Allegato A

REGOLAMENTO PER L'UTILIZZO DEL SISTEMA INFORMATICO COMUNALE

1. Premessa.

La progressiva diffusione delle tecnologie informatiche, dei dispositivi rimuovibili (CD, memory pen, dispositivi USB), come il libero accesso alla rete internet dal proprio Personal Computer o dalla propria postazione di lavoro, espongono il Comune di Teolo ad una serie di potenziali rischi, alcuni dei quali con coinvolgimento sia patrimoniale che penale, e possono creare problemi alla sicurezza ed all'immagine dell'Ente stesso.
Premesso che l'utilizzo delle risorse informatiche e telematiche dell'Ente deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito di un rapporto di lavoro, vengono qui richiamate alcune raccomandazioni, proibizioni ed obblighi che il dipendente ha nell'uso della infrastruttura informatica comunale, e più in generale nella fruizione del sistema informativo dell'Ente.

2. Norme e figure di Riferimento.

Nel presente documento si farà riferimento alle figure professionali individuate nel DPS: titolare del dato, responsabile del trattamento dei dati (anche RdT), amministratore di sistema (anche AdS), incaricato del trattamento, custode delle credenziali (CdC).
N.B.: In mancanza dell'Amm.re di Sistema, si dovrà fare riferimento al responsabile del trattamento;
in assenza del responsabile del trattamento, si farà riferimento al titolare del trattamento.
Si fa inoltre riferimento al "Disciplinare Tecnico" di riferimento (allegato al D.L.vo 196/2003 e successive integrazioni) nell'adozione delle misure minime di sicurezza per garantire la tutela e la salvaguardia dei dati personali, sensibili e giudiziari.
Per altro, essendo la materia in esame oggetto di continue e rapide evoluzioni, si fa riferimento alle indicazioni che costantemente vengono distribuite dall'AgID (Agenzia per l'Italia Digitale).

3. Utilizzo del Personal Computer.

Il Personal Computer (PC) o altro strumento analogo affidato al dipendente è uno strumento di lavoro.
Perciò l'utilizzo di detto strumento per finalità diverse dall'attività istituzionale è potenzialmente perseguibile nelle sedi opportune.
Inoltre ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.

L'accesso all'elaboratore deve essere protetto da password, che deve rispettare le regole di sicurezza minime (rif. DigitPA), e deve essere custodita dal dipendente diretto interessato con la massima diligenza, e non divulgata. La stessa password deve essere attivata per l'accesso alla rete, per l'eventuale screen saver e per il collegamento ad internet.
Non è consentita l'attivazione di ulteriori password, come ad es. la password di accensione (accesso modifiche bios) senza preventiva autorizzazione da parte dell'Amm.re del Sistema o del Responsabile del Trattamento.
Il Custode delle Credenziali (o in sua assenza l'Amministratore di Sistema), e solo per l'espletamento delle sue funzioni, ha la facoltà di accedere ai dati trattati da ciascuno, utilizzando le proprie credenziali di accesso.
L'Amministratore del Sistema, in assenza del Custode delle Credenziali, potrà accedere ai dati ed agli strumenti informatici esclusivamente per permettere all'Ente, titolare del trattamento, di accedere ai dati trattati da ogni incaricato con le modalità fissate, al solo fine di garantire l'operatività, la sicurezza del sistema ed il normale svolgimento dell'attività nei casi in cui si renda indispensabile ed indifferibile l'intervento; come ad esempio in caso di prolungata assenza od impedimento dell'incaricato, informando tempestivamente l'incaricato stesso dell'intervento di accesso realizzato.
Come da normativa, ogni accesso (ed in special modo tutti gli accessi dell'AdS) è tracciato e conservato per un periodo non inferiore ai 6 mesi.

Non è consentito installare autonomamente programmi (o aggiornamenti dei programmi) provenienti dall'esterno salvo previa autorizzazione esplicita dell'Amministratore del Sistema, in

quanto sussiste il grave pericolo di trasferire virus informatici e/o di alterare la stabilità delle applicazioni e del sistema del PC e/o della rete.
Non è consentito l'uso di programmi diversi da quelli distribuiti ed installati ufficialmente dall'Ente.
Non è consentito all'utente modificare le caratteristiche impostate sul proprio PC, salvo preventiva autorizzazione esplicita dell'Amministratore di Sistema.
Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici, o in caso di assenze prolungate dall'ufficio. 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. In ogni caso, per prolungate assenze dal posto di lavoro, e con l'improrogabile necessità di lasciare l'elaboratore acceso, deve essere eventualmente bloccato l'accesso con la relativa password.
Non è consentita l'installazione sul proprio PC di nessun dispositivo di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, memorie rimovibili, ecc.), se non con l'autorizzazione espressa dell'Amministratore di Sistema.
Ogni utente deve prestare la massima attenzione ai supporti di origine esterna (CD, mem. USB, floppy), avvertendo immediatamente il responsabile delle misure minime di sicurezza nel caso in cui vengano rilevati virus, malware, spyware, ecc. E' inoltre obbligatorio accertarsi preventivamente, tramite appositi strumenti hardware e/o software, che tali dispositivi non possano essere utilizzati, anche inconsapevolmente, per trasferire virus o altri programmi pericolosi, o per trafugare informazioni riservate dell'Ente.

4. Crimine informatico e tutela del diritto d'autore
Vista la legge 518/92 sulla tutela giuridica del software, e la legge 248 del 18/08/2000 relativa alla tutela del diritto d'autore, è vietata la riproduzione o la duplicazione con qualsiasi mezzo e a qualsiasi titolo dei programmi informatici come anche dei manuali a corredo dei programmi. Il responsabile del Servizio Informativo, o altra struttura preposta, e qualora tecnicamente possibile, può eventualmente predisporre copie di riserva dei programmi dotati di regolare licenza allo scopo di prevenire accidentali perdite dell'originale e quindi danni patrimoniali all'azienda. Tale copia di riserva potrà essere usata soltanto per ripristinare le funzionalità del programma, quando non sia possibile utilizzare il programma originale.
E' fatto specifico divieto a tutti gli utenti di installare qualunque tipo di software (anche se freeware, shareware, ...) che non sia preventivamente autorizzato dal Responsabile del Trattamento o dall'Amministratore di Sistema.
L'inosservanza di questa disposizione, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, con conseguenti costi per il ripristino, può esporre l'autore a gravi responsabilità civili e penali.

5. Tutela dei dati memorizzati sulle stazioni di lavoro personali e reimpiego dei supporti
L'azienda persegue una politica di centralizzazione nella gestione dei dati aziendali, per cui progressivamente le gestioni "locali" di dati diminuiranno, sostituite da gestioni centralizzate su server. Fino a che questo processo non sarà stato completato, potranno esistere gestioni locali di dati su stazioni di lavoro personali (personal computer connessi o non connessi in rete), ma con la possibilità di gestire localmente documenti e/o dati la cui tutela è demandata all'utente. L'effettuazione dei salvataggi con frequenza opportuna (almeno comunque settimanale) su supporti magnetici o su altro supporto adeguato, e la conservazione degli stessi in luogo idoneo (possibilmente sotto chiave e/o in contenitori ignifughi) è compito del singolo dipendente che usa la stazione (nel caso di stazioni di lavoro usate da un solo utilizzatore); nel caso di stazioni di lavoro condivise, l'operazione è eseguita da un incaricato opportunamente individuato dal Responsabile del Trattamento.
È vietato l'uso di supporti di memorizzazione removibili (floppy, memorie USB, CD-R o RW, hdd esterni, ecc.) per la memorizzazione di dati personali e/o sensibili. Deroghe a tale regola sono possibili solo nei casi in cui sia possibile dimostrare il corretto uso dei supporti di memorizzazione ai sensi del D.L. 196/2003 Allegato B, punti 21 e 22:

- è possibile il reimpiego del supporto solo nel caso non siano più recuperabili le informazioni precedentemente memorizzate;
- nel caso non sia garantibile il requisito di cui al punto precedente, il supporto removibile dopo l'uso andrà distrutto. In generale i supporti di memorizzazione - anche non removibili -

che contengono dati personali o sensibili, nel caso non possano essere cancellati in maniera da renderne irrecuperabile il contenuto, una volta dimessi - per es. per obsolescenza o per guasto -, dovranno essere distrutti o smaltiti in maniera tale che il contenuto non sia più recuperabile.

I supporti magnetici, ottici o elettronici contenenti dati sensibili e/o giudiziari (punto 21 del disciplinare tecnico) devono essere custoditi in archivi chiusi a chiave.

6. Utilizzo della rete del Comune di Teolo

Le unità di memoria e le unità di rete sono aree di condivisione di informazioni strettamente professionali e non devono 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.

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

Come precedentemente indicato, le password d'accesso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite. È assolutamente proibito entrare nella rete e nei programmi con altre credenziali (nomi utente/password di altre persone).

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: è infatti assolutamente da evitare un'archiviazione ridondante, ciò per evitare di occupare spazio inutilmente (con degrado delle prestazioni e con maggiori costi), per agevolare i salvataggi, e per consentire un corretto utilizzo del dato (senza il rischio di operare su copie errate o non allineate).

Dati non più movimentati, o conservati solo per occasionale consultazione (ad es. fotografie, scansioni, vecchi archivi), dovranno essere periodicamente (ad es.ogni 6 mesi) trasferiti su supporti ottici non modificabili (ad es. dvd-rom); la registrazione potrà essere effettuata da personale tecnico di supporto, che, verificata la corretta memorizzazione, provvederà anche alla eliminazione dei dati dai dischi di rete.

È' cura dell'utente adeguarsi alle direttive correnti effettuando la stampa dei dati solo se strettamente necessario, utilizzando perciò per quanto possibile il formato elettronico, ed evitando il consumo inutile di carta, di toner, e di energia. Nel caso, è da impostare la stampa in modalità fronte/retro.

Nel caso di stampe su dispositivi comuni (multifunzione e stampanti di rete) sarà cura dell'utente ritirarle prontamente dai vassoi qualora contengano informazioni sensibili.

È buona regola evitare di stampare su stampanti comuni documenti o file non idonei (documenti non supportati, o file con contenuto grafico di elevate dimensioni), onde evitare l'eventuale blocco della stampante; in caso di blocco o di urgenza, la stampa in corso potrà essere cancellata.

E' inoltre da limitare allo stretto necessario l'utilizzo di stampe a colori, che comportano costi elevati, verificando anche la corretta impostazione del dispositivo (stampa in bianco e nero o monocromatica).

7. Utilizzo della rete di comunicazione

Per l'Ente, internet è un bene aziendale condiviso e pertanto va gestito nel rispetto delle esigenze complessive dell'azienda. E' uno strumento fondamentale che consente di essere costantemente aggiornati attraverso siti di informazioni concernenti l'attività svolta.

Il PC abilitato alla navigazione in Internet costituisce uno strumento necessario allo svolgimento della propria attività lavorativa.

In funzione di ciò viene fatto esplicito e tassativo divieto di connettere in rete stazioni di lavoro se non previa esplicita e formale autorizzazione dell'Amministratore del Sistema. È altresì vietato alterare in qualsiasi modo la configurazione software della stazione di lavoro o di altri dispositivi direttamente connessi alla rete dati o fonia per quanto attiene all'accesso alla rete, comprendendo in ciò anche il divieto di aggiungere protocolli di rete o servizi in rete (per es. condivisione di dispositivi in rete, browsing di risorse di rete, ecc...).

È vietata l'installazione non autorizzata di modem o altri dispositivi per linee analogiche o digitali che sfruttino il sistema di comunicazione in fonia o dati per l'accesso a risorse esterne o interne all'azienda.
È vietata l'installazione di hardware o software di qualsiasi tipo (anche solo come variazione dei parametri di connessione) che consenta o faciliti il by-pass delle misure di presidio del confine aziendale (per es. software di comunicazione che garantiscano accessi che non transitino dai firewall aziendali o dagli altri accessi autorizzati e presidiati).
Si procederà con l'aggiornamento del sistema operativo e dei software antivirus e antintrusione su tutte le postazioni aventi connessione diretta con l'esterno, in quanto, se da una parte Internet offre una miriade di informazioni, comprese le procedure più aggiornate sulla sicurezza, dall'altra funge da veicolo per la trasmissione di codice pericoloso (virus - trojan - worm ecc.); è assolutamente vietato alterare le impostazioni delle funzioni di protezione.
È anche fatto divieto di utilizzare in qualsiasi modo la rete aziendale (LAN, intranet, internet) per fini non espressamente autorizzati. E' pertanto vietato usare la connessione internet per accedere a siti non pertinenti l'attività lavorativa ed è assolutamente vietato il traffico (visione, scaricamento o caricamento) di file di qualsiasi tipo non strettamente necessari all'attività lavorativa, con particolare attenzione al materiale non autorizzato o illecito (immagini e video non autorizzati, o pornografici, audio o software non autorizzati o irregolari).
E' vietato condividere cartelle o file accessibili dall'esterno, in ogni forma (anche se protetta).
Si richiama l'attenzione degli operatori circa la possibilità di tracciare il traffico effettuato; è infatti possibile, su richiesta dell'autorità preposta, l'estrazione di appositi log (registrazioni delle attività, crittografate) per gli eventuali accertamenti a fronte di specifiche segnalazioni, sia dai server dell'Ente che presso l'operatore fornitore della connettività.
È importante controllare, ogni qualvolta si visiti un sito internet, eventuali certificati esposti o finestre che propongono contratti d'installazione o altre offerte "pseudo-commerciali"; al riguardo è necessario rispondere negativamente a tali proposte in quanto nella stragrande maggioranza dei casi si installano involontariamente utility contenenti spy (programmi in grado di inviare i dati personali ed aziendali a siti di raccolta).
È fatto divieto all'utente lo scarico di ogni tipo di software, anche gratuito (freeware) e shareware, prelevato da siti internet, se non espressamente autorizzato dal Responsabile del Trattamento o dall'Amm.re di Sistema.
È tassativamente vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili salvo i casi espressamente autorizzati dal dirigente o dal responsabile del servizio, e con il rispetto delle normali procedure di sicurezza.
È da evitare, dalle postazioni dell'Ente, ogni forma di registrazione / sottoscrizione a siti i cui contenuti non siano legati all'attività lavorativa. È altresì vietata la partecipazione a forum e/o newsgroup non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), l'uso di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames), se queste attività sono eseguite con strumenti dell'Ente.
Per quanto non ulteriormente specificato, si fa riferimento alle linee guida emanante dal Garante per la Protezione dei dati personali (vedi sito www.garanteprivacy.it), e alle indicazioni dell'AgID (www.agid.gov.it).

8. Conservazione delle parole chiave di accesso e dei dispositivi di accesso
Le password di accesso alla rete, ad internet, ai programmi, ed alla posta elettronica, sono previste ed attribuite inizialmente dall'Amministratore del Sistema. Le password dovranno essere aggiornate in base alle regole che verranno comunicate; tali regole saranno anche a disposizione in apposita area riservata del sito o della rete informatica comunale.
L'eventuale impostazione di una password per lo screen saver o per il blocco del desktop, dovrà essere uguale a quella usata per gli altri accessi, e perciò periodicamente aggiornata di conseguenza.
È necessario procedere alla modifica della password almeno ogni tre mesi, che scendono a due mesi come previsto nel caso di trattamento di dati sensibili e di dati giudiziari (integrazioni al punto 5 del disciplinare tecnico allegato al Codice della privacy, d.lgs.vo n.196/2003).
L'utente è tenuto a conservare nella massima segretezza la parola di accesso ai sistemi e qualsiasi altra informazione legata al processo di autenticazione.
In base all'attuale sistema di autenticazione (che potrà essere aggiornato all'occorrenza), le password possono essere formate da lettere (maiuscole e minuscole) e numeri, ricordando che

lettere maiuscole e minuscole hanno significati diversi per il sistema; devono essere composte da almeno otto caratteri e non devono contenere riferimenti agevolmente riconducibili all'incaricato (punto 5 del disciplinare tecnico).
La password deve essere immediatamente sostituita, dandone comunicazione all'Amm.re del Sistema, nel caso si sospetti che la stessa abbia perso la caratteristica di segretezza.
Qualora l'utente venisse a conoscenza delle password di altro utente, è tenuto a darne immediata notizia al Responsabile del Trattamento o all'Amm.re del Sistema.
Inoltre l'utente è tenuto a scollegarsi dal sistema o bloccare l'accesso al sistema ogni qual volta sia costretto ad assentarsi dal locale nel quale è ubicata la stazione di lavoro, o nel caso ritenga di non essere in grado di presidiare l'accesso alla medesima (per es. perché impegnato in compiti che richiedono totalmente la sua attenzione).
L'utente è inoltre tenuto a conservare con la massima cura eventuali dispositivi alternativi per l'accesso ai sistemi aziendali (ad es. badge, codici, chiavi elettroniche, ecc.) e ad usarli conformemente alle specifiche indicazioni d'uso. La perdita o il danneggiamento degli stessi sarà sanzionata.

È necessario che i responsabili delle unità organizzative operino un costante e meticoloso controllo volto ad evitare pratiche che la normativa identifica come veri e propri crimini, ma che nella pratica comune risultano assai diffuse e a vari livelli tollerate (ad es. lo scambio di credenziali).
Ciò risulta tanto più importante se si pensa che senza la collaborazione attiva di tutte le articolazione organizzative aziendali non sarà possibile arginare i costi sempre crescenti indotti da un cattivo uso delle attrezzature informatiche (si pensi a titolo esemplificativo al proliferare dei virus informatici che potrebbe essere arginato adottando semplici regole di controllo delle informazioni provenienti dall' esterno, ecc..).
Si dispone quindi che i responsabili delle varie macro articolazioni organizzative, di concerto con l'Amm.re del Sistema, adottino gli atti e le misure necessarie a garantire un adeguato controllo relativamente alle norme di buon uso dei sistemi informatici e di telecomunicazione dell'azienda.

9. Utilizzo di PC portatili.
L'utente è responsabile del PC portatile (notebook) assegnatogli dall'Ente e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.
Ai notebook 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 notebook possono essere utilizzati all'esterno per soli motivi di lavoro o istituzionali; in caso di allontanamento dall'Ente, devono essere custoditi in un luogo protetto.
Non è ammesso l'utilizzo per scopi personali.
Particolare attenzione andrà prestata nell'utilizzo del notebook all'esterno dell'Ente; connessioni ad altre reti (cablate o wireless) potrebbero danneggiare le configurazioni del sistema, e potrebbe essere strumento di intrusione per programmi dannosi (spyware in primis).
Anche l'utilizzo di strumenti rimovibili (memory pen, dischi esterni, ecc.) deve essere effettuato con le necessarie cautele e protezioni affinché eventuali programmi dannosi non possano poi essere trasferiti all'interno dell'Ente alla prima riconnessione alla rete locale.
E' vietato l'utilizzo di sistemi portatili personali all'interno dell'Ente senza la preventiva autorizzazione dell'Amm.re di Sistema, che potrà preventivamente verificare la configurazione del dispositivo prima di consentirne la connessione in rete.

9a. Utilizzo di desktop virtuali.
L'Ente ha iniziato a sperimentare l'adozione di sistemi alternativi al PC o al notebook, per l'utilizzo delle procedure informatiche (di seguito "client virtuali" o "desktop virtuali").
L'utilizzo di queste postazioni rappresenta un miglioramento della sicurezza, oltre che delle performance e dei consumi. L'utente deve utilizzare le credenziali o il badge assegnatogli per attivare queste postazioni; dette credenziali sono strettamente personali e non devono essere ceduta ad altri per nessun motivo. L'accesso ai sistemi ed alla rete segue le stesse modalità (e regole) descritte precedentemente.
In caso di allontanamento dalla postazione di lavoro l'utente non deve lasciare attivata la sessione corrente, anche in presenza di altri utilizzatori della medesima postazione.

E' possibile l'utilizzo delle credenziali su qualsiasi altra postazione di lavoro all'interno dell'Ente, sempre ricordando che è responsabilità del titolare delle credenziali ogni operazione svolta, indipendentemente dalla postazione utilizzata.

10. Uso della posta elettronica.

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

Qualsiasi utente autorizzato al trattamento ed alla gestione di una casella di posta elettronica dovrà attenersi alle regole di seguito indicate:

a. L'invio della posta elettronica deve essere effettuato esclusivamente da personale autorizzato e a destinatari connessi all'attività dell'Ente, e solo per messaggi pertinenti il rapporto di lavoro.
b. È fatto divieto di utilizzare le caselle di posta elettronica dell'Ente (dominio) per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail-list; qualsiasi iscrizione a mailing list o news riguardanti siti di informazione concernenti l'attività o aggiornamenti per la risoluzione di problemi software o hardware può essere sottoscritta esclusivamente con l'approvazione del Responsabile per il Trattamento dei dati;
c. È fatto divieto di utilizzare messaggi estranei al rapporto di lavoro o inerenti relazioni tra colleghi.
d. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili, obsoleti (cestino, posta inviata, ecc) e soprattutto allegati ingombranti.
e. Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o pre-contrattuali per il Comune di Teolo deve essere visionata od autorizzata dal responsabile di servizio, ed in ogni modo è opportuno fare riferimento alle procedure in essere per la corrispondenza ordinaria.
f. E' possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario, ma di norma per la comunicazione ufficiale è obbligatorio avvalersi degli strumenti previsti (tra cui eventualmente la Posta Elettronica Certificata)
g. Per la trasmissione di file all'interno dell'Ente è consigliato (come da normativa vigente) utilizzare la posta elettronica, prestando attenzione alla dimensione degli allegati; i messaggi non necessari devono essere cancellati appena possibile, verificando periodicamente anche i messaggi "inviati", e svuotando il cestino.
h. È obbligatorio controllare i file allegati ai messaggi di posta elettronica prima del loro utilizzo; non eseguire download di file di ogni tipo da siti Web o Ftp non conosciuti
i. È vietato inviare catene telematiche (note anche come "di Sant'Antonio"), cartoline elettroniche, messaggi inutili, allegati eseguibili o potenzialmente pericolosi. Se si dovessero ricevere messaggi di tale tipo, si deve comunicarlo immediatamente al Responsabile del trattamento. Non si devono in alcun caso aprire od eseguire gli allegati di tali messaggi;
j. Non è concesso variare le impostazioni del browser e dei programmi di gestione della posta per nessun motivo tranne che sia ritenuto temporaneamente necessario per motivi di vitale importanza per la manutenzione dello/degli strumenti elettronici. Tale modifica potrà essere apportata solo previa informazione ed autorizzazione dell'Amministratore di Sistema o del responsabile del Trattamento dei dati (si consideri in particolare l'impostazione disabilitata per la visualizzazione dell'anteprima automatica che consente al software antivirus di disinfettare eventuale codice malevolo dei messaggi in ingresso).

Al fine di avere un utilizzo corretto del gestionale di posta elettronica si ricorda quanto segue:

a. I messaggi di posta elettronica che transitano sul dominio dell'Ente (comune.teolo.pd.it) vengono preventivamente scansionati da un filtro sui file, da un programma antivirus, e da un programma antispam.
b. Tutte le mail, sia in entrata che in uscita, vengono preventivamente controllate da tale software.
   Se il messaggio contiene in allegato dei file di tipo vietato (es.: .exe, .pif, .dll, .vbs, .scr, .cpl), verrà rifiutato senza alcuna segnalazione al destinatario (con segnalazione al mittente).

Se il messaggio contiene un virus (in base alla scansione dell'antivirus del mail server), l'intero messaggio verrà messo in "quarantena" (area riservata); verrà contestualmente inviato un messaggio all'utente destinatario ed al mittente. Il messaggio resterà in quarantena per ca. 4 giorni; dopo verrà definitivamente eliminato.
Può succedere che alcuni allegati vengano interpretati dai programmi di protezione come virus anche se sono file non dannosi (falsi positivi); in questo caso, occorre richiedere la rispedizione dall'area di quarantena nella propria casella di posta (operazione che viene eseguita dall'Amm.re del sistema).
In casi ricorrenti, è opportuno aggiornare le white list (vedi punto successivo).

c. Il programma antispam opera un primo filtro sugli indirizzi mittente, rifiutando i messaggi che provengono da server segnalati come "spam" (liste di server "spam" aggiornate quotidianamente, a disposizione dei sistemi antispam).
Può succedere che alcuni indirizzi (generalmente del tipo @tin.it o @libero.it, ma non solo) possano transitare da alcuni di questi server, in quanto le reti tin.it e/o libero.it smistano gli utenti in base alla disponibilità della propria struttura. In questo caso, anche gli indirizzi dei mittenti verranno inseriti nelle liste di "spam"; con conseguente perdita del messaggio inviato.
Per alcuni mittenti, con cui è frequente lo scambio di mail, è possibile inserire il loro indirizzo "fidato" in una "white list", che permetterà sempre il transito di tutta la corrispondenza da/per l'indirizzo in oggetto.
Attenzione: l'inserimento in white list impone il transito di tutto quanto proveniente dal mittente indicato, senza alcun ulteriore controllo (né filtri, né antivirus); perciò l'inserimento in white list è da effettuarsi solo per indirizzi assolutamente affidabili.

d. E' vietato usare il client di posta elettronica per la gestione di caselle di posta che non siano all'interno del dominio (comune.teolo.pd.it).

e. Di norma, i virus che vengono trasmessi attraverso posta elettronica si presentano come allegato al messaggio; tuttavia alcuni tipi di virus (worm), arrivano all'interno del personal computer come script, ossia sono contenuti nel corpo del messaggio e si presentano a prima vista come testo o immagine.
E' assolutamente da evitare l'apertura di ogni tipo di file (anche solo immagine e/o testo) proveniente da mittenti non noti.

f. Quando vengono ricevuti messaggi indesiderati, è consigliato inoltrarli all'indirizzo indicato per la gestione dello spam, per alimentare un elenco di casi di spam, utile per "istruire" il filtro in modo che possa eliminare futuri invii.

Per quanto non ulteriormente specificato, si fa riferimento alle linee guida emanante dal Garante per la Protezione dei dati personali (vedi sito www.garanteprivacy.it) .

11. I Virus informatici malicious code

Al fine di prevenire le infezioni informatiche si adottano le seguenti misure:

- Si dotano tutte le attrezzature di confine e tutti i server in dotazione all'Ente di un adeguato software antivirus e si stabilisce l'aggiornamento delle firme almeno in ragione giornaliera. Le regole per mantenere aggiornate le attrezzature saranno pubblicate nell'intranet aziendale, con comunicazione a tutto il personale a mezzo mail.
- Si dota di software antivirus e si predispongono adeguati meccanismi per mantenere tale software aggiornato su tutti i PC collegati alla rete in modo automatico. Per i PC non collegati alla rete ma correntemente utilizzati, l'aggiornamento dovrà avvenire a cura dell'Amministratore del Sistema con cadenza almeno mensile.
- Nel caso non sia possibile predisporre adeguati meccanismi per mantenere il software antivirus aggiornato, sarà cura del consegnatario della stazione di lavoro aggiornare il software almeno in ragione settimanale seguendo l'opportuna procedura tecnica di aggiornamento concordata con l'Amm.re di Sistema.
- Per quanto possibile sono stati configurati i profili abilitativi di tutti gli utenti aziendali con privilegi che non consentano l'installazione o l'esecuzione di alcuni tipi di programmi non autorizzati sia sulle macchine client come anche sui server.

Si invitano inoltre gli utenti:

- alla massima cautela nella gestione dei supporti magnetici e della posta elettronica: in particolare ogni qualvolta un supporto di memorizzazione (dischetto removibile, nastro magnetico, disco magneto-ottico, usb e ogni altro supporto di memorizzazione removibile) sia stato utilizzato su un computer diverso dal proprio, occorrerà verificare l'assenza di virus mediante un programma antivirus aggiornato. Se non vi è l'assoluta certezza che il proprio computer possieda un antivirus aggiornato, non deve assolutamente essere utilizzato il supporto di memorizzazione in quanto potenzialmente infetto;
- in generale sarebbe bene conoscere sempre con precisione quale sia la fonte dei dati, ed essere certi che tale fonte sia affidabile e sicura; è preferibile non utilizzare un supporto di memorizzazione removibile di cui non si conosca la fonte;
- evitare di leggere o utilizzare allegati di messaggi di posta elettronica che non provengano da fonti certe, riconosciute e sicure; nel caso pervenga un messaggio di tale natura procedere immediatamente alla eliminazione. Nel caso si abbia il sospetto che il proprio sistema di elaborazione sia stato infettato avvertire il personale tecnico competente e non operare per alcun motivo scambio di supporti di memorizzazione o posta elettronica con altri. Nel caso si abbia notizia di un nuovo tipo di virus, comunicare tale informazione al servizio Sistemi Informativi e non inviare indiscriminati messaggi a tutti i propri conoscenti, dato che ciò genera falsi allarmi e di inutili catene di Sant'Antonio.

12. Osservanza delle disposizioni in materia di privacy e delle presenti regole.
È obbligatorio attenersi alle disposizioni in materia di Privacy e di misure minime di sicurezza, come indicate nella lettera di designazione di incaricato del trattamento dei dati ai sensi del disciplinare tecnico allegato al DLgs. n. 196/2003 e successive integrazioni.
Il mancato rispetto o la violazione delle regole contenute nel presente documento 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 documento. Le proposte verranno esaminate dai dirigenti, dai responsabili di servizio e dal Responsabile del Trattamento.