



CITTÀ DI TRANI

Medaglia d'Argento

Settore

Sistemi Informativi – Centro Elaborazione Dati

**Regolamento per l'utilizzo
dei Sistemi Informativi
del Comune di Trani**

Indice

1.	Entrata in vigore del regolamento e pubblicità	pag. 3
2.	Campo di applicazione del regolamento	pag. 3
3.	Amministrazione delle Risorse Informative	pag. 4
4.	Utilizzo del Personal Computer	pag. 5
5.	Gestione e assegnazione delle credenziali di autenticazione	pag. 7
6.	Utilizzo della rete del Comune di Trani	pag. 8
7.	Utilizzo e conservazione dei supporti rimovibili	pag. 10
8.	Utilizzo di PC portatili	pag. 10
9.	Uso della posta elettronica	pag. 11
10.	Navigazione in Internet	pag. 13
11.	Protezione antivirus	pag. 14
12.	Utilizzo dei telefoni, fax e fotocopiatrici dell'Ente	pag. 14
13.	Osservanza delle disposizioni in materia di Privacy	pag. 15
14.	Accesso ai dati trattati dall'utente	pag. 15
15.	Sistema di controllo	pag. 16
16.	Sanzioni e deroghe	pag. 16
17.	Aggiornamento e revisione	pag. 16

1. Entrata in vigore del regolamento e pubblicità

- 1.1 Il nuovo regolamento entrerà in vigore il 21 luglio 2009. Con l'entrata in vigore del presente regolamento tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi abrogate e sostituite dalle presenti.
- 1.2 Copia del presente regolamento è affisso nella bacheca aziendale, all'Albo Pretorio, nonché pubblicato sul sito istituzionale dell'Ente e nell'apposita area condivisa in rete LAN dove ogni utente può visionarlo così da consentirne la massima diffusione e conoscenza.

2. Campo di applicazione del regolamento

- 2.1 Il nuovo regolamento si applica a tutti i dipendenti, senza distinzione di ruolo e/o livello, nonché a tutti i collaboratori dell'azienda a prescindere dal rapporto contrattuale con la stessa intrattenuto (collaboratori a progetto, in stage, ecc.), a tutti gli Amministratori (Consiglieri comunali, Assessori, ecc.) che abbiano accesso alla Rete del Comune di Trani, costituita dall'insieme delle Risorse informatiche, cioè dalle Risorse infrastrutturali e dal patrimonio informativo digitale. Le Risorse infrastrutturali sono le componenti hardware/software e gli apparati elettronici collegati alla Rete Informatica comunale. Il Patrimonio informativo è l'insieme delle banche dati in formato digitale e in generale tutti i documenti prodotti tramite l'utilizzo dei suddetti apparati.
- 2.2 Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche e telematiche, per "utente" deve intendersi chiunque, dirigente, dipendente o collaboratore (collaboratore a progetto, in stage, ecc.) in possesso di specifiche credenziali di autenticazione. Tale figura potrà anche venir indicata quale "incaricato del trattamento". Per "utente", deve altresì intendersi, anche l'Amministratore (Consigliere Comunale, Assessore, ecc.) che anche saltuariamente ha accesso alle risorse informatiche e telematiche per svariate ragioni.
- 2.3 È fatto altresì obbligo di notifica del presente Regolamento a tutti i fornitori e manutentori (hardware e software) delle apparecchiature informatiche comunali.

3. Amministrazione delle Risorse Informative

- 3.1 Il Dirigente del Settore Sistemi Informativi nomina, ove non vi abbia già provveduto, il Responsabile del Centro Elaborazione Dati (Amministratore di Sistema), il quale è il soggetto cui è conferito il compito tecnico di sovrintendere alle Risorse informative e telematiche del Comune di Trani, nonché alle seguenti attività:
- a) Gestire hardware/software di tutte le strutture tecniche informatiche di appartenenza del Comune di Trani, collegate in rete o meno.
 - b) Gestire esecutivamente (creazione, attivazione, disattivazione e tutte le relative attività amministrative) gli account di rete e i relativi privilegi di accesso alle risorse, assegnati agli utenti della Rete Informatica comunale secondo quanto stabilito da ogni Dirigente.
 - c) Monitorare o utilizzare qualunque tipo di sistema informatico o elettronico per controllare il corretto utilizzo delle risorse di rete, dei computer e degli applicativi, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori.
 - d) Creare, modificare, rimuovere o utilizzare qualunque account o privilegio, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori.
 - e) Rimuovere programmi software dalle risorse informatiche assegnate agli utenti, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori.
 - f) Rimuovere componenti hardware dalle risorse informatiche assegnate agli utenti, solo se rientranti nelle normali attività di manutenzione, gestione della sicurezza e di protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori.
 - g) Utilizzare le credenziali di accesso di amministrazione del sistema, o l'account di un utente tramite reinizializzazione della relativa password, per accedere ai dati o alle applicazioni presenti su una risorsa informatica assegnata a un utente in caso di prolungata assenza, irrintracciabilità o impedimento dello stesso. Tale utilizzo deve essere esplicitamente richiesto dal Dirigente di struttura dell'utente assente o impedito e deve essere limitato al tempo strettamente necessario al compimento delle attività indifferibili per cui è stato richiesto.

- 3.2 Il Responsabile del Centro Elaborazione Dati si attiene alle disposizioni impartite dal Dirigente del Settore Sistemi Informativi e ha l'onere di segnalare a quest'ultimo qualunque infrazione che minacci la sicurezza della Infrastruttura e il patrimonio informativo comunale, nonché le violazioni del presente Regolamento e delle norme in materia.
- 3.3 Il Responsabile del Centro Elaborazione Dati coordina le unità operative applicate, gli interventi tecnici dei fornitori, dei prestatori di servizi e ogni attività del Sistema Informativo relazionando al Dirigente del Settore Sistemi Informativi.
- 3.4 Il Responsabile del Centro Elaborazione Dati deve verificare settimanalmente che i sistemi antivirus centralizzati siano perfettamente operativi.

4. Utilizzo del Personal Computer

- 4.1 **Il Personal Computer affidato all'utente è uno strumento di lavoro.** Ogni utilizzo non inerente all'attività lavorativa è vietato perché può contribuire a innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza dell'Infrastruttura e dei dati. Il personal computer deve essere custodito con cura evitando ogni possibile forma di danneggiamento.
- 4.2 Il personal computer dato in affidamento all'utente permette l'accesso alla rete del Comune di Trani solo attraverso specifiche **credenziali di autenticazione** come meglio descritto al successivo punto 5 del presente Regolamento.
- 4.3 Il Comune di Trani rende noto che il personale incaricato che opera presso il Settore Sistemi Informativi – C.E.D. è autorizzato a compiere interventi nel Sistema Informatico dell'Ente, diretti a garantire la sicurezza e la salvaguardia del Sistema stesso, nonché per ulteriori motivi tecnici e/o manutentivi, ad es. aggiornamento, sostituzione, implementazione di programmi, manutenzione hardware ecc.). Detti interventi, in considerazione dei divieti di cui ai successivi punti nn. 9.2 e 10.1, potranno anche comportare l'accesso in qualunque momento ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica, nonché alla verifica sui siti internet acceduti dagli utenti abilitati alla navigazione esterna. La stessa facoltà, sempre ai fini della sicurezza del sistema e per garantire la normale operatività dell'Ente, si applica anche in caso di assenza prolungata o impedimento dell'utente.

- 4.4 Il personale incaricato del Settore Sistemi Informativi – C.E.D. ha la facoltà di collegarsi e visualizzare in remoto il desktop delle singole postazioni PC al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza contro virus, spyware, malware, ecc. L'intervento viene effettuato esclusivamente su chiamata dell'utente o, in caso di oggettiva necessità, a seguito della rilevazione tecnica di problemi nel sistema informatico e telematico. In quest'ultimo caso, e sempre che non si pregiudichi la necessaria tempestività ed efficacia dell'intervento, verrà data comunicazione della necessità dell'intervento stesso.
- 4.5 Non è consentito l'uso di programmi diversi da quelli ufficialmente installati dal personale del Settore Sistemi Informativi – C.E.D. per conto del Comune di Trani né viene consentito agli utenti di installare autonomamente programmi provenienti dall'esterno, sussistendo infatti il grave pericolo di introdurre virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti. L'inosservanza della presente disposizione espone l'Amministrazione comunale a gravi responsabilità civili. Si evidenzia inoltre, che le violazioni della normativa a tutela dei diritti d'autore sul software che impone la presenza nel sistema di software regolarmente licenziato, vengono sanzionate anche penalmente. A tal proposito, il personale del Settore Sistemi Informativi – C.E.D., procederà come previsto al successivo punto 6.6 del presente Regolamento.
- 4.6 Salvo preventiva espressa autorizzazione del personale del Settore Sistemi Informativi – C.E.D., non è consentito all'utente modificare le caratteristiche impostate sul proprio PC né procedere a installare dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, ecc.).
- 4.7 Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il personale del Settore Sistemi Informativi – C.E.D., nel caso in cui siano rilevati virus non rimossi dal sistema centralizzato, e adottando quanto previsto dal successivo punto 11 del presente Regolamento relativo alle procedure di protezione antivirus.
- 4.8 Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio o in caso di suo inutilizzo. In ogni caso, lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso. A tal proposito, il

personale del Settore Sistemi Informativi – C.E.D., può adottare procedure remote automatiche di arresto del personal computer.

- 4.9 Ogni tipo di intervento su apparecchiature informatiche che possano interessare o influenzare la rete LAN, i Server, i singoli personal computer, i notebook, le stampanti di rete, ecc. dovranno obbligatoriamente essere comunicati formalmente al personale dei Sistemi Informativi – C.E.D. con il quale saranno concordati tempi e modi d'intervento, previa autorizzazione del Dirigente della Ripartizione Sistemi Informativi – C.E.D.

5. Gestione e assegnazione delle credenziali di autenticazione

- 5.1 Le credenziali di autenticazione per l'accesso alla rete vengono assegnate dal personale del Settore Sistemi Informativi – C.E.D., previa formale richiesta del Dirigente o Responsabile del Settore – Ufficio, nell'ambito del quale verrà inserito e andrà a operare il nuovo utente. Nel caso di collaboratori a progetto, ecc., la preventiva richiesta verrà inoltrata direttamente dal Responsabile dell'ufficio con il quale il collaboratore si coordina nell'espletamento del proprio incarico.
- 5.2 Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (user id o account), assegnato dal Settore Sistemi Informativi – C.E.D., associato a una parola chiave (password) riservata che dovrà essere sostituita obbligatoriamente al primo accesso dall'operatore. Le credenziali di accesso sono strettamente personali e non devono essere comunicate ad alcuno. Non sono previste eccezioni. Non è consentita l'attivazione della password di accensione (BIOS).
- 5.3 La parola chiave, formata da lettere (maiuscole o minuscole) e/o numeri, anche in combinazione fra loro, deve essere composta da almeno otto caratteri e non deve contenere riferimenti agevolmente riconducibili all'incaricato.
- 5.4 È necessario procedere alla modifica della parola chiave a cura dell'utente, incaricato del trattamento, oltre che al primo utilizzo (punto 4.2), successivamente almeno ogni sei mesi (ogni tre mesi nel caso invece di trattamento di dati sensibili attraverso l'ausilio di strumenti elettronici), qualora non imposta dal sistema informatizzato.
- 5.5 Qualora la parola chiave dovesse essere sostituita, per decorso del termine sopra previsto e/o in quanto abbia perduto la propria

riservatezza, si procederà in tal senso d'intesa con il personale del Settore Sistemi Informativi – C.E.D., al quale dovrà essere inoltrata precisa istanza motivata.

6. Utilizzo della rete del Comune di Trani

- 6.1 Nel rispetto dei principi di trasparenza, collaborazione e condivisione, previsti dalla normativa vigente in materia, ogni Dirigente, reciprocamente, metterà a disposizione della struttura le banche dati digitali di propria competenza. I Dirigenti di Ripartizione nel rispetto del Piano Esecutivo di Gestione (P.E.G.), conferito con Delibera di Giunta, prenotano telematicamente la spesa e attendono la conferma della copertura finanziaria dal Direttore di Ragioneria.
- 6.2 Al fine di favorire il processo di riordino e di riduzione degli adempimenti amministrativi, nel rispetto della Legge 241/90 e del DPR 445/2000, gli uffici pubblici comunali, hanno l'obbligo di accedere ai sistemi informativi delle diverse ripartizioni al fine di estrarre copia di documenti e atti autorizzatori, di cui lo stesso Ente ne rilascia gli originali.
- 6.3 Il Sistema Informativo del Comune di Trani è strutturato nel cosiddetto "dominio locale" cui ogni personal computer è connesso per mezzo della rete LAN o WAN. Dette regole (policy) garantiscono la sicurezza della rete informativa comunale e la condivisione delle informazioni; pertanto, ogni apparecchiatura informatica e l'utente che ne fa uso sono soggetti a tali regole. Solo eventuali difficoltà tecnico-operative, o esigenze temporanee, valutate dal Responsabile del Centro Elaborazione Dati, possono derogarvi.
- 6.4 Per l'accesso alla rete del Comune di Trani ciascun utente deve essere in possesso della specifica credenziale di autenticazione.
- 6.5 È assolutamente proibito entrare nella rete e nei programmi con un codice d'identificazione utente diverso da quello assegnato. Le parole chiave d'ingresso alla rete e ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite.
- 6.6 Per motivi di sicurezza, è assolutamente vietato connettere autonomamente nuove apparecchiature informatiche (personal computer, notebook, stampanti di rete, ecc.) alla rete LAN comunale. Dette operazioni dovranno essere obbligatoriamente concordate con il personale del Settore Sistemi Informativi – C.E.D., previa richiesta del

Dirigente afferente l'Ufficio comunale interessato, al Dirigente Informatico che autorizzerà o meno le operazioni richieste.

- 6.7 Le cartelle utenti presenti nei server e le banche dati digitali del Comune di Trani sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto qualunque file che non riguardi l'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 del personale del Settore Sistemi Informativi – C.E.D. Si ricorda che tutti i dischi o altre unità di memorizzazione locali (es. disco C: interno PC) non sono soggetti a salvataggio da parte del personale incaricato del Settore Sistemi Informativi – C.E.D. La responsabilità del salvataggio dei dati ivi contenuti è pertanto a carico del singolo utente.
- 6.8 Il personale del Settore Sistemi Informativi – C.E.D. può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la Sicurezza sia sui PC degli incaricati sia sulle unità di rete, nonché alla rimozione di ogni altra applicazione diversa da quella ufficialmente installata dal personale incaricato del Settore Sistemi Informativi – C.E.D., non licenziata o non pertinente l'attività lavorativa.
- 6.9 Al fine di migliorare le prestazioni e la sicurezza del Sistema Informativo comunale, nonché del singolo PC o notebook collegati alla rete LAN, il personale del Settore Sistemi Informativi – C.E.D., predisporrà le procedure remote necessarie alla rimozione di software inutili e/o non strettamente legati all'attività lavorativa.
- 6.10 Per motivi di sicurezza, il personale del Settore Sistemi Informativi – C.E.D., predisporrà le procedure necessarie a inibire l'accesso alla rete LAN degli utenti oltre l'orario ordinario di servizio. Particolari esigenze dovranno essere formalmente comunicate al suddetto Settore.
- 6.11 Risulta opportuno che, con regolare periodicità (almeno ogni tre mesi), ciascun utente provveda alla pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati, essendo infatti necessario evitare un'archiviazione ridondante.

7. Utilizzo e conservazione dei supporti rimovibili

- 7.1 Tutti i supporti magnetici rimovibili (dischetti, CD e DVD riscrivibili, supporti USB, ecc.), contenenti dati sensibili o riservati, devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto o, successivamente alla cancellazione, recuperato.
- 7.2 Al fine di assicurare la distruzione e/o inutilizzabilità di supporti magnetici rimovibili contenenti dati sensibili, ciascun utente dovrà contattare il personale del Settore Sistemi Informativi – C.E.D. e seguire le istruzioni da questo impartite.
- 7.3 In ogni caso, i supporti magnetici contenenti dati sensibili devono essere adeguatamente custoditi dagli utenti in armadi chiusi.
- 7.4 È vietato l'utilizzo di supporti rimovibili personali.
- 7.5 L'utente è responsabile della custodia dei supporti e dei dati aziendali in essi contenuti.

8. Utilizzo di PC portatili (notebook)

- 8.1 L'utente è responsabile del PC portatile di cui ha la disponibilità e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.
- 8.2 Ai PC portatili si applicano le regole di utilizzo previste dal presente regolamento, con particolare attenzione alla rimozione di eventuali file elaborati prima della riconsegna.
- 8.3 I PC portatili utilizzati all'esterno, in caso di allontanamento, devono essere custoditi con diligenza, adottando tutti i provvedimenti che le circostanze rendono necessari, per evitare danni o sottrazioni.
- 8.4 Tali disposizioni si applicano anche nei confronti di incaricati esterni, ecc.

9. Uso della posta elettronica

- 9.1 **La casella di posta elettronica assegnata all'utente è uno strumento di lavoro.** Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.
- 9.2 È fatto divieto di utilizzare le caselle di posta elettronica per motivi diversi da quelli strettamente legati all'attività lavorativa. In questo senso, **a titolo puramente esemplificativo**, l'utente non potrà utilizzare la posta elettronica per:
- a) l'invio e/o la ricezione di allegati contenenti filmati o brani musicali (es. mp3, ecc.) non legati all'attività lavorativa;
 - b) l'invio e/o la ricezione di messaggi personali o per la partecipazione a dibattiti, aste on line, concorsi, forum o mailing-list, ecc.;
 - c) la partecipazione a catene telematiche (o di Sant'Antonio). Se si dovessero peraltro ricevere messaggi di tale tipo, si deve comunicarlo immediatamente al personale del Settore Sistemi Informativi – C.E.D. Non si dovrà in alcun caso procedere all'apertura degli allegati a tali messaggi.
 - d) la trasmissione a mezzo di posta elettronica di dati sensibili, confidenziali e personali di alcun genere, salvo i casi espressamente previsti dalla normativa vigente in materia di protezione dei dati personali (D.Lgs. 196 del 30/6/2003).
 - e) Inoltrare e/o inviare messaggi di posta elettronica all'interno del Comune di Trani non pertinenti l'attività lavorativa o contenenti allegati di notevole dimensione.
 - f) Inviare tramite posta elettronica user-id, password, configurazioni della rete interna, indirizzi e nomi dei sistemi informatici.
- 9.3 La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.
- 9.4 Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali del Comune di Trani, ovvero contenga documenti da considerarsi riservati, deve essere visionata o autorizzata dal Responsabile d'Ufficio.
- 9.5 È possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario. Si

evidenzia però che le comunicazioni ufficiali, da inviarsi mediante gli strumenti tradizionali (fax, posta, ...), devono essere autorizzate e firmate dal Dirigente di Ripartizione e/o dai Responsabili di Ufficio, a seconda del loro contenuto e dei destinatari delle stesse.

- 9.6 È obbligatorio porre la massima attenzione nell'aprire i file allegati di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).
- 9.7 Al fine di garantire la funzionalità del servizio di posta elettronica aziendale e di ridurre al minimo l'accesso ai dati, nel rispetto del principio di necessità e di proporzionalità, in caso di assenze programmate (ad es. per ferie o attività di lavoro fuori sede dell'assegnatario della casella) il sistema invierà automaticamente messaggi di risposta contenenti le "coordinate" di posta elettronica di un altro soggetto o altre utili modalità di contatto della struttura. In tal caso, la funzionalità deve essere attivata dall'utente.
- 9.8 In caso di assenza non programmata (ad es. per malattia) la procedura - qualora non possa essere attivata dal lavoratore avvalendosi del servizio webmail entro due giorni - verrà attivata dall'Ente purché comunicata per iscritto, a cura del Responsabile dell'Ufficio, Settore, Ripartizione di riferimento, al Settore Sistemi Informativi – C.E.D.
- 9.9 Sarà comunque consentito al superiore gerarchico dell'utente o, comunque, sentito l'utente, a persona individuata dall'azienda, accedere alla casella di posta elettronica dell'utente per ogni ipotesi in cui si renda necessario (ad es.: mancata attivazione della funzionalità di cui al punto 9.7; assenza non programmata e impossibilità di attendere i due giorni di cui al punto 9.8).
- 9.10 Il personale del Settore Sistemi Informativi – C.E.D., nell'impossibilità di procedere come sopra indicato e nella necessità di non pregiudicare la necessaria tempestività ed efficacia dell'intervento, potrà accedere alla casella di posta elettronica per le sole finalità indicate al punto 4.3.
- 9.11 Al fine di ribadire agli interlocutori la natura esclusivamente aziendale della casella di posta elettronica, i messaggi possono contenere un avvertimento standardizzato nel quale sia dichiarata la natura non personale dei messaggi stessi.
- 9.12 Tutti i messaggi di posta elettronica sono soggetti a scansione antivirus. Il sistema Informatizzato, a tutela della propria integrità, procederà alla rimozione di eventuali allegati sospetti. Qualora risulti impossibile ricevere allegati di posta elettronica, è necessario

comunicarlo al personale del Settore Sistemi Informativi – C.E.D. il quale, previa richiesta scritta, valuterà la possibilità di download del file allegato.

10. Navigazione in Internet

10.1 Il PC assegnato al singolo utente, eventualmente abilitato alla navigazione in Internet, costituisce uno strumento dell'Ente utilizzabile esclusivamente per lo svolgimento della propria attività lavorativa. È quindi assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa.

10.2 In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare internet per:

- a) l'upload o il download di software gratuiti (freeware) e shareware, nonché l'utilizzo di documenti provenienti da siti web o http, se non strettamente attinenti all'attività lavorativa (filmati e musica) e previa verifica dell'attendibilità dei siti in questione (nel caso di dubbio, dovrà essere contattato, a tal fine, il personale del Settore Sistemi Informativi – C.E.D.);
- b) effettuare ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, fatti salvi i casi direttamente autorizzati dal Dirigente di Ripartizione (o eventualmente dal Responsabile d'Ufficio e/o del Settore Sistemi Informativi – C.E.D.) e comunque nel rispetto delle normali procedure di acquisto;
- c) ogni forma di registrazione a siti i cui contenuti non siano strettamente legati all'attività lavorativa;
- d) la partecipazione a Forum non professionali, l'utilizzo di chat line, di bacheche elettroniche, facebook, myspace e qualunque registrazione sulla rete internet anche utilizzando pseudonimi (o nickname) se non espressamente autorizzati dal Responsabile d'Ufficio;
- e) l'accesso, tramite internet, a caselle webmail di posta elettronica personale non preventivamente autorizzate.

10.3 Al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa del Comune di Trani, si rende nota l'adozione di uno specifico sistema di blocco o filtro automatico che previene determinate

operazioni quali l'upload o l'accesso a determinati siti inseriti in una black list gestiti da idonea strumentazione (firewall, proxy server, ecc.).

- 10.4 Gli eventuali controlli, compiuti dal personale incaricato del Settore Sistemi Informativi – C.E.D. ai sensi del precedente punto 4.3, potranno eseguirsi mediante un sistema di controllo dei contenuti (Proxy server, ecc.) o mediante “file di log” della navigazione svolta. I file di log vengono conservati nel pieno rispetto delle disposizioni in materia di privacy e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori.

11. Protezione antivirus

- 11.1 Il sistema informatico del Comune di Trani è protetto da software antivirus aggiornato quotidianamente. Ogni utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informativo comunale mediante virus o mediante ogni altro software aggressivo.
- 11.2 Nel caso il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente sospendere ogni elaborazione in corso senza spegnere il computer, nonché segnalare prontamente l'accaduto al personale del Settore Sistemi Informativi – C.E.D., qualora il virus non risulti rimosso.
- 11.3 Ogni dispositivo magnetico di provenienza esterna all'Azienda dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, dovrà essere prontamente consegnato al personale del Settore Sistemi Informativi – C.E.D., qualora il virus non risulti rimosso.

12. Utilizzo dei telefoni, fax e fotocopiatrici aziendali

- 12.1 **Il telefono aziendale affidato all'utente è uno strumento di lavoro.** Ne viene concesso l'uso esclusivamente per lo svolgimento dell'attività lavorativa, non essendo quindi consentite comunicazioni a carattere personale o comunque non strettamente inerenti l'attività lavorativa stessa. La ricezione o l'effettuazione di telefonate personali è consentito solo nel caso di comprovata necessità e urgenza, mediante il telefono fisso aziendale a disposizione.

- 12.2 Qualora venisse assegnato un cellulare aziendale all'utente, quest'ultimo sarà responsabile del suo utilizzo e della sua custodia. Al cellulare aziendale si applicano le medesime regole sopra previste per l'utilizzo del telefono aziendale: in particolare è vietato l'utilizzo del telefono cellulare messo a disposizione per inviare o ricevere SMS o MMS di natura personale o comunque non pertinenti rispetto allo svolgimento dell'attività lavorativa. L'eventuale uso promiscuo (anche per fini personali) del telefono cellulare aziendale è possibile soltanto in presenza di preventiva autorizzazione scritta e in conformità delle istruzioni al riguardo impartite dal Responsabile dell'Ufficio.
- 12.3 È vietato l'utilizzo dei fax aziendali per fini personali, tanto per spedire quanto per ricevere documentazione, salva diversa esplicita autorizzazione da parte del Responsabile dell'Ufficio.
- 12.4 È vietato l'utilizzo delle fotocopiatrici aziendali per fini personali, salvo preventiva ed esplicita autorizzazione da parte del Responsabile dell'Ufficio.

13. Osservanza delle disposizioni in materia di Privacy

- 13.1 È obbligatorio attenersi alle disposizioni in materia di Privacy e di misure minime di sicurezza, come indicato nella lettera di designazione dell'incaricato del trattamento dei dati ai sensi del Disciplinare tecnico allegato al D. Lgs. n. 196/2003.

14. Accesso ai dati trattati dall'utente

- 14.1 Oltre che per motivi di sicurezza del sistema informativo, anche per motivi tecnici e/o manutentivi (ad esempio, aggiornamento, sostituzione, implementazione di programmi, manutenzione hardware, ecc.) o per finalità di controllo e programmazione dei costi dell'Ente (ad esempio, verifica costi di connessione a internet, traffico telefonico, ecc.), comunque estranei a qualsiasi finalità di controllo dell'attività lavorativa, è facoltà della Dirigenza dell'Ente, tramite il personale del Settore Sistemi Informativi – C.E.D. o addetti alla manutenzione, accedere direttamente, nel rispetto della normativa sulla privacy e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori, a tutti gli strumenti informatici aziendali e ai documenti ivi contenuti, nonché ai tabulati del traffico telefonico.

15. Sistemi di controllo

- 15.1 Per motivi di sicurezza e protezione dei dati, ogni attività compiuta nella rete Informatica può essere sottoposta a registrazione in appositi file e riconducibili, indirettamente, all'utente. Detti file possono essere soggetti a trattamento solo per fini istituzionali, per attività di monitoraggio e controllo e possono essere messi a disposizione dell'Autorità Giudiziaria in caso di accertata violazione delle norme vigenti. La riservatezza delle informazioni è soggetta a quanto dettato dal D. Lgs. 196/2003 e s.m.i. e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori.
- 15.2 In caso di anomalie, il personale incaricato del Settore Sistemi Informativi – C.E.D. effettuerà controlli anonimi che si concluderanno con avvisi generalizzati diretti ai dipendenti del Settore in cui è stata rilevata l'anomalia, nei quali si evidenzierà l'utilizzo irregolare degli strumenti aziendali e si inviteranno gli interessati ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite. Controlli su base individuale potranno essere compiuti solo in caso di successive ulteriori anomalie.
- 15.3 In nessun caso verranno compiuti controlli indiscriminati se non giustificati da esigenze di sicurezza dell'intero Sistema e del Patrimonio Informativo comunale.

16. Sanzioni e deroghe

- 16.1 È fatto obbligo a tutti gli utenti di osservare le disposizioni portate a conoscenza con il presente regolamento, a eccezione delle manifeste necessità e dei casi, esclusivamente attestati e motivati dal Dirigente del Settore Sistemi Informativi – C.E.D. con idoneo e formale atto amministrativo. Il mancato rispetto e/o la violazione delle regole sopra ricordate è perseguibile nei confronti del personale dipendente con provvedimenti disciplinari e/o risarcitori previsti dai vigenti CC.CC.NN.LL., nonché con tutte le azioni civili e penali consentite dalle vigenti norme.

17. Aggiornamento e revisione

- 17.1 Tutti gli utenti possono proporre integrazioni motivate al presente Regolamento indirizzandole al proprio Dirigente di riferimento, il quale

potrà inoltrarle al Dirigente del competente Settore Sistemi Informativi – C.E.D. per gli opportuni adempimenti.

- 17.2 Il presente Regolamento è soggetto a revisione ogni qualvolta se ne manifesti la necessità.