Allegato 2

Norme comportamentali per l'attuazione di uno standard minimo di sicurezza

Trattamenti cartacei e comunicazioni

1. Non comunicare a nessun soggetto non specificatamente autorizzato i dati personali comuni, sensibili, giudiziari, sanitari e/o altri dati, elementi, informazioni dei quali venite a conoscenza nell'esercizio delle vostre funzioni e mansioni all'interno del Comune. In caso di dubbio accertarsi sempre dal responsabile se il soggetto cui devono essere comunicati i dati sia o meno autorizzato a riceverli. E' vietata l'estrazione di originali e/o copie cartacee ed informatiche per uso personale di documenti, manuali, procedure, lettere, data base ecc di proprietà o in gestione del Comune, neppure se predisposte dal dipendente stesso.
2. Non effettuare colloqui con utenti o colleghi che contengano informazioni o dati personali, in presenza di persone non specificatamente incaricate a conoscere tali informazioni. In tal caso interrompere la comunicazione, riprendendola in luogo diverso e più riservato o attendere che i soggetti estranei non siano più presenti.
3. Non lasciare documenti sulla scrivania. Non lasciare documenti, lettere, fascicoli, appunti sopra la scrivania quando vi allontanate dalla postazione di lavoro. In particolare non lasciate sul tavolo materiali che non siano inerenti la pratica che state trattando in quel momento. Ciò vale soprattutto nel caso in cui abbiate mansioni di front office e di ricezione del pubblico.
4. Maneggiare e custodire con cura le stampe di materiale riservato. Non lasciate accedere alle stampe persone non autorizzate. Se la stampante non si trova sulla vostra scrivania recatevi il più in fretta possibile a ritirare le stampe. Per stampe riservate cercate di usare una stampante non condivisa oppure usate la modalità di stampa ritardata impostando un tempo sufficiente a permettervi di raggiungere la stampante prima dell'inizio della stampa. Distruggete personalmente le stampe quando non servono più o se esse siano solo delle "brutte copie" o bozze da ristampare perché errate.
5. Prestate attenzione alle fotocopie: fare fotocopie di documenti contenenti dati personali sensibili solo se strettamente necessario. Assicurarsi di non lasciare copie nella macchina e se necessario eliminare copie mal riuscite utilizzate una macchina distruggi-documenti (shredder)
6. Non gettare nel cestino le stampe di documenti che possono contenere informazioni confidenziali. Se trattate dati di particolare riservatezza, considerate la possibilità di dotarvi di una macchina distruggi-documenti (shredder). In ogni caso non gettate mai documenti cartacei senza averli prima fatti a pezzi.

Misure di sicurezza minime

Tutti i responsabili e gli incaricati dei dati devono attenersi alle seguenti misure:

I dati devono essere conservati in luoghi sicuri, con accesso protetto, meglio ancora con accesso regolamentato. L'ufficio in cui sono conservate le banche dati deve sempre essere custodito durante l'orario di apertura.

Si deve controllare e vigilare affinché i dati vengano trattati/utilizzati esclusivamente per gli scopi e con le modalità stabilite da norme di legge o da regolamenti interni.

La comunicazione tra uffici dell'Amministrazione deve contenere i soli dati necessari alle finalità per cui sono stati richiesti.

La trasmissione e la comunicazione di dati personali mediante posta, all'interno o all'esterno dell'Ente, deve avvenire sempre mediante supporti cartacei, digitali od ottici (cd/dvd) confezionati in buste o pacchi chiusi, se affidati a persone non autorizzate all'accesso.

E' indispensabile adottare tutte le misure necessarie affinché i documenti contenenti dati sensibili siano accessibili solo alle persone autorizzate.

Onde evitare accessi impropri ai dati personali, è opportuno comunicare e/o trattare gli stessi al riparo da sguardi indiscreti, soprattutto se in relazione a dati sensibili, con particolare riferimento agli sportelli, uffici, ecc.

La distruzione di documenti contenenti dati personali o dati sensibili deve avvenire in modo da rendere illeggibile il documento stesso.

Fuori orario di apertura o, comunque, in assenza di incaricati

Le banche dati su supporto cartaceo o digitale dovranno essere custodite in armadi chiusi a chiave ovvero, in mancanza di serratura, dovrà essere chiuso a chiave lo stesso locale adibito ad archivio.

Il Personal Computer, su cui sono memorizzate le banche dati o dal quale sono raggiungibili banche dati in rete, dovrà essere spento e, ove non sia possibile la chiusura a chiave dell'interruttore di accensione dello stesso, ovvero non sia prevista una password di accesso al PC, dovrà essere chiuso a chiave il locale ove è ubicato il PC.

Le chiavi degli armadi, dei locali, ovvero dei Personal Computer ove sono custodite le banche dati devono essere depositate in luogo sicuro; una copia di dette chiavi dovrà essere custodita dal Responsabile dell'ufficio o da un suo delegato.

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.

L'accesso all'elaboratore è protetto da password, che deve essere custodita dall'incaricato con la massima diligenza e non divulgata. La password deve essere attivata per l'accesso al PC e alla rete e per l'accesso a qualsiasi applicazione di rete. Non è consentita l'attivazione della password di accensione (bios).

Non è consentito installare autonomamente programmi provenienti dall'esterno, salvo autorizzazione esplicita dell'Amministratore di Sistema, perché sussiste il grave pericolo di portare Virus informatici e di alterare la stabilità delle applicazioni dell'elaboratore.

Non è consentito utilizzare strumenti *software* e/o *hardware* atti ad intercettare , falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici fatto salvo i sistemi di cifratura dei dati adottati dall'Ente al fine di rispettare la privacy. L'Art.4 della legge 547/93 ha introdotto nel codice penale il reato di "*accesso abusivo ad un sistema informatico o telematico*" all'Art.615-ter, che recita testualmente *"Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha diritto di escluderlo, è punito con la reclusione fino a tre anni".* Seguono delle ipotesi aggravate a seconda che il soggetto agente rivesta una determinata qualifica (es. Pubblico Ufficiale), o se si è usata violenza, o ancora se dal fatto deriva distruzione o danneggiamento del sistema.

Non è consentito l'uso di programmi diversi da quelli distribuiti ed installati ufficialmente dal Comune di Grado (dlg 518/92 sulla tutela giuridica del software e L.248/2000 nuove norme di tutela del diritto d'autore).

Non è consentito all'utente di modificare le caratteristiche impostate sul proprio Personal Computer, salvo previa autorizzazione esplicita dell'Amministratore del Sistema.

Sui *PC* dotati di scheda audio non è consentito l'ascolto di *files* audio, musicali, streaming audio-video da internet se non a fini prettamente lavorativi come corsi di formazione.

Non è consentita l'installazione sul proprio Personal Computer di alcun dispositivo di memorizzazione, comunicazione od altro (come ad esempio *masterizzatori, memorie USB, modem, Bluetoot, sistemi di comunicazione via GSM o GPRS, UMTS ecc. tali da permettere la comunicazione di dati in possesso dell'Ente all'esterno*), se non con l'autorizzazione espressa dell'Amministratore di Sistema.

Il Personal Computer deve essere spento alla fine dell'attività lavorativa quotidiana prima di lasciare gli uffici od in caso di assenze prolungate dall'ufficio. 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. In ogni caso dopo 10 minuti di inutilizzo del PC acceso con un utente attivo il sistema blocca automaticamente l'accesso che sarà garantito nuovamente solo inserendo la password dell'utente che ci lavorava.

Ogni utente, ove autorizzato, deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente l'Amministratore di Sistema nel caso in cui siano rilevati virus ed adottando quanto previsto dalle procedure di protezione antivirus.

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.

Utilizzo di PC portatili

L'utente è responsabile del Personal Computer portatile assegnatogli dall'Amministratore del Sistema e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro. Tale PC deve essere dotato di Password d'accensione e possibilmente del sistema di cifratura dei dati del disco fisso.

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

I Personal Computer portatili utilizzati all'esterno (convegni, ecc.), in caso di allontanamento, devono essere custoditi in un luogo protetto.

Utilizzo della rete del Comune di Grado

Le unità di rete sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità, vengono svolte regolari attività di controllo, amministrazione e backup da parte dell'Amministratore di Sistema.

Le password d'ingresso alla rete ed ai programmi sono segrete e vanno gestite secondo le procedure impartite. E' assolutamente proibito entrare nella rete e nei programmi con altri nomi utente.

L'Amministratore del Sistema può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza sia sui Personal Computer degli incaricati sia sulle unità di rete.

Costituisce buona regola la periodica (almeno ogni sei mesi) pulizia degli archivi, con cancellazione dei file obsoleti od inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati: è infatti assolutamente 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 comuni. E' buona regola evitare di stampare documenti e file non adatti su stampanti comuni: in caso di necessità la stampa in corso può essere cancellata.

Per la legge sulla privacy e sicurezza sono stati definiti, per ogni dipendente dell'Ente che lavora in un ambito d'ufficio, dei profili d'accesso ai dati dell'Ente. Ad ogni dipendente quindi è consentito accedere solo a trattamenti di dati, banche dati, archivi di dati o di chiavi d'accesso a cui è stata data regolare informativa ed autorizzazione. Se una persona, quindi, viene in possesso di dati di cui non ha autorizzazione scritta è obbligata ad avvisare immediatamente, per iscritto, , (basta una semplice e-mail) il Dirigente dell'Area e o il Responsabile del Servizio. Se ha scaricato dei dati e salvati, questi devono essere distrutti immediatamente.

Gestione delle Password

Le password di ingresso al PC, alla rete e di accesso ai programmi, sono previste ed assegnate dall'Amministratore di sistema. E' obbligatoria l'autonoma sostituzione della password da parte degli incaricati alla prima connessione al sistema.

Le password possono essere formate da lettere (maiuscole o minuscole) e numeri ricordando che lettere maiuscole o minuscole hanno significati diversi per il sistema ma devono avere almeno 8 caratteri.

Le password utilizzate dagli incaricati al trattamento hanno una durata massima di mesi 2, trascorsi i quali le password devono essere sostituite.

La password deve essere immediatamente sostituita nel caso si sospetti che la stessa abbia perso la segretezza.

Qualora l'utente venisse a conoscenza delle password di altro utente, è tenuto a darne immediata notizia alla persona interessata la quale avrà il compito di cambiarla immediatamente.

Utilizzo dei supporti digitali

Tutti i supporti digitali (come dischetti, CD, DVD, memorie USB, cassette, cartucce, dischi fissi ecc.) contenenti dati sensibili, anche quando sono o sembrano essere difettosi, devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato poiché una persona esperta potrebbe recuperare i dati memorizzati anche dopo la loro cancellazione.

I supporti digitali contenenti dati sensibili devono essere custoditi in archivi chiusi a chiave.

Non è consentito scaricare nel PC o nelle unità di rete files contenuti in supporti digitali non aventi alcuna attinenza con la propria prestazione lavorativa. Se si viene a conoscenza di tali dati dovete immediatamente avvisare, possibilmente per iscritto, il Dirigente dell'Area o Responsabile del Servizio.

Tutti i files di provenienza incerta od esterna, ancorché attinenti l'attività lavorativa, devono essere sottoposti al controllo ed alla relativa autorizzazione all'utilizzo da parte del Responsabile.

Uso della posta elettronica

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

E' fatto divieto di utilizzare le casella di posta elettronica dell'Ente per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mailing-list salvo diversa ed esplicita autorizzazione.

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

E' possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario.

La posta elettronica diretta all'esterno della rete informatica dell'ente può essere intercettata da estranei e, dunque, non deve essere usata per inviare documenti di lavoro "Strettamente Riservati" o che contengono dati personali di natura SENSIBILE e/o GIUDIZIARIA a meno che non si adotti un sistema di cifratura dei dati o il sistema di Posta Elettronica Certificata presente presso l'Ufficio Protocollo.

Per la trasmissione di files all'interno della rete dati del Comune di Grado è possibile utilizzare la posta elettronica prestando attenzione alle dimensioni degli allegati.

E' obbligatorio controllare i file attachements di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).

E' vietato inviare catene telematiche (o di Sant'Antonio). Se si dovessero ricevere messaggi di tale tipo, si deve comunicarlo immediatamente all'Amministratore del Sistema. Non si deve in alcun modo attivare gli allegati di tali messaggi.

Non è consentito l'uso durante il normale orario lavorativo di comunicazioni via e-mail che non sfruttino il sistema di posta elettronica del Comune di Grado se non a scopo di prove preventivamente autorizzate. Ne consegue che i collegamenti a sistemi di posta come Libero-Tiscali-Yahoo-Gmail ed altri non devono essere assolutamente utilizzati.

E' indispensabile che in fondo ad ogni messaggio di posta elettronica ci siano le proprie coordinate personali per poter essere immediatamente conosciuti all'esterno della struttura. Queste devono contenere almeno: Nome, Cognome, Ruolo o incarico, Nome del Comune, Indirizzo, Cap, Città, PV, Telefono e fax del proprio servizio.

Uso della rete internet e dei relativi servizi

Il Personal Computer abilitato alla navigazione in Internet costituisce uno strumento 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 software gratuito (freeware) e shareware prelevato da siti Internet, se non espressamente autorizzato dall'Amministratore del Sistema.

E' tassativamente vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line o simili salvo casi autorizzati dal rispettivo Dirigente e con il rispetto delle normali procedure di acquisto o da norme di legge e per fini strettamente istituzionali.

E' da evitare ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.

E' vietata la partecipazione a Forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames).

Protezione antivirus

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

Ogni utente è tenuto a controllare il regolare funzionamento e l'aggiornamento periodico del software installato.

Non è consentito l'utilizzo di supporti digitali come floppy disk, cd dvd r/rw, memorie USB, hard disk esterni, nastri magnetici, ecc… di provenienza ignota.

Ogni supporto digitale di provenienza esterna all'Amministrazione dovrà essere verificato mediante programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, dovrà essere consegnato all'Amministratore del Sistema.