TERME MARINE E SPIAGGIA GRADO

Regolamento

per il corretto utilizzo

degli strumenti informatici e telematici

Adottato dalla S.p.A. GIT Gestione Impianti Turistici – Grado (GO)

Data di prima emissione**:** 01.11.2010

Data prima revisione:

Data seconda revisione:

Scopo

Premesso che l'utilizzo delle risorse informatiche e telematiche deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito di un rapporto di lavoro, la S.p.a. G.I.T. Gestione Impianti Turistici di Grado (di seguito la Società) ha adottato un Regolamento interno diretto ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla Sicurezza nel trattamento dei dati.

Tali prescrizioni si aggiungono ed integrano le specifiche istruzioni già fornite a tutti gli incaricati, in attuazione della normativa vigente e di quanto sancito in materia di responsabilità amministrativa delle persone giuridiche (D. Lgs. 231/01).(Vgs Codice Etico – Linee di Condotta)

Campo di applicazione

Il presente regolamento deve essere conosciuto ed applicato da tutte le unità organizzative che fanno parte della Società. Particolare attenzione dovrà essere posta da tutti i soggetti che trattano dati personali, sensibili e/o giudiziari.

Riferimenti normativi e fonti

Codice in materia di Protezione dei Dati Personali (D.Lgs. n.196 del 30 giugno 2003)
Disciplinare tecnico in materia di Misure Minime di Sicurezza (Art. da 33 a 36 del Codice)
D. Lgs. 231/01
DPR 513/97
T.U. 15/12/2000
Fonti da cui consultare la normativa:
· Sito Internet del Garante per la protezione dei dati personali:
www.garanteprivacy.it

Articoli tratti dal Codice Civile

- **Art. 2104 Diligenza del prestatore di lavoro**
  Il prestatore di lavoro deve usare la diligenza richiesta dalla natura della prestazione dovuta, dall'interesse dell'impresa e da quello superiore della produzione nazionale. Deve inoltre osservare le disposizioni per l'esecuzione e per la disciplina del lavoro impartite dall'imprenditore e dai collaboratori di questo dai quali gerarchicamente dipende.

- **Art. 2105 Obbligo di fedeltà**
  Il prestatore di lavoro non deve trattare affari, per conto proprio o di terzi, in concorrenza con l'imprenditore, né divulgare notizie attinenti all'organizzazione e ai metodi di produzione dell'impresa, o farne uso in modo da poter recare ad essa pregiudizio.

- **Art. 2106 c.c. - Sanzioni disciplinari**

  L'inosservanza delle disposizioni contenute nei due articoli precedenti può dar luogo all'applicazione di sanzioni disciplinari, secondo la gravità dell'infrazione.

Articoli tratti dal C.C.N.L.

- **Art. 35 - Doveri del Lavoratore**

Al lavoratore incombe l'obbligo di:

- eseguire con la massima diligenza il compito a lui affidato, assumendosene la personale responsabilità ed attenendosi alle direttive della Società fissate con ordini di servizio o con particolari disposizioni;
- osservare l'orario di lavoro ottemperando alle norme di controllo stabilite per ciascun Servizio od Ufficio (registro, fogli di presenza, orologi, registratori, etc.);
- non abbandonare, al termine del turno, il posto di lavoro senza prima aver avuto la sostituzione prevista;
- comportarsi in modo corretto ed educato nei confronti dei superiori, colleghi, dipendenti e pubblico;
- serbare il segreto su tutto ciò che concerne gli affari e le operazioni della Società;
- avere la massima cura di tutti gli apparecchi, oggetti, locali, dotazioni personali di proprietà della Società, rispondendo pecuniariamente, salvo le maggiori responsabilità, dei danni arrecati per accertata sua colpa, mediante trattenute sullo stipendio, previa comunicazione del relativo addebito;
- uniformarsi all'ordinamento gerarchico della Società nei rapporti attinenti al servizio;
- osservare scrupolosamente tutte le norme di legge sulla prevenzione infortuni che la Società porta a sua conoscenza nonché tutte le particolari disposizioni a riguardo emanate dalla Società stessa;
- osservare scrupolosamente le norme che vietano il contrabbando e il favoreggiamento di clandestini;
- comunicare tempestivamente qualsiasi variazione intervenuta rispetto a quanto reso noto – a norma dell'art. 7 - al momento dell'assunzione o successivamente.

Articoli tratti dalla Legge 20 maggio 1970, n. 300 - Statuto dei Lavoratori

- **Art. 4. Impianti audiovisivi.**

1. È vietato l'uso di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori.

2. Gli impianti e le apparecchiature di controllo che siano richiesti da esigenze organizzative e produttive ovvero dalla sicurezza del lavoro, ma dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori, possono essere installati soltanto previo accordo con le rappresentanze sindacali aziendali, oppure, in mancanza di queste, con la commissione interna. In difetto di accordo, su istanza del datore di lavoro, provvede l'Ispettorato del lavoro, dettando, ove occorra, le modalità per l'uso di tali impianti.

3. Per gli impianti e le apparecchiature esistenti, che rispondano alle caratteristiche di cui al secondo comma del presente articolo, in mancanza di accordo con le rappresentanze sindacali aziendali o con la commissione interna, l'Ispettorato del lavoro provvede entro un anno dall'entrata in vigore della presente legge, dettando all'occorrenza le prescrizioni per l'adeguamento e le modalità di uso degli impianti suddetti.

4. Contro i provvedimenti dell'Ispettorato del lavoro, di cui ai precedenti secondo e terzo comma, il datore di lavoro, le rappresentanze sindacali aziendali o, in mancanza di queste, la commissione interna, oppure i sindacati dei lavoratori di cui al successivo art. 19 possono ricorrere, entro 30 giorni dalla comunicazione del provvedimento, al Ministro per il lavoro e la previdenza sociale.

- **Art. 7. Sanzioni disciplinari.**

1. Le norme disciplinari relative alle sanzioni, alle infrazioni in relazione alle quali ciascuna di esse può essere applicata ed alle procedure di contestazione delle stesse, devono essere portate a conoscenza dei lavoratori mediante affissione in luogo accessibile a tutti. Esse devono applicare quanto in materia è stabilito da accordi e contratti di lavoro ove esistano.
2. Il datore di lavoro non può adottare alcun provvedimento disciplinare nei confronti del lavoratore senza avergli preventivamente contestato l'addebito e senza averlo sentito a sua difesa.
3. Il lavoratore potrà farsi assistere da un rappresentante dell'associazione sindacale cui aderisce o conferisce mandato.
4. Fermo restando quanto disposto dalla legge 15 luglio 1966, n. 604, non possono essere disposte sanzioni disciplinari che comportino mutamenti definitivi del rapporto di lavoro; inoltre la multa non può essere disposta per un importo superiore a quattro ore della retribuzione base e la sospensione dal servizio e dalla retribuzione per più di dieci giorni.
5. In ogni caso, i provvedimenti disciplinari più gravi del rimprovero verbale non possono essere applicati prima che siano trascorsi cinque giorni dalla contestazione per iscritto del fatto che vi ha dato causa.
6. Salvo analoghe procedure previste dai contratti collettivi di lavoro e ferma restando la facoltà di adire l'autorità giudiziaria, il lavoratore al quale sia stata applicata una sanzione disciplinare può promuovere, nei venti giorni successivi, anche per mezzo dell'associazione alla quale sia iscritto ovvero conferisca mandato, la costituzione, tramite l'ufficio provinciale del lavoro e della massima occupazione, di un collegio di conciliazione ed arbitrato, composto da un rappresentante di ciascuna delle parti e da un terzo membro scelto di comune accordo o, in difetto di accordo, nominato dal direttore dell'ufficio del lavoro. La sanzione disciplinare resta sospesa fino alla pronuncia da parte del collegio.

1. Definizioni - previste dall'art. 4, commi 1, 2 e 3 del D.Lgs. 196/03

Trattamento
Qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati.

Dato personale
Qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.

Dati identificativi
Dati personali che permettono l'identificazione diretta dell'interessato.

Dati sensibili
I dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.

Dati giudiziari
I dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale.

Titolare
La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.

Responsabile
La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali.

Incaricato
Le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile.

Interessato
La persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali.

Comunicazione
Il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

Diffusione
Il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

Dato anonimo
Il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile.

Blocco
La conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento.

Banca di dati
Qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti.

Garante
L'autorità di cui all'art. 153, istituita dalla legge 31 dicembre 1996, n. 675.

Comunicazione elettronica
Ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico.
Sono escluse le informazioni trasmesse al pubblico tramite una rete di comunicazione elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad un abbonato o utente ricevente, identificato o identificabile.

Chiamata
La connessione istituita da un servizio telefonico accessibile al pubblico, che consente la comunicazione bidirezionale in tempo reale.

Reti di comunicazione elettronica
I sistemi di trasmissione, le apparecchiature di commutazione o di instradamento e altre risorse che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, incluse le reti satellitari, le reti terrestri mobili e fisse a commutazione di circuito e a commutazione di pacchetto, compresa Internet, le reti utilizzate per la diffusione circolare dei programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica, nella misura in cui sono utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato.

Rete pubblica di comunicazioni
Rete di comunicazioni elettroniche utilizzata interamente o prevalentemente per fornire servizi di comunicazione elettronica accessibili al pubblico.

Servizio di comunicazione elettronica
Servizi consistenti esclusivamente o prevalentemente nella trasmissione di segnali su reti di comunicazioni elettroniche, compresi i servizi di telecomunicazioni e i servizi di trasmissione nelle reti utilizzate per la diffusione circolare radiotelevisiva, nei limiti previsti dall'articolo 2, lettera c), della direttiva 2002/21/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002.

Utente
Qualsiasi persona fisica che utilizza un servizio di comunicazione elettronica accessibile al pubblico, per motivi privati o commerciali, senza esservi necessariamente abbonata.

Dati relativi al traffico
Qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione.

Dati relativi all'ubicazione
Ogni dato trattato in una rete di comunicazione elettronica che indica la posizione geografica dell'apparecchiatura terminale dell'utente di un servizio di comunicazione elettronica accessibile al pubblico.

Servizio a valore aggiunto
Il servizio che richiede il trattamento dei dati relativi al traffico o dei dati relativi all'ubicazione diversi dai dati relativi al traffico, oltre a quanto è necessario per la trasmissione di una comunicazione o della relativa fatturazione.

Posta elettronica
Messaggi contenenti testi, voci, suoni o immagini trasmessi attraverso una rete pubblica di comunicazione, che possono essere archiviati in rete o nell'apparecchiatura terminale ricevente, fino a che il ricevente non ne ha preso conoscenza.

Misure minime
Il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31.

Strumenti elettronici
Gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento.

Autenticazione informatica
L'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità.

Credenziali di autenticazione
I dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l' autenticazione informatica.

Password
Letteralmente: Parola d'ordine
In ambito informatico e crittografico una password (in italiano: "parola chiave", "parola d'ordine", o anche "parola d'accesso") è una sequenza di caratteri alfanumerici utilizzata per accedere in modo esclusivo ad una risorsa informatica.
Una password è solitamente associata ad uno specifico username (in italiano nome utente o identificatore utente) al fine di ottenere un'identificazione univoca da parte del sistema a cui si richiede l'accesso.

Profilo di autorizzazione
L'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti.

Sistema di autorizzazione
L'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.

Documento informatico

Per documento informatico si intende la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.
Il richiamo alla rappresentazione informatica di atti, dati e fatti implica che il documento informatico può essere costituito anche da un filmato e da ogni altra informazione digitalizzata.
Il principio proposto dal CNIPA circa la validità del documento informatico è stato così espresso: "Gli atti, dati e documenti formati dalla pubblica amministrazione e dai privati con strumenti informatici o telematici, i contratti stipulati nelle medesime forme, nonché la loro archiviazione e trasmissione con strumenti informatici sono validi e rilevanti a tutti gli effetti di legge".
Tale principio è stato accolto dal DPR 513/97, che recita: "Il documento informatico da chiunque formato, l'archiviazione su supporto informatico e la trasmissione con strumenti telematici, sono validi e rilevanti a tutti gli effetti di legge se conformi alle disposizioni del presente regolamento".
Il principio è inoltre ripreso dal Testo Unico del 15 Dicembre 2000.

Nello specifico:

Articolo 8
Il documento informatico da chiunque formato, la registrazione su supporto informatico e la trasmissione con strumenti telematici, sono validi e rilevanti a tutti gli effetti di legge, se conformi alle disposizioni del presente testo unico.
A tale riguardo, si rende noto che l'art. 491-bis del c.p. punisce le falsità previste dal capo III del codice penale riguardanti un documento informatico pubblico o privato, avente efficacia probatoria.

Articolo 10
Forma ed efficacia del documento informatico

1. Il documento informatico sottoscritto con firma digitale, redatto in conformità alle regole tecniche di cui all'articolo 8, comma 2 e per le pubbliche amministrazioni, anche di quelle di cui all'articolo 9, comma 4, soddisfa il requisito legale della forma scritta e ha efficacia probatoria ai sensi dell'articolo 2712 del Codice civile.

2. Gli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto sono assolti secondo le modalità definite con decreto del Ministro delle finanze.
3. Il documento informatico, sottoscritto con firma digitale ai sensi dell'articolo 23, ha efficacia di scrittura privata ai sensi dell'articolo 2702 del codice civile.
4. Il documento informatico redatto in conformità alle regole tecniche di cui all'articolo 8, comma 2 soddisfa l'obbligo previsto dagli articoli 2214 e seguenti del codice civile e da ogni altra analoga disposizione legislativa o regolamentare.

2. Utilizzo del Personal Computer

Il Personal Computer affidato al dipendente è uno strumento di lavoro. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza, nonché violare quanto prescritto dall'art. 617-quinquies c.p. e dal D. Lgs. 231/01.
L'accesso all'elaboratore è protetto dalle credenziali di accesso (composte da Identificativo Utente e **Password** di almeno otto caratteri) che devono essere custodite dall'incaricato con la massima diligenza e non divulgate. Ogni elaboratore ha una password che controlla l'autorizzazione ad accenderlo, la cosiddetta Password di avvio. Successivamente, mediante l'inserimento delle credenziali di accesso (Identificativo Utente e Parola Chiave), viene autorizzato il collegamento alla rete telematica aziendale e l'accesso al computer locale. Possono essere utilizzate password diverse per l'accesso al computer, alla rete ed alle applicazioni con particolari esigenze di sicurezza, nonché per lo screen saver (salva schermo).

Per ogni incaricato viene creata una "credenziale di autenticazione" che consente l'accesso all'elaboratore ed alla rete telematica aziendale, attraverso una procedura di autenticazione (login). A tal fine, ad ogni incaricato è stata assegnata in via riservata una credenziale per l'autenticazione che consiste in un codice identificativo (user ID) ed una parola chiave riservata di almeno 8 caratteri (password). E' vietato l'accesso contemporaneo con le stesse credenziali da più elaboratori.

In caso di assenza, anche momentanea, dalla propria postazione di lavoro, devono essere adottate misure atte a escludere che soggetti non autorizzati possano acquisire informazioni o accedere ai dati trattati con strumenti elettronici. A tal proposito, a titolo meramente esemplificativo, si consiglia di adottare un sistema di oscuramento (screen-saver) dotato di password, ovvero di uscire dal programma che si sta utilizzando, ove sia protetto da parola chiave. In alternativa l'utente può spegnere l'elaboratore che sta utilizzando.

Tutti gli strumenti informatici e telematici messi a disposizione (computer desktop e portatili, apparati connessi ad Internet, sistemi per comunicazioni e-mail, sms, blackberry, etc.) costituiscono degli strumenti di lavoro da utilizzare esclusivamente per l'esecuzione delle mansioni affidate. Non è quindi consentita la memorizzazione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.

Per assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza od impedimento che renda indispensabile ed indifferibile intervenire per necessità operative o di sicurezza, si potrà rimuovere la password di accesso ai sistemi locali o di rete in conformità a quanto previsto dal Disciplinare tecnico in materia di misure di sicurezza - Allegato B) del D.Lgs. 196/03.

In tal caso, il soggetto verrà informato di eventuali interventi effettuati in Sua assenza.
La password di accesso alle applicazioni / banche dati aziendali non deve contenere riferimenti agevolmente riconducibile all'incaricato; deve contenere, preferibilmente, caratteri speciali e lettere maiuscole e minuscole, in modo da rendere più complesso qualunque tentativo di forzatura o di violazione della stessa. La password non deve essere in ogni caso divulgata o comunicata a terzi, deve essere conservata in luogo segreto e non deve essere trascritta in foglietti visibili da altri soggetti.

I supporti rimovibili (cd-rom, dvd-rom, chiavette USB, ecc.) devono essere custoditi in modo da evitare l'utilizzo da parte di soggetti non autorizzati. Si consiglia, in particolare, di riporli in un contenitore munito di serratura: i supporti non più utilizzabili possono essere eliminati solo dopo che i dati contenuti sono stati resi effettivamente inutilizzabili.

Per poter riutilizzare i supporti di memorizzazione di dati, si deve procedere alla cancellazione dei dati precedentemente registrati, in modo da evitare che soggetti terzi possano conoscere o comunque risalire alle informazioni memorizzate in precedenza.

L'utente è responsabile della dotazione informatica assegnatagli e deve custodirla con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

Non è permesso installare autonomamente programmi e modificare le caratteristiche hardware e software sul PC assegnato. Sussiste il grave pericolo di portare virus informatici e le altre minacce alla sicurezza delle informazioni che sono classificate con il termine generico di malware (malicious software). Inoltre sussiste la concreta possibilità di alterare la funzionalità delle applicazioni dell'elaboratore e di introdurre vulnerabilità nella sicurezza del sistema.

Non è consentito l'uso di programmi diversi da quelli forniti ufficialmente dai Sistemi Informativi.
Ai sistemi portatili si applicano le regole di utilizzo previste per i PC Desktop connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna: questi non devono essere lasciati incustoditi, specialmente in occasione di utilizzo esterno all'azienda (convegni, riunioni, telelavoro, ecc.).

Nell'utilizzare il Fax occorre prestare attenzione, in particolar modo, nel caso in cui vengano inviati documenti contenenti dati sensibili: digitare correttamente il numero di telefono, controllare l'esattezza del numero digitato prima di premere il tasto invio, verificare che non vi siano inceppamenti della carta ovvero che non vengano presi più fogli, attendere la stampa del rapporto di trasmissione, verificando la corrispondenza del numero di pagine da inviare con quelle effettivamente inviate. Qualora vengano trasmessi dati idonei a rivelare lo stato di salute, è opportuno anticipare l'invio chiamando il destinatario della comunicazione al fine di assicurare il ricevimento nelle mani del medesimo, evitando che terzi estranei o non autorizzati conoscano il contenuto della documentazione inviata.

Nell'utilizzare il Fax in ricezione e/o stampanti poste al di fuori della propria postazione lavorativa – stampanti multifunzionali e/o dipartimentali – è opportuno assicurare una tempestiva acquisizione dei documenti al fine di evitare l'accesso di persone non autorizzate.

Non è consentita l'installazione sul proprio PC di nessun dispositivo di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, chiavi USB, ecc.).

Agli utenti incaricati del trattamento dei dati sensibili, personali e/o giudiziari è fatto divieto l'accesso contemporaneo con le stesse credenziali di accesso da più elaboratori.

Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente l'Amministratore del Sistema nel caso in cui siano rilevati virus ed adottando quanto previsto dal successivo punto 8 del presente Regolamento.

Non è consentita la memorizzazione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.

3. Utilizzo del protocollo informatico, dei documenti e dell'archivio telematico

Il legislatore definisce sistema di gestione informatica dei documenti l'insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure informatiche utilizzati dalle amministrazioni per la gestione dei documenti; il protocollo informatico si colloca all'interno del sistema come infrastruttura di base destinata ad avviare concretamente il processo di ammodernamento della pubblica amministrazione. Ogni sistema di protocollo informatico deve ottemperare alle specifiche indicazioni riportate nel DPR 445-28/12/2000 e nel regolamento attuativo DPCM 31/10/2000.

L'attuale quadro normativo e regolamentare in materia di gestione informatica del protocollo, dei documenti e degli archivi, comprende anche i documenti residenti presso le unità di rete condivise.
L'archivio telematico di rete deve contenere esclusivamente informazioni strettamente professionali, che vanno regolarmente esaminate per non creare inutili duplicazioni.

Su queste unità, vengono svolte regolari attività di controllo, amministrazione e backup da parte dell'Amministratore del Sistema.
Le credenziali di accesso ai sistemi di Rete ed alle applicazioni sono riservate e individuali.

E' proibito entrare nella Rete e nei programmi impersonando altri utenti, anche con il loro esplicito consenso.

L'Amministratore del Sistema può, in qualunque momento, procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la Sicurezza delle Informazioni sia sui PC degli incaricati sia sulle unità di rete. Tali operazioni verranno notificate per conoscenza al Direttore Area Operativa.

Costituisce buona regola la periodica (almeno ogni sei mesi) pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. E', infatti, da evitare un'archiviazione ridondante.

E' cura dell'utente effettuare la stampa dei dati solo se strettamente necessaria e di ritirarla prontamente dai vassoi delle Stampanti di Rete. E' buona regola evitare di stampare su tali dispositivi documenti a carattere riservato, contenenti dati sensibili o dati giudiziari.

4. Gestione delle password (Parole Chiave)

Le password di accesso ai sistemi informatici sono configurate dagli utenti. E' consentita l'autonoma sostituzione delle password da parte degli utenti ogni volta che lo riterranno necessario. In nessun caso l'Amministratore del Sistema o qualsiasi responsabile di Entità o Area deve conoscere le credenziali di accesso degli utenti: l'Amministratore del Sistema, se richiesto con nota interna da parte del Direttore Area Operativa, può rimuovere qualsiasi password per esigenze operative.

Le password di accensione del computer devono avere una lunghezza non inferiore a sette caratteri. Le password per l'ingresso ai servizi di rete e per l'accesso ai programmi, alle banche dati, agli archivi che contengono dati personali e/o sensibili devono avere una lunghezza non inferiore ad otto caratteri. Evitare di scegliere password banali e facilmente indovinabili: l'ideale sarebbe una combinazione di caratteri composta da lettere, numeri e simboli scelti in maniera casuale.
Le password utilizzate dagli utenti hanno una durata massima di tre mesi, trascorsi i quali le password devono essere sostituite.

La password deve essere immediatamente sostituita, dandone informazione all'amministratore del Sistema, nel caso si sospetti che la stessa abbia perso la segretezza.

Il possesso e la detenzione abusiva e la diffusione dei codici di accesso è delegata alla responsabilità dell'utilizzatore di tali codici o password è esplicitamente vietato ed illegale esercitare qualunque attività di utilizzo di tecniche di appropriazione indebita di password tramite mezzi o comportamenti (615-quater c.p.).

I momenti successivi a queste attività, riproduzione, diffusione, comunicazione e consegna dei codici, sono sanzionati esplicitamente dal D. Lgs. 231/01.

5. Utilizzo dei supporti magnetici ed ottici

Tutti i supporti magnetici ed ottici riutilizzabili (dischetti, cassette a nastro, cd-rom riscrivibili, chiavi USB, ecc.) contenenti dati sensibili devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato. Una persona esperta potrebbe infatti recuperare i dati memorizzati anche dopo la loro cancellazione.

I supporti magnetici ed ottici riutilizzabili (dischetti, nastri magnetici, CD-ROM o DVD riscrivibili, memorie PenDrive USB, ecc.) contenenti dati sensibili o giudiziari **di cui si sia cessato l'utilizzo**, devono essere gestiti in modo da evitare che il loro contenuto possa essere successivamente recuperato da terzi.

Non è consentito scaricare file contenuti in supporti magnetici ed ottici non aventi alcuna attinenza con la propria prestazione lavorativa.

6. Utilizzo di PC portatili e sistemi smartphone

L'utente è responsabile del PC portatile assegnatogli dall'Amministratore del Sistema e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

Ai PC portatili si applicano le regole di utilizzo previste per i PC connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna.

I PC portatili non devono essere lasciati incustoditi, specialmente in occasione di utilizzo esterno all'azienda (convegni, riunioni, telelavoro ecc.).

E' cura del referente del PC portatile, ogni qualvolta il sistema è utilizzato fuori del contesto aziendale, aggiornare le impronte virali e consegnarlo periodicamente all'Entità Sistemi Informativi per l'aggiornamento. Tuttavia non è consentito installare apparati per l'accesso alla rete Internet senza il consenso della struttura dell'Entità Sistemi Informativi.

E' assolutamente vietato configurare sistemi "smartphone" per la lettura dell'account di posta elettronica aziendale (casella postale, rubrica, calendario), come l'accesso alle applicazioni e alle informazioni presenti sui vari volumi di rete, senza il consenso del supporto tecnico dell'Entità Sistemi Informativi. Questa tecnologia ha visto il suo diffondersi in virtù delle nuove necessità di comunicazione sorte in azienda, ed al grado di risposta da parte del mercato nel fornire strumenti sempre più perfezionati per favorire la comunicazione Internet da cellulare.

7. Uso della Posta Elettronica

La casella di posta, assegnata dall'Azienda all'utente, è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

E' fatto divieto di utilizzare le caselle di posta elettronica aziendale per l'invio di messaggi personali.

E' buona norma evitare messaggi completamente estranei al rapporto di lavoro o alle relazioni tra colleghi. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.

La posta elettronica diretta in **uscita** dalla rete informatica aziendale viene inoltrata a destinazione attraverso i servizi di posta di Internet. Essa non ha più le caratteristiche di sicurezza di un messaggio di posta interna all'azienda e, quindi, può essere intercettata e letta da estranei.

Per la trasmissione di file all'interno dell' azienda è possibile utilizzare la posta elettronica, prestando attenzione alla dimensione degli allegati. Per file di dimensioni rilevanti si utilizzano le cartelle condivise di rete predisposte dall' Amministratore di Sistema, mentre per le comunicazioni con allegati di grosse dimensioni da e verso Internet, è necessario utilizzare l'apposito sito FTP. Per l'utilizzo dei servizi FTP è tuttavia necessario concordare, tramite Nota Interna, con la struttura Sistemi Informativi le modalità e le tempistiche per l'attuazione della procedura stessa.

Qualsiasi file allegato alla posta elettronica può essere potenzialmente pericoloso.

Esistono i mezzi tecnologici per camuffare un file allegato in modo da farlo sembrare del tutto innocuo. Inoltre, diverse minacce si propagano anche utilizzando come file allegati degli archivi compressi in formato ZIP o RAR. Tali archivi contengono il virus e sono protetti da password.

Il testo del messaggio e' volutamente fuorviante. Chi ha creato il virus vuole convincere l'utente ad aprire l'archivio digitando la password indicata nel testo del messaggio e, quindi, ad eseguire il virus. I programmi Antivirus non sono in grado di aprire e controllare archivi protetti da password, di conseguenza, questo tipo di attacco potrebbe penetrare le difese predisposte dall'Entità Sistemi Informativi.

La posta elettronica può essere falsificata in ogni sua parte.

Ad esempio: gli ultimi Worm che si sono propagati via Internet falsificano mittente, oggetto e corpo del testo in modo da indurre l' utente ad eseguire il file allegato.

Un messaggio di posta elettronica potrebbe provenire da un mittente diverso da quello indicato nel campo mittente e contenere allegati potenzialmente pericolosi per la Sicurezza delle Informazioni.

La posta elettronica che arriva da mittente sconosciuto va comunque considerata con legittimo sospetto. Esiste una finestra temporale più o meno ampia tra l' inizio della propagazione iniziale di una minaccia alla Sicurezza delle Informazioni (Virus, Worm, Security Exploit, ecc.) e la sua rilevazione da parte degli esperti del settore. Tra l' analisi del problema e la diffusione delle contromisure e rimedi passa altro tempo. In tale periodo la minaccia si propaga indisturbata su numerosi computer che a loro volta diffondono il contagio. Ne consegue che, in qualsiasi momento, ci potrebbero essere dei messaggi di posta elettronica pericolosi non ancora riconosciuti come tali. In tali circostanze è d'obbligo raccomandare sempre la massima cautela nella gestione degli allegati di posta elettronica.

Gli autori delle frodi, di fatto, inviano tali messaggi nel tentativo di persuadere il maggior numero di persone a divulgare informazioni riservate: il messaggio di posta elettronica può sembrare attendibile, ma un'eventuale risposta potrebbe esporre a rischio il sistema informativo aziendale.

Non è possibile utilizzare propri account di servizi web mail.

8. Uso della rete Internet e dei relativi servizi

Il PC abilitato alla navigazione in Internet costituisce uno strumento aziendale necessario allo svolgimento della propria attività lavorativa. E' assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa stessa.

E' fatto divieto all'utente lo scarico di programmi (download di software) da siti Internet. Si vedano anche i punti 2.4 e 2.5 del presente regolamento.

E’ da evitare ogni forma di registrazione a siti i cui contenuti non siano legati all’attività lavorativa.
Non sono consentiti: l'utilizzo di servizi di Internet Relay Chat (IRC), l'utilizzo di bacheche elettroniche (Newsgroup) che non abbiano attinenza con l'attività lavorativa.

Per le postazioni tecnologiche attestate su reti dati dedicate (progetti ad hoc - fuori dal contesto della rete aziendale), valgono le stesse regole di fruibilità del servizio tradizionale: rimane responsabilità del fruitore del sistema verificare costantemente l’aggiornamento delle impronte virali ed effettuare connessioni per scopi attinenti alle attività lavorative.

9. Uso dei Sistemi Informativi e dei Sistemi Telematici

Definendo in precedenza "sistema informatico" un'apparecchiatura più o meno complessa destinata a svolgere qualsiasi funzione utile all’uomo attraverso l’utilizzazione, anche solo parziale, di tecnologie informatiche, si intende per "sistema telematico" l'interazione a distanza delle informazioni e delle elaborazioni proprie di un "sistema informatico".

Identificando l'accesso con il momento in cui l'utente si trova nella condizione, avendo superato qualsiasi barriera prevista dai sistemi, di conoscere direttamente dati, informazioni o programmi in esso contenuti, si ammonisce l’utente a osservare quanto previsto nel D.lgs. 231/01, in particolare, per quanto concerne l’accesso abusivo ad un sistema informatico o telematico nonché alla diffusione delle informazioni derivanti a seguito di tale accesso.

Si ammonisce, altresì, l'utente a non intercettare interrompere o impedire le comunicazioni informatiche e/o telematiche (art. 617 - quater c.p.), tantomeno a danneggiare informazioni, dati o programmi informatici nonché i Sistemi Informativi o Telematici aziendali e/o di pubblica utilità, come previsto dagli artt. 615 - quinquies; 635 bis - 635 ter - 635 quater; 635 quinquies del c.p.

10. Protezione antivirus

Ogni utente deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale mediante virus o per mezzo di ogni altro software aggressivo.

Ogni utente è tenuto a controllare il regolare funzionamento ed a segnalare all' Amministratore di Sistema le eventuali anomalie riscontrate.
Nel caso che il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente:
a) sospendere ogni elaborazione in corso;
b) spegnere il computer per limitare la propagazione del virus sulla rete telematica aziendale;
c) segnalare l'accaduto all'Amministratore di Sistema ed attendere istruzioni.

11. Osservanza delle disposizioni in materia di Privacy

E' obbligatorio attenersi alle disposizioni in materia di Privacy e di misure minime di sicurezza, come indicate nella lettera di individuazione di incaricato del trattamento dei dati, ai sensi del già citato Codice in materia di Protezione dei Dati Personali (D.Lgs. n.196 del 30 giugno 2003) e del Disciplinare tecnico in materia di Misure Minime di Sicurezza

12. Non osservanza della normativa aziendale

II mancato rispetto o la violazione delle regole contenute nel presente Regolamento è perseguibile con provvedimenti disciplinari nonché con le azioni civili e penali consentite.

13. Aggiornamento e revisione

Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni al presente Regolamento. Le proposte verranno esaminate dal Responsabile Entità Sistemi Informativi di concerto con il Direttore Area Operativa.

Il presente Regolamento è soggetto a revisione periodica; nel caso di rilevanti mutamenti nel quadro normativo o nel contesto tecnologico in cui si opera il presente documento sarà adeguato con la massima sollecitudine.