REGOLAMENTO RELATIVO ALL'UTILIZZO DEGLI STRUMENTI INFORMATICI COMUNALI.

Premessa

Negli ultimi anni l'utilizzo di risorse informatiche (computer, periferiche, software, internet, interconnessione con altri soggetti) da parte del comune è notevolmente aumentato in quantità e complessità. Tutto ciò ha avuto importanti ricadute in termini di sicurezza, ed è necessario quindi stabilire una serie di regole di comportamento che, nel rispetto della normativa vigente in tema di trattamenti di dati personali e relative misure minime di sicurezza, garantiscano:

- l'efficienza ed il corretto utilizzo delle risorse informatiche;
- la riservatezza delle informazioni e dei dati;
- il rispetto delle leggi in materia di risorse in informatiche;

Le seguenti regole devono essere seguite da tutti gli utenti della rete aziendale e cioè: dipendenti che utilizzano il pc, amministratori, stagisti, tirocinanti, collaboratori, volontari del servizio civile ecc.; per quanto non qui previsto è comunque richiesto un atteggiamento ispirato alla correttezza ed alla buona fede.

Art.1) Strumenti forniti

Gli uffici del comune di San Fior sono dotati di :

1. Personal computer collegati in rete locale abilitati alla navigazione in internet (con l'eccezione di quelli adibiti a esclusive funzioni di sportello), dotati di software di base, d'ufficio e gestionale e di una serie di periferiche (stampanti, scanner, ecc.)
2. Una mail istituzionale assegnata ad ogni ufficio

L'ufficio protocollo inoltre gestisce in maniera centralizzata la mail di posta certificata comune.sanfior.tv@pecveneto.it .

Art. 2) Misure di sicurezza relative alla rete locale

Ad ogni utente sono assegnate delle credenziali personali di accesso al computer ed al dominio di rete formate da un nome utente e da una password: il nome utente è formato dalla prima lettera del nome seguita dal cognome; la password è liberamente scelta da ogni utente che può cambiarla autonomamente in qualsiasi momento. La password soggiace ai criteri di complessità previsti dalla normativa vigente (numero di caratteri, scadenza, ecc.), e deve essere mantenuta riservata: non ci sono ragioni tecniche che giustifichino la condivisione delle proprie credenziali di accesso con altri utenti; nel caso di pc adibiti esclusivamente a funzioni di sportello con utilizzo intermittente da parte di diversi operatori sono assegnate credenziali di accesso specifiche della postazione e non personali.

Le credenziali di accesso di ciascun dipendente inquadrato in una determinata U.O. permettono:

- l'accesso a tutti i pc di quella Unità Organizzativa, e l'utilizzo di qualsiasi risorsa locale (files sul disco fisso, stampanti, programmi, posta elettronica);
- l'accesso alle risorse di rete assegnate all'ufficio o specifiche di quell'utente (cartella “files” sul server, stampanti di rete ecc.);
- l'accesso ad internet dai pc a ciò abilitati (tutti tranne quelli con esclusive funzioni di sportello);

Le credenziali di accesso di ogni componente della giunta comunale permettono l'accesso al pc installato nell'ufficio del sindaco, o in altra postazione a ciò dedicata.

Le credenziali di accesso degli altri soggetti permettono l'effettuazione delle operazioni individuate come necessarie specificamente in ogni singolo caso, dal responsabile del servizio interessato in collaborazione con il responsabile ced

Il responsabile Ced non può risalire alla password degli utenti ma, se necessario per ragioni di manutenzione, può cambiarla comunicando all'interessato l'avvenuta variazione

Durante le sessioni di lavoro i pc non possono essere lasciati incustoditi ed accessibili a terzi. Pertanto ogni qualvolta l'utente si allontani o si assenti dalla postazione è tenuto a bloccarne l'accesso o chiudere la sessione e disconnettere il proprio utente

Art. 3) Misure di sicurezza relative ad internet

La rete interna comunale è comunicante con internet, ed in generale con le reti informatiche esterne, tramite dispositivi ai quali sono associate politiche di sicurezza.
In particolare viene attuato un filtraggio preventivo rispetto a siti internet o a contenuti ritenuti inequivocabilmente non inerenti l'attività lavorativa quali:

- pornografia;
- gioco d'azzardo;
- giochi on-line;
- violenza, istigazione all'odio, razzismo, armi;
- attivismo politico, religiosità, spiritualità;
- sport, hobbystica;

Qualora, tali sistemi di filtraggio impediscano l'utilizzo di siti o risorse utili all'attività lavorativa, il dipendente interessato deve inviare segnalazione scritta al Ced.

I dati relativi alla navigazione in internet dai pc della rete comunale (nello specifico: Data della connessione – Ora della connessione – Indirizzo di rete del pc comunale – servizio richiesto dal pc comunale [es. web, mail, ftp ecc.] – Indirizzo di rete computer chiamato [server o generalmente host] [es. server web, mail ecc.] – Esito della richiesta [operazione permessa/bloccata] – riferimento alla regola del firewall) sono memorizzati tramite i dispositivi sopra citati e possono essere oggetto di controllo. I contenuti delle pagine visualizzate non sono memorizzati.

Art. 4) Altre misure di sicurezza

Le ulteriori misure di sicurezza fisiche, logiche e organizzative relative alla prevenzione dei rischi di distruzione dei dati, ed al loro corretto trattamento, sono elencate dettagliatamente all'interno del Documento programmatico per la sicurezza annualmente aggiornato ed al quale si rimanda.

Art. 5) Criteri di utilizzo dei sistemi informatici

a) Internet e a posta elettronica:

Le caselle di posta elettronica istituzionale sono riservate all'attività lavorativa e sono assegnate agli uffici, non ai singoli dipendenti utilizzatori:

- è vietato inviare o ricevere comunicazioni personali su tali caselle di posta elettronica;
- non sono rilasciabili caselle di posta elettronica recanti i nomi dei dipendenti ed il dominio del comune @comune.san-fior.tv.it.

Le caselle di posta elettronica assegnate ad un ufficio possono essere utilizzate per l'invio da qualsiasi dipendente inquadrato nell'ufficio stesso utilizzando il proprio pc; la ricezione può, a scelta del responsabile, essere configurata su uno o più computer; nel caso sia centralizzata su un solo computer ogni componente dell'ufficio potrà accedere alla posta in arrivo utilizzando tale pc con le proprie credenziali. La posta elettronica va comunque scaricata ogni giorno per tutti gli indirizzi a cura del dipendente che normalmente utilizza il pc sul quale è impostata la ricezione,

oppure di altro appartenente alla medesima Unità organizzativa..
Tutti gli operatori possono inoltre inviare e ricevere i messaggi tramite il protocollo usando la casella di e-mail certificata.
Per rendere maggiormente evidente anche all'esterno la natura non personale dell'utilizzo delle mail assegnate agli uffici del comune è obbligo inserire alla fine di ogni messaggio mail spedito la seguente dicitura:
“L'indirizzo xxxx@comune.san-fior.tv.it si riferisce ad una casella di posta elettronica istituzionale assegnata all'ufficio xxxx del comune di San Fior; le comunicazioni inviate a tale indirizzo sono conoscibili da tutti gli appartenenti a tale ufficio e, se giuridicamente rilevanti, verranno registrate nel protocollo ufficiale del comune.”

La navigazione in internet a fini personali utilizzando i pc dell'ufficio è vietata.
Per navigazione a fini personali si intende a titolo esemplificativo e non esaustivo:

- l'utilizzo della propria mail tramite sistemi di web-mail o con la configurazione di programmi di posta;
- l'effettuazione di pagamenti ed acquisti on-line, la consultazione di cataloghi di beni o servizi per acquisti privati;
- l'accesso a propri sistemi di home banking, di gestione del patrimonio, di informazione finanziaria;
- l'accesso a corsi di studio on line, o la ricerca e consultazione di materiale di studio per corsi tradizionali frequentati a scopi personali;
- l'accesso a siti di giornali on line, agenzie di stampa, blog e a siti informativi in generale per motivi non attinenti alle mansioni da espletare;

b) Comunicazioni interne

Le comunicazioni interne tra dipendenti ed uffici devono avvenire utilizzando l’apposito modulo all’interno dei programmi Halley

c) Comportamenti generali

E' vietato:
- utilizzare (consultare, modificare, stampare) sul pc dell'ufficio, memorizzare sullo stesso pc o sul server file a scopi personali, quale che sia la fonte (floppy, cd, dvd, supporti usb, internet, ecc.) ed il contenuto (testi, immagini, audio, video, fogli di calcolo, archivi, presentazioni ecc);
- installare sul pc dell'ufficio software di proprietà privata dei dipendenti;
- installare sul pc dell'ufficio software scaricato da internet diverso dalle estensioni del browser necessarie per alcuni siti (es. flash player);

Art. 6) Controlli

a) Controlli Internet:
viene garantito al direttore generale l'accesso ai dati memorizzati dai dispositivi di sicurezza. L'accesso ai dati è graduato in modo da considerarli in prima analisi in forma complessiva ed anonima, cioè non direttamente riconducibili ad un utente. Sulla e-mail assegnata al direttore generale viene recapitata una relazione giornaliera automatica che evidenzia:
- il traffico internet complessivo diviso per fascia oraria con quantificazione degli eventi e della quantità di dati scambiati;
- l'indicazione dei primi dieci (per quantità di dati scambiati) siti visitati dagli utenti nel giorno;
- l'indicazione dei primi dieci pc (per quantità di dati scambiati) che hanno visitato internet nel giorno;
- l'indicazione dei primi dieci pc (per quantità di dati scambiati) che hanno utilizzato la posta elettronica nel giorno;

La rilevazione di anomalie quali ad esempio a titolo meramente esemplificativo:

- l'utilizzo di internet in orario non compatibile con gli orari di servizio;
- la consultazione di siti ritenuti non attinenti con l'attività lavorativa, in relazione al loro contenuto, o perché la modalità o frequenza di consultazione lasci presumere un utilizzo a fini personali;
- l'utilizzo ritenuto eccessivo dei servizi internet e di mail;

può dar luogo:

- ad un richiamo collettivo al rispetto delle regole previste nel presente regolamento;
- in caso di reiterazione dei comportamenti ritenuti scorretti, alla loro precisazione e quantificazione, alla identificazione del soggetto che li compie, ed all'attivazione delle conseguenti sanzioni disciplinari;

I controlli sulla navigazione internet potranno estendersi al massimo ai dati relativi ai 30 giorni precedenti quello dell'effettuazione del controllo.
Per l'effettuazione di tale attività il Direttore generale potrà avvalersi, a richiesta, del responsabile ced e della ditta che ha in gestione tali apparati;

b) Controlli sull'utilizzo delle mail istituzionali

Viene garantita al direttore generale la possibilità di accedere con le proprie credenziali a tutti i pc e di conseguenza la possibilità di accedere alle mail e rilevare eventuali utilizzi impropri. Tale controllo viene svolto alla presenza del dipendente o dei dipendenti utilizzatori del pc senza ulteriori formalità.

c) Controlli sui pc degli utenti:

Viene garantito al direttore generale l'accesso alle cartelle di ogni ufficio memorizzate sul server ed ai dischi fissi dei singoli pc direttamente dalla propria postazione. Qualora risultasse una violazione rispetto a quanto stabilito all'art. 5 lett. B, procederà alla copia del materiale ritenuto non conforme al presente regolamento, all'identificazione del soggetto autore dell'abuso ed all'attivazione delle conseguenti sanzioni disciplinari.

Art. 7) Conservazione ed accesso ai dati

I dati relativi alla navigazione in internet vengono rilevati tramite i dispositivi interposti tra la rete informatica interna e le reti informatiche esterne.
Una loro rappresentazione testuale/grafica sintetica viene inviata giornalmente alla e-mail del direttore generale;i dati integrali in forma testuale sono invece reperibili:

- sul sito internet di controllo dell'apparato limitatamente ai trenta giorni precedenti alla consultazione;
- sul server della ditta che ha in gestione gli apparati di controllo senza limitazioni tecniche di tempo.

I dati relativi alla navigazione in Internet sono conservati per almeno due anni salvo diverso limite imposto da norme di legge, o necessario per l'attuazione di provvedimenti disciplinari. Tali dati sono accessibili al Direttore generale per finalità di controllo ed al responsabile ced per manutenzione degli apparati in uso.