Regolamento (UE) 2016/679

del Parlamento europeo e del Consiglio, del 27 aprile 2016
relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali

Regolamento interno per l'utilizzo dei sistemi e strumenti informatici e posta elettronica

01 SCOPO E AMBITO DI APPLICAZIONE

Scopo del presente documento è disciplinare l'utilizzo delle postazioni di lavoro da parte del personale dipendente. Le indicazioni contenute devono essere applicate per un corretto utilizzo delle risorse informatiche messe a loro disposizione per lo svolgimento delle proprie attività oltre a dettare norme comportamentali.

02 PRINCIPI GENERALI

Nell'impartire le seguenti prescrizioni, il Centro Servizi tiene conto del diritto alla protezione dei dati personali, della necessità che il trattamento sia disciplinato assicurando un elevato livello di tutela delle persone. Le prescrizioni potranno essere aggiornate alla luce dell'esperienza e dell'innovazione tecnologica. I trattamenti rispettano le garanzie in materia di protezione dei dati e si svolgono nell'osservanza dei principi di necessità, correttezza, per finalità determinate, esplicite e legittime osservando il principio di pertinenza e non eccedenza e nella misura meno invasiva possibile.
Il Centro Servizi, utilizzando sistemi informativi per esigenze produttive o organizzative o, comunque, quando gli stessi si rivelano necessari per la sicurezza sul lavoro, si avvale legittimamente, nel rispetto dello Statuto dei lavoratori , di sistemi che potrebbero consentire indirettamente un controllo a distanza e determinano un trattamento di dati personali riferiti o riferibili ai lavoratori. Il trattamento di dati che ne consegue è considerato lecito.

L'Ente rispetta le procedure d'informazione ai lavoratori in relazione all'introduzione o alla modifica di sistemi automatizzati per la raccolta e l'utilizzazione dei dati, nonché in caso di introduzione o di modificazione di procedimenti tecnici destinati a controllare i movimenti o la produttività dei lavoratori.

Il regolamento, inoltre, oltre a dettare una disciplina per l'utilizzo degli strumenti informatici/telefonici aziendali, vuole costituire un utile strumento per sensibilizzare il personale su altri aspetti, altrettanto importanti, nella gestione dei sistemi informatici aziendali, quali il rispetto della normativa sulla tutela legale del software (e quindi il controllo sulla regolarità del software presente nello stesso sistema informatico), e quella sulla tutela del know-how aziendale, quando queste importanti informazioni di proprietà dell'impresa sono custodite nel sistema informatico.

Tra l'altro, se correttamente applicato e fatto rispettare, il regolamento può essere anche un efficace strumento per limitare il rischio d'insorgenza della responsabilità amministrativa a carico dell'Ente: si ricorda, infatti, che, alla luce della normativa vigente, può essere soggetto all'applicazione di sanzioni pecuniarie e interdittive, nel caso di commissione da parte di un dipendente di specifici reati.

03 DESTINATARI

Destinatario del presente documento è da considerarsi tutto il personale del Centro Servizi, dotato di una stazione di lavoro informatizzata, senza distinzione di ruolo e/o livello, nonché a tutti i collaboratori dell'Ente stesso, a prescindere dal rapporto di collaborazione contrattuale intrattenuto (lavoratori somministrati, collaboratori a progetto, in stage, ecc.).

04 DESCRIZIONE DEL DOCUMENTO

Le risorse, hardware e software, in dotazione al personale quali personal computer, notebook, tablet, Smartphone, chiavette UMTS, stampanti, scanner, applicazioni gestionali e di business, software di base, strumenti di sviluppo, programmi di utilità, ecc. (d'ora in avanti "dispositivi informatici") costituiscono un valore strategico per il Centro Servizi e come tali devono essere adeguatamente protette.

Al fine di ridurre al minimo i rischi d'indisponibilità, accesso non autorizzato, distruzione o perdita, anche accidentale, di informazioni il Centro Servizi ha definito:

- linee di comportamento atte ad impedire il presentarsi di problemi e/o minacce alla sicurezza nel trattamento dei dati
- regole per l'accesso, l'utilizzo e la protezione delle proprie risorse informative da parte del personale aziendale

L'utilizzo improprio della postazione di lavoro e/o l'introduzione di software diverso da quello fornito e installato dal personale autorizzato dal Centro Servizi, potrebbero compromettere il corretto funzionamento dei beni informatici e arrecare danni quali accessi abusivi, virus informatici, trattamento illecito, sia alle apparecchiature in dotazione sia alla rete.

Gli utenti hanno diritto ad accedere alle risorse informatiche aziendali per le quali sono stati espressamente autorizzati e ad utilizzarle esclusivamente per gli scopi inerenti le mansioni svolte.

Pertanto ogni soggetto è tenuto a:

- adottare, nell'ambito delle proprie attività, tutte le misure di sicurezza atte a prevenire la possibilità di accessi non autorizzati, furti, frodi, danneggiamenti, distruzioni o altri abusi nei confronti delle risorse informatiche;
- attuare le suddette prescrizioni, anche attraverso l'adozione delle modalità d'utilizzo riportate nel presente documento, ed a segnalare eventuali violazioni alle medesime o situazioni che possano presentare dubbi relativamente alla sicurezza delle informazioni trattate;
- non rivelare in nessun caso informazioni utili ad attaccare il sistema informatico (quali password, contenuto di files di configurazione, indirizzi IP delle postazioni, numeri telefonici di modem, ecc.). Si fa presente che è punibile penalmente chiunque, a scopo di profitto o per recare danno, si procura, o fornisce ad altri, "codici, parole chiave o altri mezzi idonei all'accesso" a un sistema informatico "protetto da misure di sicurezza".

05 LINEE GUIDA PER L'USO DEI DISPOSITIVI INFORMATICI

I dispositivi informatici affidati al dipendente sono strumenti di lavoro ed ogni utilizzo non inerente l'attività lavorativa può generare disservizi e costi di manutenzione, pertanto gli utenti

devono essere consapevoli delle loro specifiche responsabilità nella custodia e nel corretto utilizzo della propria stazione di lavoro.

06 CUSTODIA DELLA POSTAZIONE DI LAVORO

Il dipendente/collaboratore è direttamente responsabile dei dispositivi informatici a lui assegnato pertanto:

- deve attivare manualmente lo screen saver (o configurarlo automaticamente) in modo che in caso di assenza temporanea dall'ufficio attraverso la pressione simultanea dei tasti CTRL-ALT-CANC e la selezione dell'opzione "Blocca Computer", al fine di impedire durante l'assenza, l'accesso alle applicazioni da parte di personale non autorizzato;
- spegnere la postazione ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio o in caso di suo inutilizzo. In ogni caso, 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;
- non deve modificare le caratteristiche impostate sul proprio PC. E' vietato installare software, sia esso freeware o di pubblico dominio, dispositivi quali modem e/o router esterni, chiavette per la navigazione Internet non previste nella configurazione standard del personal computer assegnato.

Oltre a quanto fin qui riportato, per i dispositivi mobili (notebook, smartphone, tablet, iPad ecc.) devono essere prese ulteriori misure cautelative al fine di custodirli con diligenza. È buona regola adottare ogni misura idonea a prevenire la sottrazione del dispositivo mobile o di parte di accessori del medesimo, anche quando vengono lasciati all'interno dei locali lavorativi e non, ed evitare di lasciare, anche solo temporaneamente, i dispositivi mobili incustoditi. In caso di furto o smarrimento di dispositivi informatici dotati di collegamento alla rete del Centro Servizi, l'utente deve immediatamente avvisare l'ufficio CED dell'Azienda, che attuerà i provvedimenti cautelativi del caso.

07 ACCESSO ALLE RISORSE INFORMATICHE

Gli strumenti adottati dal Centro Servizi per l'accesso alle risorse informatiche (es. codici di accesso, user-id, token crittografici) sono di uso strettamente personale e l'utente è tenuto a custodirli in modo appropriato.

Gli accessi alla rete aziendale, alla posta elettronica, al sistema di archiviazione delle mail e in generale a tutte le applicazioni aziendali sono regolati da uno o più set di credenziali individuali (composti di un username e una password), le quali dovranno essere custodite dal personale aziendale con la massima diligenza, non divulgate e non devono essere memorizzate in funzioni di log-in automatico. Tali credenziali dovranno essere configurate in modo che non siano facilmente individuabili (devono contenere lettere minuscole, maiuscole, numeri e caratteri speciali) e che abbiano una lunghezza non inferiore agli 8 (otto) caratteri o, comunque, non inferiore al numero di caratteri stabilito dalla normativa in essere (è ammesso un numero di caratteri inferiore solo se il sistema operativo utilizzato ne dovesse limitare il numero. In questo caso l'utente dovrà, comunque, utilizzare il numero massimo di caratteri consentiti). Sono da evitare password che siano riconducibile ad informazioni personali (nome, cognome, luogo di nascita, username, ecc.), che contengano parole semplici ("password", "pa$$word", "accesso", ecc.), serie di tasti ("qwerty" , "qazwsx", "123456", ecc.) o sequenze ("abcd1234", "aaaaaa", ecc.). L'utente può essere chiamato a

rispondere, oltre che per i propri fatti illeciti, anche per quelli commessi da chiunque utilizzi il suo codice identificativo e la sua password in seguito ad un suo negligente comportamento sulla custodia delle credenziali di accesso o ad una impostazione di una password che non rispetti i requisiti sopra esposti.

A fronte di problemi di accesso alle postazioni di lavoro riconducibili ad una errato inserimento della password, sia esso dovuto ad incuria nella digitazione o dimenticanza della stessa, che causano un blocco dell'account, si rimanda al paragrafo 17 ove viene specificata la corretta procedura da utilizzare dagli utenti per la richiesta di assistenza IT al personale autorizzato dall'azienda.

Il personale aziendale è tenuto a seguire le seguenti istruzioni:

- non è possibile conservare sul proprio Personal Computer i dati inerenti la propria attività lavorativa, ma è obbligo utilizzare le cartelle di rete messa a disposizione, siano esse ad accesso condiviso (share di gruppo) od esclusivo (share ad accesso riservato del singolo utente);
- si ricorda che tutti i dischi o altre unità di memorizzazione locali (es. disco C: interno PC) non sono soggette a salvataggio da parte del personale IT;
- non è possibile condividere sul proprio computer cartelle con altri utenti, in modo tale da evitare accessi non regolamentati e non controllati alla propria postazione;
- non è consentito inserire una password di accensione (a livello di bios);
- è assolutamente proibito entrare nella rete e nei programmi con un codice d'identificazione utente diverso da quello assegnato;
- non è consentito avere sulla propria postazione di lavoro e/o su share di rete materiale in formato elettronico di carattere personale (foto, documenti non attinenti alla mansione svolta, film, musica).

La rete aziendale si basa sul protocollo TCP/IP. Tutte le apparecchiature connesse alla rete sono configurate per ricevere l'indirizzo IP dinamicamente dal server DHCP, oppure con un IP assegnato staticamente secondo la tipologia di apparecchiatura.

Il personale aziendale è tenuto a seguire le seguenti istruzioni:

- non è consentito collegare alla rete aziendale (fissa o wireless) qualunque tipo di dispositivo personale (notebook, smartphone, tablet, iPad, ecc.) o non preventivamente autorizzato;
- è assolutamente vietato connettere alla rete apparati configurati con indirizzo IP statico, assegnato direttamente dall'utente, senza una preventiva autorizzazione dall'Amministratore di sistema. Introdurre una macchina con un IP duplicato potrebbe causare un conflitto con l'indirizzo di un server, oppure di un altro dispositivo della rete stessa e causare gravi malfunzionamenti;
- non è ammessa la connessione alla rete aziendale di apparati atti a effettuare connessioni con altre reti verso l'esterno (router, bridge, modem, ecc.);
- è fatto assoluto divieto di configurare servizi già messi a disposizione in modo centralizzato, quali ad esempio, e non solo, DNS (Domain Name Service), DHCP (Dynamic Host Configuration Protocol), NTP (Network Time Protocol), mailing, accesso remoto, proxy server;
- è fatto assoluto divieto di intercettare e analizzare i pacchetti sulla rete del Centro Servizi,

utilizzando analizzatori di rete sia software sia hardware.

08 UTILIZZO DEL SOFTWARE

Non è consentito l'uso di programmi diversi da quelli distribuiti e installati ufficialmente dalle strutture preposte cosi come non è consentito installare autonomamente programmi. Eventuali richieste d'installazione devono essere inoltrate all'ufficio CED e nel caso installerà quanto richiesto (si rimanda al paragrafo 17 per un maggior dettaglio inerente le modalità di richiesta).

L'inosservanza di questa disposizione, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre l'Ente a gravi responsabilità civili e penali in caso di violazione 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.

A tal proposito il Centro Servizi effettua periodici controlli sui dispositivi informatici volti a rilevare l'eventuale presenza di software non autorizzato. Tale attività non prevede in nessun caso il monitoraggio, neppure preterintenzionale, delle attività del lavoratore o del contenuto di dati personali nel PC.

In ogni caso, il dipendente sarà responsabile e sarà chiamato a manlevare e tenere indenne l'Ente da qualsiasi danno o richiesta di risarcimento che sia avanzata da soggetti terzi.

Si evidenzia, inoltre, che nessun tipo di dato, con qualsiasi modo e qualsiasi supporto, può essere portato all'esterno del Centro Servizi.

09 UTILIZZO DI DISPOSITIVI ESTERNI O RIMOVIBILI

- NON è consentito l'utilizzo di dispositivi esterni PERSONALI (dischetti, CD e DVD riscrivibili, supporti USB, ecc.);
- Laddove si rendano necessari per fini lavorativi dispositivi quali chiavi USB, hard disk esterni, supporti ottici, schede di memoria SD/xD/CF… ecc. devono essere autorizzati, richiesti e acquistati secondo le procedure aziendali in essere;
- Tutti i supporti magnetici rimovibili (dischetti, CD e DVD riscrivibili, supporti USB, ecc.), contenenti dati sensibili e informazioni costituenti know-how aziendale, devono essere trattati con particolare cautela, onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto o, successivamente alla cancellazione, recuperato;
- In ogni caso, i supporti magnetici contenenti dati sensibili devono essere dagli utenti adeguatamente custoditi;
- L'utente è responsabile della custodia dei supporti e dei dati aziendali in esso contenuti

10 PREVENZIONE DEI VIRUS INFORMATICI

Ogni personal computer affidato agli utenti è dotato di un software antivirus centralizzato ad aggiornamento automatico, al fine di prevenire l'introduzione di virus informatici che possano compromettere l'integrità del software e delle stazioni di lavoro.

L'utente deve sempre tenere conto del fatto che il programma antivirus non fornisce una protezione assoluta e in particolare tra due aggiornamenti consecutivi esiste una finestra temporale di rischio, entro la quale si possono introdurre virus non ancora noti dal programma stesso.

Pertanto sarà cura dell'utente rispettare le seguenti linee guida:

- mantenere la configurazione del sistema operativo in modo da permettere la visualizzazione dell'estensione dei file. Tale accorgimento rende più difficile il mascheramento da parte di file potenzialmente pericolosi (programmi EXE e script di vario tipo) che impiegano estensioni doppie (es. "leggimi.txt.vbs" oppure "logo.jpg.exe");
- è fatto divieto disabilitare, disattivare i servizi relativi o modificare le impostazioni al software dell'antivirus;
- ripulire immediatamente le stazioni che si rivelino, o siano segnalate, come infette, segnalando qualsiasi sospetta presenza di virus che pregiudichi o abbia pregiudicato il sistema, ed eventualmente interrompendo qualsiasi attività nel caso in cui l'azione di ripulitura non andasse a buon fine. In tal caso è opportuno procedere alla disconnessione fisica dalla rete, scollegando il cavo di rete o spegnendo il dispositivo informatico;
- porre la massima attenzione nel ricevere, per necessità di svolgimento della propria attività lavorativa, contenuti dalla rete Internet (es. documenti di testo, tabelle, ecc.) cercando di valutare l'attendibilità dal sito cui si è collegati (ad es. valutando all'interno dell'URL la presenza di estensioni a dominio di dubbia liceità e/o utilizzo dell'indirizzo IP al posto del nome di dominio).

Nell'utilizzo della posta elettronica:

- evitare di aprire allegati che contengono un'estensione doppia o con estensione JS, VBS, SHS, PIF, EXE, COM o BAT;
- se si ricevono e-mail non richieste o con contenuti pubblicitari, evitare di seguire i collegamenti a indirizzi Web eventualmente presenti nel testo delle e-mail;
- nel caso si riceva un messaggio di e-mail da una persona conosciuta, ma con un contenuto insolito, effettuare un controllo con il mittente prima di aprire l'eventuale allegato; infatti alcuni virus sono in grado di trasmettere messaggi con allegati che sembrano spediti da mittenti conosciuti;
- evitare di cliccare su icone dall'apparenza innocua che ricordano applicazioni associate ad immagini o musica, mostrate dagli allegati di posta elettronica in quanto possono nascondere "worm".

11 CARTELLE DI RETE CONDIVISE

Le cartelle di rete sono aree di condivisione d'informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto qualunque file personale o che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità.

All'interno di tali cartelle devono essere identificate delle sottocartelle, chiaramente riconducibili all'utente, che devono essere da lui utilizzate come repository del backup dei dati eventualmente conservati nella postazione di lavoro assegnata o come locazione per la conservazione dei documenti trattati nel proprio lavoro.

Particolare attenzione deve essere prestata alla duplicazione dei dati sulle unità di rete. È assolutamente da evitare un'archiviazione ridondante.

12 UTILIZZO DELLE STAMPANTI DI RETE / DOCUMENTAZIONE

È cura dell'utente effettuare la stampa dei dati solo se questa è strettamente necessaria e di ritirarla prontamente dai vassoi delle stampanti comuni, in quanto è buona regola non dimenticare documenti nelle stampanti, fotocopiatrici o fax.

In caso di stampa di documento nelle stampanti poste in aree comuni il titolare della stampa dovrà:

- recarsi immediatamente presso la postazione oggetto della richiesta di stampa;
- attendere il completamento dell'operazione di stampa e ritirare tutti i fogli generati;
- distruggere fogli stampati erroneamente;
- segnalare eventuali blocchi o anomalie riscontrate in fase di stampa.

Analogamente per la trasmissione/ricezione via fax l'utente dovrà attendere il rapporto di trasmissione stampato dall'apparecchio fax.

Ogni documentazione stampata/ricevuta dovrà essere riposta nei propri spazi di archiviazione (armadi, cassettiere, ecc.) evitando di lasciare carteggi sulla propria scrivania, in particolar modo quando si termina l'attività giornaliera o si è assenti per un periodo prolungato.

13 UTILIZZO DI INTERNET

Il libero accesso alla rete Internet espone il Centro Servizi e i dipendenti a rischi di natura patrimoniale, oltre alle responsabilità penali conseguenti alla violazione di specifiche disposizioni di legge riguardanti il diritto d'autore e la legge sulla privacy, creando evidenti problemi alla sicurezza.

Il personal computer e/o dispositivo mobile costituisce uno strumento aziendale necessario allo svolgimento della propria attività lavorativa. È quindi da ritenersi **PROIBITA** la navigazione in Internet attraverso il personal computer e/o dispositivi mobili in dotazione per motivi diversi da quelli strettamente concernenti lo svolgimento dell'attività lavorativa stessa.

È inoltre fatto divieto all'utente:

- 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;
- l'effettuazione di ogni genere di transazione finanziaria, ivi comprese le operazioni di remote banking, acquisti on-line e simili, fatti salvi i casi direttamente autorizzati dall'Azienda e comunque nel rispetto delle normali procedure di acquisto;
- la partecipazione a forum non professionali;
- l'utilizzo di chat (esclusi gli strumenti espressamente autorizzati);
- l'utilizzo di bacheche elettroniche;
- le registrazioni in guest books anche utilizzando pseudonimi (o nicknames);
- l'utilizzo di social networks;
- ogni forma di registrazione a siti i cui contenuti non siano strettamente legati all'attività

lavorativa;
- ogni altra attività che possa essere potenzialmente dannosa per il Centro Servizi.

La navigazione Internet per gli utenti all'interno della rete del Centro Servizi è regolamentata in modo da tutelare l'Ente nell'ambito della vigente normativa attraverso un sistema di Web Filtering, che consente la definizione e l'applicazione di policy sull'utilizzo di Internet.

Al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa il Centro Servizi quindi, rende nota l'adozione di uno specifico sistema di blocco o filtro automatico, che previene determinate operazioni quali l'upload o l'accesso a determinati siti inseriti in una black list.

Ai fini del controllo della regolarità del traffico internet e dell'efficienza della banda utilizzata, la navigazione internet può essere sottoposta a monitoraggio e registrazione.

14 POSTA ELETTRONICA/INVIO SMS TRAMITE POSTA ELETTRONICA

La casella di posta elettronica assegnata all'utente è uno strumento di lavoro che rimane di esclusiva proprietà del Centro Servizi, anche dopo la cessazione del rapporto lavorativo, pertanto le persone assegnatarie sono direttamente responsabili del corretto utilizzo e funzionamento, e devono mantenerla in ordine, cancellando documenti inutili e soprattutto allegati di grandi dimensioni.

Si evidenziano le seguenti regole comportamentali:
- la posta elettronica e l'invio di sms tramite posta elettronica non vanno utilizzati ai fini personali, ma unicamente a fini lavorativi. La posta elettronica non va utilizzata come strumento di archiviazione dati, che viene assicurata attraverso altri canali, quali ad es. lo spazio messo a disposizione nelle unità di rete. In ogni caso il dipendente, salvo il caso fortuito o evento tecnico a lui non imputabile, si impegna a preservare il contenuto delle mail comprensivo di tutti i dati;
- la lista dei destinatari della corrispondenza elettronica deve essere strettamente limitata alle persone che hanno effettiva necessità di essere messe a conoscenza del contenuto del messaggio stesso;
- la comunicazione di lavoro inquadrata all'interno di un'organizzazione deve rispondere a requisiti di efficienza e di pertinenza, ed in termini generali deve pertanto essere inviata solamente alla persona titolata a gestire l'informazione;
- tramite l'indirizzo di posta elettronica possono essere inviati file allegati; l'invio deve essere commisurato alla capacità delle infrastrutture adottate al fine di non causare l'indisponibilità dei sistemi e dei dati;
- la casella di posta deve essere mantenuta in ordine, cancellando documenti inutili, posta non necessaria, allegati di grosse dimensioni;
- è vietato l'utilizzo della posta aziendale per la partecipazione a dibattiti, forum o mailing-list salvo diversa ed esplicita autorizzazione o necessità legate alle attività lavorativa opportunamente giustificate;
- sono da evitare messaggi estranei al rapporto di lavoro o alle relazioni tra colleghi;
- è obbligatorio controllare i file allegati ai messaggi di posta elettronica prima del loro utilizzo (non eseguire il download di file eseguibili o documenti da siti Web o Ftp non conosciuti).

Nella configurazione standard, gli utenti aziendali assegnatari della casella di posta elettronica:

- accedono al server di posta con credenziali a loro assegnate al momento della creazione dell'account;
- utilizzano una mailbox che può essere soggetta a parametri di configurazione specifici (arco temporale o dimensione massima) determinati dalla mansione dell'utente;
- usufruiscono del servizio di backup centralizzato essendo i messaggi depositati direttamente sul server.

E' possibile abilitare la funzionalità di risposta automatica. In tale messaggio, ogni lavoratore, può indicare le informazioni per contattare un altro collega (ad esempio nome, email e/o telefono) in caso di necessità o di urgenza.

In caso di assenza programmata e prolungata del lavoratore e nell'impossibilità di consultare la posta da remoto, il titolare della casella di posta elettronica deve impostare, mediante opportuna configurazione il messaggio di "fuori sede" nel quale specifica:

- la durata del periodo di assenza;
- gli eventuali contatti e-mail alternativi.

Nella comunicazione dell'assenza, propria o di colleghi di lavoro, è vietato specificare la motivazione dell'assenza, (es. per malattia, maternità ecc.) in quanto si tratterebbe di trattamento di dati sensibili non autorizzato dal titolare.

Per quanto concerne l'utilizzo di servizi di posta elettronica personali esterni al Centro Servizi:

- non sono consentiti quelli che implichino la configurazione di un client di posta basati su protocollo POP3 o IMAP;
- è consentita fuori dall'orario di lavoro o durante le pause l'accesso a servizi di posta elettronica tramite Webmail, se il sito specifico non è in contraddizione rispetto ai controlli che regolano la navigazione Internet.

L'utente deve adeguare la propria firma nelle mail in modo uniforme allo standard del Centro Servizi come da esempio di riportato di seguito, e non sono ammesse altre varianti di firma, salvo deroga autorizzata del Centro Servizi o traduzione del testo stesso in altra lingua:

(nome e cognome)

(funzione)

DATI DEL CENTRO SERVIZI

L'apertura di messaggi di posta, in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, è subordinata all'intervento da parte di un altro soggetto indicato dall'utente, che verificherà il contenuto dei messaggi e inoltrerà al titolare del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. Nel caso la password utilizzata dell'utente per l'accesso non sia disponibile, il Responsabile Sistemi Informativi provvederà alla modifica della configurazione utente con una nuova password; di tale eventualità verrà data specifica informativa al dipendente interessato.

In caso di cessazione del rapporto di lavoro, il Centro Servizi potrà, in modo facoltativo, inserire un avvertimento ai destinatari nel quale sia dichiarata la fine della collaborazione del dipendente con l'Ente. Il disclaimer sarà attivo per un periodo definito dalla Direzione aziendale in base alla mansione del lavoratore, e in ogni caso non superiore a un mese. Durante tale periodo, al fine di gestire le nuove richieste, le e-mail in arrivo potranno essere inoltrate ad altro dipendente. Trascorso il termine, la casella di posta elettronica del dipendente cessato sarà disabilitata.

15 UTILIZZO DEI TELEFONI , FAX E FOTOCOPIATRICI AZIENDALI

Telefono fisso
Il telefono aziendale affidato all'utente è uno strumento di lavoro. Ne è concesso l'uso esclusivamente per lo svolgimento dell'attività lavorativa, non essendo quindi consentite comunicazioni a carattere personale o comunque non strettamente inerenti all'attività lavorativa stessa. La ricezione o l'effettuazione di telefonate personali sono consentite solo nel caso di comprovata necessità e urgenza. Ai fini del controllo della regolarità del traffico telefonico e dell'efficienza della banda utilizzata, l'utilizzo della fonia può essere sottoposto a monitoraggio e registrazione.

Utilizzo telefono cellulare
Qualora fosse assegnato un cellulare aziendale all'utente, quest'ultimo sarà responsabile del suo utilizzo e della sua custodia. Al cellulare dell'Ente si applicano le medesime regole sopra previste per l'utilizzo del telefono aziendale: in particolare è vietato l'utilizzo del telefono cellulare messo a disposizione per inviare o ricevere SMS o MMS di natura personale o comunque non pertinenti rispetto allo svolgimento dell'attività lavorativa. E' vietata, inoltre, l'installazione di app o altro software di qualsiasi tipologia se non preventivamente concordato con l'Ente. L'eventuale uso promiscuo (anche per fini personali) del telefono cellulare aziendale è possibile soltanto in presenza di preventiva autorizzazione scritta . In caso di furto o smarrimento dell'apparecchio il dipendente dovrà darne immediata comunicazione al Centro Servizi, ai fini dell'immediato blocco dell'utenza. Se il furto o lo smarrimento si verificano in circostanze o in tempi in cui non è possibile comunicare con l'Ente, il dipendente dovrà provvedere personalmente al blocco della Sim contattando il gestore di telefonia mobile. Il dipendente dovrà quindi presentare la formale denuncia di furto o smarrimento e farne pervenire copia all'Ente per gli adempimenti successivi. E' obbligatorio l'uso del PIN di sicurezza della SIM. Ai fini del controllo della regolarità dell'uso del telefono potrà essere chiesto alla compagnia telefonica il dettaglio delle chiamate e il dettaglio di eventuali servizi a pagamenti utilizzati o attivati.

Utilizzo fax
Analogamente alla posta elettronica il servizio fax è considerato, per motivi organizzativi, una componente del circuito di comunicazione aziendale e, quindi, viene trattato con le stesse regole di un qualsiasi documento aziendale. È vietato, quindi, l'utilizzo dei fax aziendali per fini personali, tanto per spedire quanto per ricevere documentazione, salva diversa esplicita autorizzazione da parte del Responsabile di ufficio.

Utilizzo fotocopiatrici /scanner
È vietato l'utilizzo delle fotocopiatrici e/o scanner aziendali per fini personali, salvo preventiva ed esplicita autorizzazione da parte del Responsabile di ufficio.

16 ACCESSO ESTERNO RETE AZIENDALE

Su richiesta, se giustificata da comprovati motivi che comportino l'assenza dal posto di lavoro, è possibile attivare un accesso esterno alla rete aziendale assicurato tramite VPN.

Si evidenziano le seguenti regole comportamentali:

- il dispositivo/personal computer utilizzato per il collegamento VPN è da considerarsi dispositivo collegato alla rete aziendale, pertanto valgono tutti gli accorgimenti e prescrizioni per l'utente previste dal presente documento, sia durante la sessione di collegamento in VPN sia durante l'utilizzo del dispositivo/pc in locale;
- è compito e responsabilità dell'utente assicurarsi che il sistema operativo del dispositivo utilizzato per il collegamento VPN sia aggiornato e che sia protetto da antivirus aggiornato;
- l'utente deve assicurarsi che il dispositivo non venga utilizzato da altri;
- le credenziali fornite all'utente per il collegamento VPN sono personali e all'utente è proibito cederle o permettere ad altre persone il collegamento VPN alla rete aziendale;
- è proibito trasferire/copiare file dalla rete aziendale al dispositivo locale sia in download che in upload;
- in nessun caso l'utente può eseguire lavori per conto proprio o per terzi utilizzando le attrezzature assegnategli;
- in occasione dei rientri il dipendente è tenuto, salvo eccezione motivata ed accolta, a portare in ufficio e ad utilizzare la postazione mobile assegnata, al fine di evitare la duplicazione dei costi relativi alle attrezzature.

A fini di controllo della regolarità dei collegamenti VPN alla rete aziendale e di efficienza nell'utilizzo della banda internet, l'orario di inizio, di fine e la durata dei collegamenti VPN di ogni utente potrà essere oggetto di monitoraggio e registrazione.

17 RICHIESTA DI ASSISTENZA

Per quanto concerne le richieste di assistenza IT siano esse riguardanti qualsiasi problematica inerente alle postazioni di lavoro, ai dispositivi in genere (stampanti, scanner ecc.) e/o alle applicazioni aziendali e/o generici dubbi su quale comportamento adottare, la procedura prevede l'invio della richiesta al personale IT aziendale tramite mail (……..). Solo nel caso d'impossibilità nell'utilizzare la propria postazione e/o la propria posta elettronica è possibile aprire la richiesta a mezzo telefono.

Le richieste di assistenza concernenti lo sblocco account o reset della password possono essere richieste solo dal titolare delle credenziali.

L'intervento risolutivo potrà essere eseguito direttamente sul PC dell'utente, oppure attraverso collegamento remoto. Il personale incaricato del servizio IT ha quindi l'autorizzazione a collegarsi e visualizzare in remoto il desktop delle singole postazioni PC al fine di garantire l'assistenza tecnica e la normale attività operativa, e la massima sicurezza contro virus, spyware, malware, etc. L'intervento sarà effettuato su chiamata dell'utente o, in caso di oggettiva necessità, a seguito della rilevazione tecnica di problemi nel sistema informatico e telematico. Sempre che non si pregiudichi la necessaria tempestività ed efficacia dell'intervento sarà data comunicazione della necessità dell'intervento stesso.

18 CONTROLLI

Premesso che i sistemi hardware e software installati non sono preordinati al controllo a distanza ed in particolare:

- non vengono registrati sistematicamente i messaggi di posta elettronica al di là di quelli necessari per svolgere tecnicamente il servizio di e-mail;
- non viene memorizzata sistematicamente ogni pagina web visualizzata dal lavoratore;
- non vengono analizzati e registrati i caratteri inseriti tramite la tastiera o altro dispositivo di input;
- non vengono analizzati in modo occulto i personal computer e portatili in modo particolare.

Controlli saltuari o occasionali per ragioni legittime, specifiche e non generiche, saranno effettuati esclusivamente dal personale CED. Tali ragioni legittime possono essere:

- blocco del PC;
- infezione da virus non rilevato dal sistema di sicurezza;
- guasto di elementi hardware che rendono impossibile la prosecuzione dall'attività lavorativa;
- instabilità o blocco di sistemi software;
- instabilità o blocco della Linea Internet.

Graduazione dei controlli: i controlli iniziali, riferibili a navigazioni non aziendali e comunque non autorizzate, saranno riferiti alla totalità degli utenti. Il perdurare delle attività di navigazione non consentite autorizzano l'azienda a scendere ulteriormente nel particolare effettuando controlli al livello di gruppi omogenei. In caso di estrema ratio, qualora si rilevino ulteriori abusi che possano precludere la sicurezza dei sistemi informativi, possano essere lesivi del patrimonio aziendale e possano identificare anche reati di natura penale, l'attività di controllo verrà effettuata con modalità di identificazione personale.

Il personale del Servizio IT è autorizzato a procedere, in qualunque momento, alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la Sicurezza o palesemente estranei allo svolgimento dell'attività lavorativa sia sulle singole postazioni sia sulle unità di rete.

Il datore informa che delle attività di navigazione e di uso della mail aziendale può venir tenuta traccia indirettamente (log di sistema delle apparecchiature). Tali informazioni sono necessarie per verificare la sicurezza e funzionalità dei sistemi anche ai sensi e per il GDPR.

In caso si verificassero abusi saranno presi i necessari provvedimenti.

Se durante i controlli, che avverranno saltuariamente e a campione per evitare illeciti, abusi o semplicemente per verificare la funzionalità e sicurezza dei sistemi informatici, si viene a conoscenza di dati personali sensibili, chi effettua i controlli informerà chi ha il potere di informare il dipendente.

Premesso che al dipendente è vietato navigare in siti che possano rivelare dati sensibili, i dati che ogni sistema informatico può tenere traccia potranno essere contestati al dipendente e potranno essere tenuti e usati nelle sedi giudiziarie.

19 SOGGETTI PREPOSTI

Ai Responsabili del trattamento, agli Amministratori di Sistema e agli addetti alla manutenzione sono state impartite precise istruzioni sulle tipologie di controlli ammessi e sulle relative modalità.

Nel caso di eventuali interventi per esigenze di manutenzione del sistema, sarà posta opportuna cura nella prevenzione di accessi illegittimi a dati personali presenti in cartelle o spazi di memoria.

I soggetti preposti al trattamento dei dati (in particolare, gli incaricati della manutenzione) svolgeranno solo operazioni strettamente necessarie al perseguimento delle relative finalità, senza realizzare attività di controllo a distanza, anche di propria iniziativa.

I dipendenti potranno conoscere gli estremi identificativi delle figure preposte che sono riportati nell'organigramma aziendale.

I soggetti che operano quali amministratori di sistema o figure analoghe, cui siano rimesse operazioni connesse al regolare funzionamento dei sistemi, sono edotti e consapevoli delle linee di condotta da tenere, attraverso un'adeguata attività formativa sui profili tecnico-gestionali e di sicurezza delle reti, sui principi di protezione dei dati personali e sul segreto nelle comunicazioni.

20 ACCESSO AI DATI TRATTATI DALL'UTENTE

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

21 ENTRATA IN VIGORE DEL REGOLAMENTO

Con l'entrata in vigore del presente regolamento tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi abrogate e sostituite dalle presenti.

Copia del regolamento, oltre ad essere affisso nella bacheca aziendale, potrà essere consegnato ai dipendenti. Si evidenzia che la consegna di una copia a ciascun collaboratore è una scelta facoltativa del Centro Servizi. Si ricorda, infatti, che, ai sensi dell'art. 7 Legge n. 300/1970, l'unico obbligo a carico dell'Ente, ai fini dell'esercizio del potere disciplinare, è quello di dare adeguata pubblicità delle norme mediante l'affissione in luogo accessibile a tutti: per agire disciplinarmente nei confronti del dipendente, il presente regolamento potrà pertanto essere solo affisso in luogo accessibile a tutti. Questo esplicita chiaramente l'obbligo di tutti gli utenti di adeguarsi alle norme in esso contenute, anche nell'eventualità di non aver ricevuto formalmente il documento. L'accettazione e l'obbligo di adeguamento al presente

regolamento sono disgiunti dalla presenza della firma del dipendente in calce.

È fatto obbligo a tutti gli utenti di osservare le disposizioni portate a conoscenza con il presente regolamento. Il mancato rispetto o la violazione delle regole sopra ricordate è perseguibile nei confronti del personale dipendente con provvedimenti disciplinari e risarcitori previsti dal vigente CCNL, e con tutte le azioni civili e penali consentite.

Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni motivate al presente Regolamento.

Merlara, il __ / __ / _____

Per presa visione, ricevuta ed accettazione

_____
(Cognome e Nome del dipendente)