente***.

Ogni utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico mediante virus o mediante ogni altro software aggressivo (ad esempio non aprile mail e/o relativi allegati di origine sospetta, non navigare su siti non professionali ecc..).

Ogni utente è tenuto a controllare la presenza e il regolare funzionamento del software antivirus istituzionale. Nel caso il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente sospendere ogni elaborazione in corso, nonché segnalare prontamente l'accaduto al personale del Servizio IT.

Ogni dispositivo magnetico di provenienza esterna all'Ente o i supporti di memorizzazione utilizzati (vv. precedente "U*tilizzo e conservazione dei supporti removibili*") dovranno essere verificati mediante il programma antivirus prima del loro utilizzo e, nel caso venga rilevato un virus non eliminabile dal software, non dovranno essere utilizzati.

UTILIZZO DI FAX, FOTOCOPIATRICI, SCANNER E STAMPANTI DELL'ENTE

Gli utenti vengono informati che i fax e gli strumenti di stampa sono di proprietà dell'Ente e sono resi disponibili all'utente per rendere la prestazione lavorativa. Pertanto, ne viene concesso l'uso esclusivamente per tale finalità, non essendo quindi consentite comunicazioni a carattere personale o comunque non strettamente inerenti all'attività lavorativa stessa.

È vietato l'utilizzo delle fotocopiatrici dell'Ente per fini personali, salvo preventiva ed esplicita autorizzazione da parte del Responsabile di Ufficio.
Per quanto concerne l'uso delle stampanti gli utenti sono tenuti a:

- Stampare documenti solo se strettamente necessari per lo svolgimento delle proprie funzioni operative e di ritirarli prontamente dai vassoi delle stampanti comuni;
- Prediligere le stampanti di rete condivise, rispetto a quelle locali/personali, per ridurre l'utilizzo di materiali di consumo (toner ed altri consumabili);
- Prediligere la stampa in bianco/nero e fronte/retro al fine di ridurre i costi, se possibile.

E' stato implementato un sistema di stampa privata tramite codice, conosciuto solamente dall'utente, per i documenti sensibili.

Le stampanti e le fotocopiatrici dell'Ente devono essere spente ogni sera prima di lasciare gli uffici o in caso di inutilizzo prolungato.

L'utilizzo dei fax per l'invio di documenti che hanno natura strettamente confidenziale, è generalmente da evitare. Nei casi in cui questo sia necessario, si deve preventivamente avvisare il destinatario, in modo da ridurre il rischio che persone non autorizzate possano venirne a conoscenza, e successivamente chiedere la conferma telefonica di avvenuta ricezione.

E' vietato l'invio di scansioni con dati sensibili dell'Ente su dischi comuni.

UTILIZZO DI STRUMENTI DI TELEFONIA MOBILE E/O DI CONNETTIVITA' IN MOBILITA'

A seconda del ruolo o della funzione del singolo utente, l'Ente rende disponibili impianti di telefonia fissa e mobile e inoltre dispositivi quali smartphone e tablet che consentono di usufruire sia della navigazione in internet tramite rete dati che del servizio di telefonia tramite rete mobile.

Le specifiche relative ai limiti entro cui l'utente potrà utilizzare tali strumenti sono riportate nella scheda tecnica consegnata unitamente al dispositivo.
L'utente dovrà attenersi ai suddetti limiti e in caso contrario potrà essere richiesto il rimborso dei costi sostenuti per il loro superamento.

Come per qualsiasi altra dotazione istituzionale, il dispositivo mobile rappresenta un bene dell'Ente concesso in uso per scopi esclusivamente lavorativi. La ricezione o l'effettuazione di comunicazioni a carattere personale è consentito solo nel caso di comprovata necessità ed urgenza. A tal fine si informano gli utilizzatori dei servizi di fonia, che il Titolare potrà richiedere ai provider di telefonia i dettagli necessari ad effettuare controlli sull'utilizzo ed i relativi costi di traffico effettuato nel tempo al fine di una corretta fatturazione. I controlli, come meglio specificato nel prosieguo, verranno effettuati secondo le modalità descritte nel prosieguo.

Ai dispositivi mobili dell'Ente si applicano le medesime regole sopra previste per gli altri dispositivi informativi (come l'indirizzo email), per quanto riguarda il mantenimento di un adeguato livello di sicurezza informatica, per le parti applicabili. In particolare, si raccomanda il rispetto delle regole per una corretta navigazione in internet.

L'utilizzo degli strumenti di telefonia mobile dell'Ente risponde alle regole che si riportano di seguito:

- Ogni Utente assegnatario del dispositivo è responsabile dell'uso appropriato dello stesso, e, conseguentemente, anche della sua diligente conservazione;
- I dispositivi devono essere dotati di password di sicurezza (cd. codice pin del dispositivo) che ne impedisca l'utilizzo da parte di soggetti non autorizzati;
- Ogni Utente deve adottare le necessarie e dovute cautele per assicurare la segretezza della password e, qualora ritenga che un soggetto non autorizzato possa esserne venuto a conoscenza, dovrà provvedere immediatamente a cambiarla dandone comunque comunicazione al Titolare;
- In caso di danneggiamento l'Utente assegnatario dovrà darne immediato avviso al Titolare, in caso di furto o smarrimento del dispositivo mobile in oggetto, l'Utente assegnatario dovrà denunciare il fatto alle competenti autorità pubbliche e darne successivo avviso al Titolare;

- Ove detti eventi siano riconducibili ad un comportamento negligente, imprudente dell'Utente e/o comunque a sua colpa nella custodia del bene, lo stesso sarà ritenuto unico responsabile dei danni derivanti;
- In caso di furto o smarrimento il Titolare si riserva la facoltà di attuare la procedura di remote-wipe (cancellazione da remoto di tutti i dati sul dispositivo), rendendo il dispositivo inutilizzabile e i dati in esso contenuti irrecuperabili;
- Non è consentito all'Utente caricare o inserire all'interno del dispositivo o SIM qualsiasi dato personale non attinente con l'attività lavorativa svolta. In ogni caso, al fine di evitare e/o ridurre al minimo la possibile circolazione di dati personali sull'apparecchio, si ricorda agli assegnatari di cancellare tutti i dati eventualmente presenti prima di consegnare il cellulare agli uffici competenti per la restituzione o la riparazione;
- È consentito all'Utente effettuare riprese, fotografie, registrazioni di suoni con qualsiasi tipologia di apparecchiatura elettronica esclusivamente adatta a scopi lavorativi/professionali;
- Non è consentito all'Utente effettuare procedure di jailbreak, modifiche del firmware o procedure di sblocco a vario titolo, tali da permettere l'illegittima installazione di software e/o applicazioni coperte da copyright;
- È onere dell'Utente mantenere installato software antivirus sullo smartphone; in caso di problemi l'Utente potrà rivolgersi all' Amministratore di Sistema;
- L'eventuale installazione di applicazioni, sia gratuite che a pagamento, sugli smartphone e tablet deve essere espressamente autorizzata, rimanendo, diversamente, a carico dell'Utente le spese che il Titolare dovrà sostenere, nonché le responsabilità derivanti dall'installazione non autorizzata;
- Salvo diversi specifici accordi, al momento della consegna del tablet o smartphone l'Utente è tenuto a verificare la disattivazione del sistema di geolocalizzazione potenzialmente attivabile sugli smartphone e tablet, consapevole che, in caso contrario, il Titolare potrebbe venire a conoscenza, seppur incidentalmente, dei dati relativi alla posizione del dispositivo stesso e del suo assegnatario.

PARTECIPAZIONE A SOCIAL MEDIA

L'utilizzo a fini promozionali di Facebook, Twitter, Linkedin, dei blog e dei forum, anche professionali (ed altri siti o social media) è gestito ed organizzato esclusivamente dall'Ente attraverso specifiche direttive ed istruzioni operative al personale a ciò espressamente addetto, rimanendo escluse iniziative individuali da parte dei singoli utenti o collaboratori.

Fermo restando il diritto della persona alla libertà di espressione, l'Ente ritiene comunque opportuno indicare agli utenti alcune regole comportamentali, al fine di tutelare tanto la propria immagine ed il patrimonio dell'Ente, anche immateriale, quanto i propri collaboratori, i propri clienti e fornitori, gli altri partners, oltre che gli stessi utenti utilizzatori dei social media, fermo restando che è vietata la partecipazione agli stessi social media durante l'orario di lavoro ed espletamento della prestazione lavorativa.
Il presente articolo deve essere osservato dall'Utente sia che utilizzi dispositivi messi a disposizione dall'Ente, sia che utilizzi propri dispositivi, sia che partecipi ai social media a titolo personale, sia che lo faccia per finalità professionali, come dipendente dell'Ente.

La condivisione dei contenuti nei social media deve sempre rispettare e garantire la segretezza sulle informazioni dell'Ente, nel rispetto del segreto d'ufficio, segreto professionale e privacy.

La condivisione dei contenuti nei social media deve sempre rispettare e garantire la segretezza sulle informazioni considerate dall'Ente riservate ed in genere, a titolo esemplificativo e non esaustivo, sulle informazioni inerenti attività, dati contabili, finanziari, progetti, procedimenti svolti o in svolgimento presso gli uffici.
Inoltre, ogni comunicazione e divulgazione di contenuti dovrà essere effettuata nel pieno rispetto dei diritti di proprietà industriale e dei diritti d'autore, sia di terzi che dell'Ente. L'utente, nelle proprie comunicazioni, non potrà quindi inserire il nominativo e il logo dell'Ente, né potrà pubblicare disegni, modelli od altro connesso ai citati diritti.

Ogni deroga a quanto sopra disposto potrà peraltro avvenire solo previa specifica autorizzazione del Titolare.

L'utente deve garantire la tutela della riservatezza e dignità delle persone; di conseguenza, non potrà comunicare o diffondere dati personali (quali dati anagrafici, immagini, video, suoni e voci) di colleghi e in genere di collaboratori, se non con il preventivo personale consenso di questi, e comunque, non potrà postare nei social media immagini, video, suoni e voci registrati all'interno dei luoghi di lavoro, se non con il preventivo consenso del Responsabile d'ufficio, salvo, in ogni caso, il rispetto delle regole imposte dalla vigente normativa in materia di protezione dei dati personali.

Qualora l'utente intenda usare social network, blog, forum su questioni anche indirettamente professionali (es. post su prodotti, servizi, fornitori, partner, ecc.) egli esprimerà unicamente le proprie opinioni personali; pertanto, ove

necessario od opportuno per la possibile connessione con l'Ente, in particolare in forum professionali, l'utente dovrà precisare che le opinioni espresse sono esclusivamente personali e non riconducibili all'Ente.

OSSERVANZA DELLE DISPOSIZIONI IN MATERIA IN PRIVACY

È obbligatorio attenersi alle disposizioni in materia di Privacy e di misure adeguate di sicurezza ai sensi del Regolamento Europeo GDPR EU 2016/679, come indicato nella lettera di autorizzazione al trattamento dei dati e relative istruzioni.

ACCESSI AI DATI TRATTATI DALL'UTENTE

E' facoltà dell'Ente, tramite il personale del Servizio IT, nel pieno rispetto della normativa sulla privacy, accedere a tutti gli strumenti informatici istituzionali e ai documenti ivi contenuti per motivi di sicurezza del sistema informatico, per motivi tecnici e/o manutentivi (ad esempio, aggiornamento, sostituzione, implementazione di programmi, manutenzione hardware), per finalità di controllo e programmazione dei costi aziendali (ad esempio, verifica costi di connessione ad Internet, traffico telefonico), estranei a qualsiasi finalità di controllo dell'attività lavorativa, nonché ai tabulati del traffico telefonico.

SISTEMA DI CONTROLLO

Il Garante alla Privacy nel provvedimento del 2007 su citato ha fornito le linee guida che bilanciano due diverse esigenze:

- il diritto di controllo da parte del datore di lavoro circa le modalità di utilizzo degli strumenti informatici, con particolare riferimento a servizi di e-mail ed accesso ad Internet, messi a disposizione degli incaricati,
- ed il diritto di questi ultimi a non subire intrusioni illecite nella propria sfera privata.

Il presente documento, deve essere considerato come integrazione dell'autorizzazione e delle istruzioni aventi ad oggetto i criteri e le modalità operative di accesso ed utilizzo del servizio internet e di posta elettronica da parte degli addetti.

Restano ferme, ove non espressamente modificate nel presente documento, tutte le indicazioni in particolare per quanto riguarda l'indicazione del Titolare del trattamento e dei diritti riconosciuti ai singoli interessati. Con riguardo al principio secondo cui occorre perseguire finalità determinate, esplicite e legittime, il datore di lavoro può riservarsi di controllare direttamente o

attraverso la propria struttura l'effettivo adempimento della prestazione lavorativa e, se necessario, il corretto utilizzo degli strumenti di lavoro (cfr. artt. 2086, 2087 e 2104 cod. civ.).

Nell'esercizio di tale prerogativa occorre rispettare la libertà e la dignità dei lavoratori, in particolare per ciò che attiene alle regole per l'installazione di apparecchiature che possano anche attivare finalità di controllo a distanza dell'attività dei lavoratori" (art. 4, l. n. 300/1970 così come aggiornata nel settembre 2015), tra cui sono certamente comprese strumentazioni hardware e software mirate al controllo dell'utente di un sistema di comunicazione elettronica.

Per queste ragioni è assolutamente proibito a chiunque ogni trattamento effettuato mediante sistemi hardware e software preordinati al controllo a distanza grazie ai quali sia possibile ricostruire, a volte anche minuziosamente, l'attività dei lavoratori.

E' il caso, ad esempio:

- della lettura e della registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio e-mail;
- della riproduzione ed eventuale memorizzazione sistematica delle pagine web visualizzate dal lavoratore;
- della lettura e della registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo;
- dell'analisi occulta di computer portatili affidati in uso.

L'ente utilizzando sistemi informativi per esigenze produttive o organizzative (ad es. per rilevare anomalie o per manutenzioni) o, comunque, quando gli stessi si rivelano necessari per la sicurezza sul lavoro, può avvalersi legittimamente, nel rispetto dello Statuto dei lavoratori di sistemi che consentono indirettamente un controllo a distanza (c.d. controllo preterintenzionale) e determinano un trattamento di dati personali riferiti o riferibili ai lavoratori.

L'ente promuove ogni opportuna misura, organizzativa e tecnologica volta a prevenire il rischio di utilizzi impropri (da preferire rispetto all'adozione di misure "repressive", come suggerisce il Garante) e, comunque, a "minimizzare" l'uso di dati riferibili ai lavoratori.

Per questo, dal punto di vista organizzativo, l'ente ha valutato e valuterà attentamente l'impatto sui diritti dei lavoratori prima dell'installazione di

apparecchiature suscettibili di consentire il controllo a distanza e dell'eventuale trattamento.

In caso di anomalie, il personale incaricato del servizio IT effettuerà controlli anonimi che si concluderanno con un avviso generalizzato diretto ai dipendenti dell'area o del settore in cui è stata rilevata l'anomalia, nei quali si evidenzierà l'utilizzo irregolare degli strumenti aziendali e si inviteranno gli interessati ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite.

Log di Sistema: il sistema registra informazioni sui siti web visitati e sulla quantità di byte scaricati o inviati.
Il file di log contiene per ogni accesso:

- l'indirizzo web del sito visitato,
- il tempo di connessione, eventuali compilazioni di form con richiesta di memorizzazione dei dati.

Il Log consente l'estrazione di dati statistici che possono evidenziare anomalie (accesso a siti non autorizzati, utilizzi non moderati del download, ecc.) che possono portare a verifiche per gruppi ampi di utenti, sui quali compiere le dovute azioni di avviso.

Le e-mail inviate e ricevute non vengono tracciate in maniera sistematica e mirata al fine di controllare le attività dell'utente; il traffico di e-mail è registrato solo per garantire un corretto servizio di posta elettronica, a fini statistici o di dimensionamento del sistema stesso.

Nessuno è autorizzato a verificare il contenuto della Posta Elettronica e dei file di log della navigazione in internet, fatti salvi i controlli da parte del datore di lavoro circa le modalità di utilizzo degli strumenti informatici e, naturalmente, per verifiche e indagini richieste dalle autorità.
Gli unici soggetti preposti al controllo operativo degli ambienti di posta elettronica e di internet sono gli Amministratori di Sistema, i quali, appositamente incaricati, agiscono con la supervisione del Titolare.
Ai soggetti preposti corre ***l'obbligo di svolgere solo operazioni strettamente necessarie al perseguimento delle finalità riconducibili alla ricerca e all'esame di situazioni anomale e alle attività di manutenzione dei Sistemi***.

E' proibito a soggetti privi dello specifico incarico da parte dell'ente di effettuare qualunque genere di attività finalizzate al controllo sulla posta elettronica e sull'accesso a Internet, anche per perseguire finalità lecite. In ogni caso, qualora

necessario, i controlli saranno comunque effettuati da un numero limitato di persone.

L'eventuale controllo sulla posta elettronica e sull'accesso a Internet è lecito solo se sono rispettati i principi di pertinenza e non eccedenza. Nel caso in cui un evento dannoso o una situazione di pericolo non sia stato impedito con preventivi accorgimenti tecnici, l'ente adotta misure che consentano la verifica di comportamenti anomali.

Chiunque tra il personale dipendente o collaboratore, può segnalare un'anomalia circa la navigazione web o l'uso della Posta Elettronica. La segnalazione va inoltrata al Titolare del Trattamento dei dati personali e/o, se presente, al proprio responsabile.

Il controllo aggregato, di sua natura anonimo, può concludersi con un avviso generalizzato relativo ad un rilevato utilizzo anomalo degli strumenti aziendali e con l'invito ad attenersi scrupolosamente a compiti assegnati e istruzioni impartite. L'avviso può essere circoscritto ad incaricati afferenti all'area o settore in cui è stata rilevata l'anomalia.
Se dopo gli opportuni controlli collettivi e i relativi avvisi, l'anomalia si ripete, possono essere effettuati controlli su base individuale, nominativi, sui singoli dispositivi e postazioni.

Deve essere inoltrato, con la dovuta riservatezza, un preventivo avviso individuale alla persona oggetto del controllo con espresse le ragioni legittime della verifica e le modalità tecniche con cui verrà effettuata.

MANCATA OSSERVANZA DELLE PRESENTI REGOLE E SANZIONI

Le presenti regole rivestono carattere di obbligatorietà e la loro mancata osservanza costituisce illecito che, quando rilevato, può portate l'Ente ad intervenire sul piano disciplinare nei confronti dell'utente, applicando il sistema sanzionatorio in vigore e, ricorrendone gli estremi, alla segnalazione dello stesso alle competenti autorità.

In caso di violazione accertata da parte degli utenti, il Responsabile privacy o l'Amministratore di sistema si riservano la facoltà di sospendere, bloccare o limitare gli accessi dell'account dell'utente coinvolto qualora appaia ragionevolmente necessario per proteggere l'integrità, la sicurezza e/o la funzionalità dei beni e degli strumenti informatici dell'Ente.

L'ente, in ottica di quanto precedentemente definito, nel caso constati che la posta elettronica e la rete Internet sono utilizzate indebitamente, può intervenire disciplinarmente nei confronti dell'Utente applicando il sistema sanzionatorio in vigore.
Rimane salva la denuncia all'autorità costituita qualora il comportamento costituisca reato.

COMUNICAZIONI

Le presenti regole sono portate a conoscenza degli utenti nei seguenti modi**:**

- Trasmissione per posta elettronica interna a tutti i dipendenti e a tutti gli utenti provvisti di un indirizzo e-mail istituzionale;
- Mediante messa a disposizione nella cartella condivisa dei Regolamenti comunali;
- Messa a disposizione, per consultazione, ai nuovi utenti al momento dell'assegnazione di un account.

Villafranca Padovana 10/11/2022