Città di Trani

Medaglia d'Argento al Merito Civile

Provincia BAT

REGOLAMENTO IT

Anno 2025

SOMMARIO

Premessa

Il presente disciplinare intende fornire ai dipendenti e collaboratori, denominati anche utenti o persone autorizzate al trattamento dei dati personali, del Comune di Trani le indicazioni per una corretta e adeguata gestione delle informazioni personali, in particolare attraverso l'uso di sistemi, applicazioni e strumenti informatici dell'Ente.

Tutti gli strumenti utilizzati dal lavoratore, intendendo con ciò i PC, notebook, risorse, e-mail ed altri strumenti con relativi software e applicativi (di seguito più semplicemente "Strumenti"), sono messi a disposizione dal Comune di Trani per rendere la prestazione lavorativa. Gli Strumenti, nonché le relative reti informatiche dell'Ente a cui è possibile accedere tramite gli stessi, rappresentano il domicilio informatico del Comune di Trani. I dati personali e le altre informazioni dell'utente, che sono registrati negli Strumenti o che si possono eventualmente raccogliere tramite il loro uso, sono utilizzati per finalità istituzionali, per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio dell'Ente.

Per tutela del patrimonio dell'Ente si intende la sicurezza informatica e la tutela del sistema informatico dell'Ente.

Tali informazioni sono altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, considerato che il presente disciplinare costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli, sempre nel rispetto di quanto disposto dal Regolamento Europeo n. 2016/679 e dal Codice in materia di protezione dei dati personali ai sensi del D.lgs 196/03 così come modificato dal D.lgs 101/18.

Viene, infine, precisato che non sono installati o configurati sui sistemi informatici in uso agli utenti apparati hardware o strumenti software aventi come scopo il controllo a distanza dell'attività dei lavoratori, nel rispetto della disciplina lavoristica ex L. 300/70 e D.lgs 151/2015 (Job Acts).

L'utilizzo delle risorse informatiche e telematiche deve sempre ispirarsi, in applicazione di quanto disposto dagli artt. 2104 e 2105 c.c., al **principio della diligenza, fedeltà e correttezza, comportamenti che normalmente si adottano nell'ambito dei rapporti di lavoro**, adottando, quindi, tutte le cautele e le precauzioni necessarie per evitare le possibili conseguenze dannose alle quali un utilizzo non avveduto di tali strumenti può produrre, anche in considerazione della difficoltà di tracciare una netta linea di confine tra l'attività lavorativa, la sfera personale e la vita privata del lavoratore e di terzi che interagiscono con quest'ultimo.

In tale contesto, l'Autorità Garante per la protezione dei dati personali ha emanato la deliberazione n. 13 del 1° marzo 2007 "Lavoro: Le linee guida del Garante per posta elettronica e internet" con la quale ha inteso **prescrivere ai datori di lavoro alcune misure per conformare alle disposizioni vigenti il**

trattamento di dati personali effettuato per verificare il corretto utilizzo, nello svolgimento del rapporto di lavoro, della posta elettronica e della rete internet.

La progressiva diffusione delle nuove tecnologie informatiche, le maggiori possibilità di interconnessione tra computer e l'aumento di informazioni trattate con strumenti elettronici aumentano infatti i rischi legati alla sicurezza e all'integrità delle informazioni oltre alle conseguenti responsabilità previste dalla normativa vigente in materia.

Il Comune di Trani con il presente atto adotta un Disciplinare interno diretto ad evitare che comportamenti inconsapevoli possano innescare problemi alla gestione della Rete informatica e/o minacce alla sicurezza nel trattamento dei dati personali di qualsivoglia tipo (personale, sensibile e giudiziario) e per richiamare le indicazioni e le misure necessarie ed opportune per il corretto utilizzo, nel rapporto di lavoro, dei personal computer (fissi e portatili), dei dispositivi elettronici in genere, della posta elettronica e di internet, **definendone le modalità di utilizzo nell'ambito dell'attività lavorativa.**

Le prescrizioni di seguito previste si aggiungono ed integrano le specifiche istruzioni già fornite a tutti i dipendenti del Comune di Trani, in attuazione del Codice in materia di protezione dei dati personali e del Regolamento Generale sulla protezione dei dati personali (Regolamento UE 2016/679).

Il Comune di Trani *(d'ora in avanti anche "Ente")* **deve provvedere a garantire un servizio continuativo, nel suo stesso interesse, ed assicurare la riservatezza delle informazioni e dei dati, in maniera tale da evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla sicurezza nel trattamento dei dati o diminuire l'efficienza delle risorse informatiche.** L'Ente riconosce il valore fondamentale dell'utilizzo di strumenti di comunicazione sia nella comunicazione interna che con l'utenza esterna, anche al fine di ridurre i tempi di risposta e di migliorare pertanto l'efficienza del proprio operato istituzionale.

Le regole di gestione del patrimonio informativo dell'Ente – inteso come dati, documenti digitali ex D.Lgs. 82/2005, etc – sono stabilite dal manuale di gestione documentale approvato con DGC n. 46 del 23.05.2025 e che qui si richiama a fare parte integrante e sostanziale del presente documento.

CAPO I – Disposizioni Generali

Art. 1 - Campo di applicazione

Il presente Disciplinare **si applica a tutti i dipendenti, senza distinzione di ruolo o livello, nonché a tutti i collaboratori del Comune di Trani** a prescindere dal rapporto contrattuale con lo stesso intrattenuto (consulenti, tirocinanti, borsisti, volontari, ditte esterne autorizzate, ecc.).
Inoltre, il presente Disciplinare regolamenta l'utilizzo di tutti i dispositivi collegati alla rete informatica e quindi direttamente gestibili e controllabili a norma di legge, attraverso gli opportuni strumenti, dal personale autorizzato.
Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche e telematiche, per "utente" deve intendersi ogni soggetto, in possesso di specifiche credenziali di autenticazione, operante su computer in rete informatica.
Il presente Disciplinare contiene le disposizioni relative alle corrette modalità di utilizzo della rete informatica e di tutte le risorse, in conformità e nel rispetto di quanto previsto dalla specifica normativa di settore e dalle ulteriori disposizioni emanate dall'Ente.
Gli strumenti informatici oggetto del presente Disciplinare sono di proprietà dell'Ente e sono messi a disposizione degli Utenti al fine di permettere il quotidiano svolgimento delle proprie prestazioni lavorative. Essi sono essenzialmente individuabili nei computer, negli apparati removibili, nei sistemi di identificazione e di autenticazione informatica, Internet e negli strumenti di scambio di comunicazioni e file, nella posta elettronica, posta elettronica certificata e in qualsiasi altro programma e apparecchiatura informatica destinata a memorizzare o a trasmettere dati e informazioni.
È responsabilità di tutti i soggetti che utilizzano gli strumenti informatici messi a disposizione, di applicare e rispettare puntualmente le disposizioni del presente disciplinare.
È esentato dall'applicazione del presente Disciplinare, e limitatamente a quanto necessario per il corretto svolgimento delle proprie funzioni, il responsabile dei sistemi informativi.

Art. 2 - Riferimenti normativi

Legge 23 dicembre 1993 n. 547 aggiornamento del Codice penale rispetto ai reati informatici;

Legge 18 marzo 2008, n.48 "Ratifica ed esecuzione della Convenzione del Consiglio d' Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento interno" Codice Amministrazione Digitale (D.lgs. 7 marzo 2005, n. 82);ù

Direttiva NIS (Direttiva 2016/1148) recepita attraverso il D.lgs. 18 maggio 2018, n. 65, in vigore dal 24 giugno 2018 (strategia europea per la sicurezza informatica recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione; riservato alle solo infrastrutture critiche) ;

Decreto del Presidente del Consiglio dei ministri 8 agosto 2019 (Decreto di costituzione del CSIRT presso la Presidenza del Consiglio dei ministri – Dipartimento Informazioni per la Sicurezza);

Regolamento (UE) 2016/679 o GDPR sullaprotezione dei dati personali e D.lgs. 196/2003 novellato dal D.lgs. 101/2018;

Provvedimento Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008(G.U. n. 300 del 24 dicembre 2008)(modificato in base al provvedimento del 25 giugno 2009);

Direttiva 2016/680 recepita con D.lgs. 18 maggio 2018, n. 51 (sicurezza informatica dei dati trattati dalle autorità);

eIDAS (electronicaI Dentification Authentication and Signature) o Regolamento (UE)2014/910 (sicurezza informatica applicata alla firma e alle transazioni elettroniche);

DPCM 17 febbraio 2017 o Decreto Gentiloni (delinea i nuovi assetti organizzativi dell'architettura nazionale di cyber security. Viene anche varata una nuova strategia nazionale di cyber security con l'adozione del nuovo Piano Nazionale);

Misure minime di sicurezza ICT per le pubbliche amministrazioni (Circolare 18 aprile 2017, n. 2/2017)

Circolari AgID (n. 2 e 3 del 2018);

Piano Triennale per l'informatica della PA (AgID);

Accessibilità art. 4 della Direttiva europea 2016/2102 recepita con la Legge n. 4 del 9 gennaio 2004 e successive integrazioni e modificazioni;

Legge 20.5.1970, n. 300, recante "Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro e norme sul collocamento";

"Linee guida del Garante per posta elettronica e internet" in Gazzetta Ufficiale n. 58 del 10 marzo 2007;

Articolo 23 del D.Lgs. n. 151/2015 (c.d. Jobs Act) che modifica e rimodula la fattispecie integrante il divieto dei controlli a distanza, nella consapevolezza di dover tener conto, nell'attuale contesto produttivo, oltre agli impianti audiovisivi, anche degli altri strumenti «dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori» e di quelli «utilizzati dal lavoratore per rendere la prestazione lavorativa»;

Art. 3 – Principi

I principi alla base del presente regolamento sono i seguenti:

i. Tutela dei diritti, delle libertà e della dignità delle persone;
ii. Tutela del dipendente: alla luce dell'art. 4, comma 1, L. n. 300/1970 e s.m.i., la regolamentazione della materia indicata nel presente Disciplinare non è finalizzata all'esercizio di un controllo a distanza dei lavoratori da parte del datore di lavoro ma solo a permettere a quest'ultimo di utilizzare i servizi informatici per fare fronte ad esigenze produttive od organizzative e di sicurezza nel trattamento dei dati personali. È sempre garantito al singolo lavoratore il controllo sui propri dati personali secondo quanto previsto dagli articoli 15-16-17-18-20-21-78 del Regolamento UE 2016/679.
iii. Tutela del patrimonio informativo dell'organizzazione e riduzione dei rischi connessi al trattamento dei dati e quindi della probabilità di:
    a. Accessi illegittimi ai sistemi o agli applicativi;
    b. Modifiche indesiderate alle informazioni;

c. Perdita della disponibilità dei dati;

iv. Conformità normativa e allineamento agli standard di mercato;

v. Riduzione della superficie di esposizione rispetto alle vulnerabilità ovvero le debolezze sistemiche trasformabili in un evento indesiderato nel caso si attui una minaccia;

vi. Corretto bilanciamento tra usabilità e sicurezza, adottando contromisure basate sull'Analisi dei rischi;

vii. Adozione della Regola del minimo previlegio rispetto alla finalità (separation of duties policy), in ottica di stratificazione dei profili e degli accessi;

viii. Diritto alla disconnessione degli utilizzatori dai sistemi mobile al di fuori dell'orario di lavoro.

Art. 4 – Condotta ed utilizzo dei sistemi informativi

a) I sistemi e i servizi IT sono forniti agli utenti per rendere la propria prestazione lavorativa in accordo alla missione dell'Ente;

b) Gli utenti sono responsabili dell'utilizzo dei sistemi e dei servizi IT in modo eticamente corretto, sicuro, legale e conforme al presente regolamento, tenendo nella massima considerazione i diritti, le libertà fondamentali, la sensibilità delle persone come anche gli obiettivi primari dell'Ente;

c) L'utilizzatore di sistemi e servizi IT è direttamente responsabile di tutte le attività effettuate con gli account dell'organizzazione ricevuti, con particolare riguardo alle informazioni inviate o richieste, caricate o visualizzate nel proprio personal computer, applicativo software o piattaforma web dell'ente e non;

d) All'utilizzatore di sistemi e servizi IT sono tassativamente vietate le seguenti attività:

- La creazione o la trasmissione di qualsiasi materiale o documento, in qualsiasi formato, che possa essere ragionevolmente ritenuto offensivo, diffamatorio o osceno;
- La creazione o la trasmissione di materiale o documento in qualsiasi formato che possa ragionevolmente essere ritenuto suscettibile di molestare, intimidire, danneggiare o turbare qualcuno o qualcosa;
- La trasmissione non autorizzata di documenti su canali o sistemi non sicuri o non omologati dai Sistemi Informativi dell'Ente;
- L'invio di dati di tipo sensibili su canali non sicuri (un esempio di strumento da evitare per inviare dati sensibili è la posta elettronica dell'organizzazione, che viaggia in chiaro quando inviata ad altro dominio di posta; è da ritenersi invece accettabilmente sicuro l'invio ad altro utente di posta dello stesso dominio. In caso di dubbi è necessario

contattare i Sistemi Informativi dell'Ente o adottare tecniche di criptazione con invio della chiave su altro media);

- La creazione o la trasmissione di qualsiasi documento non riconducibile alle funzioni o ai compiti di competenza oppure estraneo alle attività dell'organizzazione;
- L'accesso non autorizzato ai sistemi o ai servizi IT;

e) L'introduzione degli strumenti mobile (forniti dall'organizzazione o BYOD) pone il problema dell'equilibrio tra vita privata e vita professionale, data la progressiva trasformazione degli strumenti di comunicazione da asincroni a tempo reale. È riconosciuto all'utilizzatore il diritto alla disconnessione dai dispositivi mobile al di fuori dell'orario di lavoro e dai turni di pronta disponibilità.

CAPO II – RUOLI

Art. 5 - Utente dei servizi e degli applicativi

i. L'Utente dei servizi e degli applicativi è un individuo espressamente autorizzato ad effettuare trattamenti di dati attraverso applicazioni software. Le autorizzazioni possono essere nominali o per funzione ovvero per appartenenza a uno specifico gruppo di lavoro;
ii. Le autorizzazioni sono concesse dal Responsabile di Unità Operativa che individua ambito e profilo di autorizzazione con comunicazione ai Sistemi Informativi, che provvede alle necessarie impostazioni a livello di sistema o di applicativo;
iii. L'Utente dei servizi e degli applicativi deve attenersi scrupolosamente alle procedure operative indicate nei manuali d'uso, nelle note operative, negli aiuti in linea, illustrati durante le sessioni formative o comunicate durante il cosiddetto learning by doing (imparare facendo);
iv. Gli utenti dei servizi e degli applicativi hanno l'obbligo di segnalare immediatamente al proprio Responsabile qualsiasi evento o situazione di rischio della sicurezza dei sistemi e delle reti di comunicazione, al fine di tutelare il patrimonio informativo dell'organizzazione e garantire la necessaria continuità operativa.

Art. 6 - Dirigenti o Responsabili di Area

i. Il Responsabile di Area, in forza della nomina a soggetto Designato, provvede all'autorizzazione degli utenti (incaricati del trattamento dei dati) individuando ambito e profilo di autorizzazione anche in funzione degli applicativi software in uso;
ii. Con periodicità almeno annuale provvede alla verifica dell'ambito e del profilo di autorizzazione degli utilizzatori assegnati alla propria Unità Operativa, comunicando ai Sistemi Informativi (Sistema Informativo Dell'organizzazione) le eventuali variazioni;
iii. Il Responsabile di Area ha l'obbligo di segnalare immediatamente al Responsabile dei Sistemi Informativi eventuali anomalie o situazioni di rischio della sicurezza dei sistemi e delle reti di comunicazione, al fine di tutelare il patrimonio informativo dell'organizzazione e garantire la necessaria continuità operativa.

Art. 7 Responsabile Sistemi Informativi

Il Responsabile dei Sistemi Informativi è il responsabile delle tecnologie dell'Informazione e della Comunicazione dell'Ente. Il Responsabile dei Sistemi Informativi è direttamente coinvolto nella definizione delle strategie ICT e delle policy di gestione e innovazione dell'ICT dell'organizzazione, entrambi necessarie per la sicurezza del patrimonio informativo dell'organizzazione. È responsabile del governo del sistema informativo ovvero l'insieme delle attività promosse e gestite dal management e dai sistemi informativi, al fine di trovare la migliore integrazione possibile tra IT, mission e vision dell'organizzazione, in un'ottica di riduzione dei rischi per:

a) Raccogliere e razionalizzare le esigenze dei propri "Clienti Interni";
b) Contribuire all'analisi e alla definizione dei processi dell'organizzazione;
c) Contribuire alla definizione dei requisiti funzionali e architetturali degli strumenti informativi;
d) Contribuire alla gestione del cambiamento dovuto all'introduzione di nuovi strumenti informativi;
e) Definire e gestire il budget destinato ai Sistemi Informativi;
f) Definire degli standard metodologici e tecnologici di riferimento;
g) Organizzare e gestire il funzionamento quotidiano dei sistemi informativi, ottimizzando le risorse interne e gli appalti verso fornitori esterni;
h) Organizzare e gestire il flusso delle informazioni sulla base dell'esperienza agevolando l'uso della tecnologia nel complesso informativo;
i) Sviluppare e implementare nuove policy e procedure specifiche per Unità Operative e promuovere la conformità;
j) Gestire la conformità ai requisiti del modello di governance adottate dall'organizzazione;
k) Garantire la sicurezza dei sistemi informatici e la rete a cui sono collegati;
l) Fornire i nuovi dipendenti delle necessarie istruzioni/procedure rispetto alle mansioni svolte e agli strumenti utilizzati;
m) Mantenere la funzionalità dei sistemi informatici nelle varie aree;
n) Impedire l'accesso non autorizzato alle informazioni dell'organizzazione, file personali ed email.

Art. 8 - Fornitori di prodotti e servizi

I fornitori di prodotti e servizi dei Sistemi Informativi sono coloro che provvedono all'approvvigionamento di beni o alla prestazione di servizi all'organizzazione. In fase di appalto,

dichiarano di accettare le regole e le procedure del presente regolamento. In caso di outsourcing di un servizio relativo a un sistema oppure ad un applicativo, il personale tecnico è nominato Amministratore di Sistema dal titolare dell'azienda appaltatrice, che nello specifico svolge il ruolo di Responsabile (esterno) del trattamento ai sensi dell'art. 28 del GDPR. Almeno una volta l'anno, il titolare dell'azienda appaltatrice comunica al Direttore dei Sistemi Informativi l'elenco degli Amministratori di Sistema nominati e autorizzati a effettuare il servizio relativo all'appalto.

Art. 9 - Responsabile per la transizione digitale

Il Responsabile della Transizione al Digitale (RTD) è la figura all''interno della PA che ha tra le sue principali funzioni quella di garantire operativamente la trasformazione digitale dell'amministrazione, coordinandola nello sviluppo dei servizi pubblici digitali e nell'adozione di nuovi modelli di relazione trasparenti e aperti con i cittadini.

All'ufficio del RTD sono attribuiti i compiti di:

i. Coordinamento strategico dello sviluppo dei sistemi informativi di telecomunicazione e fonia;
ii. Indirizzo e coordinamento dello sviluppo dei servizi, sia interni sia esterni, forniti dai sistemi informativi di telecomunicazione e fonia dell'amministrazione;
iii. Indirizzo, pianificazione, coordinamento e monitoraggio della sicurezza informatica relativamente ai dati, ai sistemi e alle infrastrutture anche in relazione al sistema pubblico di connettività;
iv. Accesso dei soggetti disabili agli strumenti informatici e promozione dell'accessibilità;
v. Analisi periodica della coerenza tra l'organizzazione dell'amministrazione e l'utilizzo delle tecnologie dell'informazione e della comunicazione, al fine di migliorare la soddisfazione dell'utenza e la qualità dei servizi nonché di ridurre i tempi e i costi dell'azione amministrativa;
vi. Cooperazione alla revisione della riorganizzazione dell'amministrazione;
vii. Indirizzo, coordinamento e monitoraggio della pianificazione prevista per lo sviluppo e la gestione dei sistemi informativi di telecomunicazione e fonia;
viii. Progettazione e coordinamento delle iniziative rilevanti ai fini di una più efficace erogazione di servizi in rete a cittadini e imprese mediante gli strumenti della cooperazione applicativa tra pubbliche amministrazioni, inclusa la predisposizione e l'attuazione di accordi di servizio tra amministrazioni per la realizzazione e compartecipazione dei sistemi informativi cooperativi;

ix. Promozione delle iniziative attinenti all'attuazione delle direttive impartite dal Presidente del Consiglio dei ministri o dal Ministro delegato per l'innovazione e le tecnologie;

x. Pianificazione e coordinamento del processo di diffusione, all'interno dell'amministrazione, dei sistemi di identità e domicilio digitale, posta elettronica, protocollo informatico, firma digitale o firma elettronica qualificata e mandato informatico, e delle norme in materia di accessibilità e fruibilità nonché del processo di integrazione e interoperabilità tra i sistemi e servizi dell'amministrazione;

xi. Pianificazione e coordinamento degli acquisti di soluzioni e sistemi informatici, telematici e di telecomunicazione, al fine di garantirne la compatibilità con gli obiettivi di attuazione dell'agenda digitale ed in particolare, con quelli stabiliti nel piano triennale.

CAPO III – Strumenti

Art. 10 - Utilizzo del personal computer

Il personal computer affidato all'Utente è uno strumento di lavoro. Ogni utilizzo non inerente all'attività lavorativa è vietato perché può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. Il Pc deve essere custodito con cura evitando ogni possibile forma di danneggiamento.
Il personal computer dato in affidamento all'Utente permette l'accesso alla rete informatica solo attraverso specifiche credenziali di accesso ed autenticazione.
Il Responsabile dei sistemi informativi è autorizzato a compiere interventi nel sistema informatico, diretti a garantire la sicurezza e la salvaguardia del sistema stesso, nonché per ulteriori motivi tecnici e/o manutentivi. Detti interventi 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. 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 od impedimento del dipendente.
Ha la facoltà di collegarsi, previa autorizzazione dell'Utente, 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 e malware in genere. 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 formale comunicazione della necessità dell'intervento stesso.
Il personal computer viene fornito con configurazione software predefinita che non può essere per alcun motivo modificata da parte dell'utente. Le richieste di installazione di nuovo software o di modifica della configurazione devono essere richieste al **Responsabile dei sistemi informativi dell'Ente** che provvederà ad effettuarle. L'utente non può modificare le impostazioni del Pc autonomamente.

Di conseguenza:

- non verranno forniti privilegi di "amministratore";

- non è consentita l'installazione di mezzi di comunicazione personali (come ad esempio modem e dispositivi bluetooth, smartphone, chiavette per l'accesso ad internet etc.);
- non è consentito utilizzare strumenti software e/o hardware atti a intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici;
- non è consentito copiare sul proprio computer file contenuti in supporti magnetici, ottici e dispositivi usb non aventi alcuna attinenza con la propria prestazione lavorativa;
- il 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;
- qualora ci si allontani dalla propria postazione, occorre spegnere o "bloccare" il computer o disconnettersi (per il sistema operativo windows premendo contemporaneamente i tasti Alt+Ctrl+Canc e cliccando su blocca computer o in alternativa attivando la protezione sul proprio screensaver); 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;
- non è consentito utilizzare strumenti potenzialmente in grado di consentire accessi non autorizzati alle risorse informatiche;
- non è consentito configurare o utilizzare servizi diversi da quelli messi a disposizione da parte dell'Ente (quali DNS, DHCP, server internet Web, FTP,…);
- non è consentito intercettare pacchetti sulla rete (sniffer) o software dedicati a carpire, in maniera invisibile, dati personali, password e ID dell'utente oppure a controllare ogni attività, ivi inclusa la corrispondenza e i dati personali;
- non è consentito impostare password nel bios;
- non è consentito disassemblare il computer, asportare qualsiasi apparecchiatura in dotazione all'Utente;
- non è consentito avviare il personal computer con sistemi operativi diversi da quello installato dal personale tecnico specializzato per conto dell'Ente;
- non è consentito utilizzare connessioni in remoto per l'accesso alle risorse informatiche, al di fuori del perimetro dell'Ente e fatte salve le connessioni realizzate e autorizzate da parte del **Responsabile dei sistemi informativi dell'Ente**;
- salvo preventiva espressa formale autorizzazione del **Responsabile dei sistemi informativi dell'Ente,** non è consentito l'uso di programmi diversi da quelli ufficialmente installati dal personale tecnico per conto dell'Ente, 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'Ente 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 o comunque libero e quindi non protetto dal diritto d'autore, saranno sanzionate anche penalmente;

- non è consentito collegare alla rete informatica Personal Computer o Pc Portatili e, più in generale, qualsiasi dispositivo hardware senza la formale autorizzazione del **Responsabile dei sistemi informativi dell'Ente.**

Art. 11 - Hardware e Software

Tutto l'hardware ed il software potrà essere acquistato solo previa richiesta di parere tecnico favorevole da parte del **Responsabile dei sistemi informativi dell'Ente**, che controllerà le richieste di acquisto al fine di valutarne la compatibilità e programmare l'applicazione delle misure di sicurezza informatica.
A tal fine le richieste di acquisto dell'hardware e del software dovranno essere indirizzate al **Responsabile dei sistemi informativi dell'Ente** per la verifica tecnica di compatibilità o per la proposizione di soluzioni alternative. I supporti originali dei software acquistati e le relative licenze devono essere conservati presso il **Servizio CED dell'Ente**, così da consentire le operazioni di verifica della disponibilità di licenze e l'eventuale reinstallazione delle procedure.

Il personale non può utilizzare eventuale software di proprietà personale. Tutto ciò comprende anche le applicazioni regolarmente acquistate e registrate, programmi shareware e/o freeware, eventuale software scaricato da Internet o proveniente da CD/DVD allegati a riviste e/o giornali o altro software posseduto a qualsiasi titolo. Qualora fosse necessario per fini strettamente collegati all'attività lavorativa, l'utilizzo di software di proprietà personale, potrà essere installato solo previa richiesta di parere tecnico favorevole da parte del Responsabile dei sistemi informativi dell'Ente, che controllerà la compatibilità con le misure di sicurezza informatica dell'Ente.

Nell'ipotesi di utilizzo di software realizzato direttamente dall'utente finale potrà essere installato solo previa richiesta di parere tecnico favorevole da parte del Responsabile dei sistemi informativi dell'Ente, che controllerà la compatibilità con le misure di sicurezza informatica e qualora vengano trattati dati sensibili, darne comunicazione anche al Responsabile della Protezione dei Dati personali dell'Ente.

Il software per elaboratori è considerato opera di ingegno e come tale è tutelato dalle Leggi sul diritto di autore. L'utilizzo del software è regolamentato da licenze d'uso che devono essere assolutamente

rispettate da tutti. (Dlgs. 518/92 sulla tutela giuridica del software e L. 248/2000 “nuove norme di tutela del diritto d’autore”).
È vietato provare ad installare arbitrariamente il software scaricato da Internet o contenuto nei vari supporti distribuiti con le riviste, con i libri e con i quotidiani anche se si tratta di software allegato a riviste del settore. Prima di installare questi programmi, qualora l’uso fosse collegato ad esigenze lavorative, sarà necessario il benestare del **Responsabile dei sistemi informativi dell’Ente**.

Art. 12 - Computer portatili, tablet e smartphone

L' Utente è responsabile dell’integrità dei computer portatili, tablet e smartphone affidati dall’Ente e dei dati ivi contenuti. L’Utente è tenuto a custodirlo con diligenza sia durante l'utilizzo nel luogo di lavoro sia durante i suoi spostamenti. A tali dispositivi si applicano le regole di utilizzo previste per i personal computer. Nel caso di utilizzo condiviso con altri Utenti, prima della riconsegna occorre provvedere alla rimozione definitiva di eventuali file elaborati. I dischi rigidi, se contenenti dati sensibili, dovranno essere criptati al fine di evitare, in caso di furto o di smarrimento, l’accesso a dati riservati e/o personali da parte di soggetti non autorizzati. Tutti i dispositivi portatili dovranno essere resi noti al Responsabile dei sistemi informativi dell’Ente che provvederà all’applicazione di tutte le misure di sicurezza previste da disciplinare interno e dalla normativa vigente.

Art. 13 – Stampanti, Fotocopiatori, Scanner, Fax e Telefoni

Gli Strumenti di stampa, copia e scansione, così come anche il telefono dell’Ente, sono di proprietà del Comune di Trani e sono resi disponibili all’utente per rendere la prestazione lavorativa.
Pertanto ne viene concesso l’uso esclusivamente per tale fine.
Il telefono dell’Ente eventualmente affidato all’utente è uno strumento di lavoro. Ne viene concesso l’uso esclusivamente per lo svolgimento dell’attività lavorativa e non sono quindi consentite comunicazioni a carattere personale e/o non strettamente inerenti l’attività lavorativa stessa. La ricezione o l’effettuazione di comunicazioni a carattere personale è consentito solo nel caso di comprovata necessità ed urgenza.
Qualora venisse assegnato un cellulare dell’Ente all’utente, quest’ultimo sarà responsabile del suo utilizzo e della sua custodia. Ai cellulari e smartphone dell’Ente si applicano le medesime regole sopra previste per gli altri dispositivi informatici per quanto riguarda il mantenimento di un adeguato livello di sicurezza informatica. In particolare si raccomanda il rispetto delle regole per una corretta navigazione in Internet, se consentita.

Per gli smartphone dell'Ente è vietata l'installazione e l'utilizzo di applicazioni (o altresì denominate "app" nel contesto degli smartphone) diverse da quelle autorizzate dal Servizio CED dell'Ente.
È vietato l'utilizzo delle fotocopiatrici dell'Ente per fini personali, salvo preventiva ed esplicita autorizzazione da parte del Responsabile del Settore.
Per quanto concerne l'uso delle stampanti gli utenti sono tenuti a rammentare che la transizione al digitale prevede che tutta la documentazione debba essere trattata esclusivamente in formato elettronico. Pertanto la stampa è consentita principalmente per gli uffici aperta al pubblico. Di seguito le prescrizioni per l'utilizzo dei multifunzione:
- stampare documenti solo se strettamente necessari per lo svolgimento delle proprie funzioni operative;
- prediligere la stampa in bianco/nero e fronte/retro al fine di ridurre i costi.
Le stampanti e le fotocopiatrici dell'Ente devono essere spente ogni sera prima di lasciare gli uffici o in caso di inutilizzo prolungato.
Nel caso in cui si rendesse necessaria la stampa di informazioni riservate l'utente dovrà utilizzare i codici di stampa per evitare la possibile perdita o divulgazione di tali informazioni e persone terze non autorizzate.

Art. 14 - Credenziali di accesso

I sistemi di controllo degli accessi assolvono il compito di prevenire che persone non autorizzate possano accedere a un sistema informatico ed alle relative applicazioni.
Lo scopo è di cautelare l'Ente e i suoi dipendenti da ogni tipo di manomissione, furto o distruzione di dati oltre che di limitare l'accesso a specifici dati da parte di personale non autorizzato.
Le credenziali di autenticazione nell'intranet (accesso rete informatica), vengono inizialmente assegnate dal Responsabile dei sistemi informativi dell'Ente e successivamente obbligatoriamente reimpostate dal dipendente stesso secondo criteri prestabiliti dalla normativa vigente e con modalità operative di seguito meglio specificate. Non sono ammesse impostazioni autonome della password al Bios del computer onde evitare impedimenti all'accesso in caso di prolungata assenza o impedimento dell'incaricato e considerata la necessità di questo Ente di garantire in ogni caso la continuità dei servizi istituzionali.

Le credenziali di autenticazione per l'accesso alla rete e per l'utilizzo del servizio di posta elettronica istituzionale vengono assegnate dal personale del Servizio CED dell'Ente previa formale richiesta da

effettuarsi via protocollo dell'Ente, sottoscritta dal Dirigente Responsabile del Settore presso il quale l'Utente dovrà operare.

Le credenziali di autenticazione sono composte da un codice (account utente) facilmente riconducibile al soggetto e da una *password e/o PIN conosciuti al solo utilizzatore*. **È tassativamente vietato rivelare la propria password** di accesso alla rete, agli applicativi o servizi disponibili (inclusi i siti regionali o ministeriali), anche a terzi autorizzati. Qualsiasi azione effettuata utilizzando la coppia "account utente e passworde/o PIN" sarà attribuita in termini di responsabilità all'utente titolare registrato, a meno di comprovato illecito da parte di terzi.
La *lunghezza minima della password* deve essere di almeno 14 caratteri; considerato che i sistemi di violazione impiegano tempistiche esponenzialmente proporzionali con la lunghezza della password da violare, è necessario considerare almeno 14 caratteri per gli account dei servizi on-line (es. posta elettronica, piattaforme web) e per gli account qualificati amministrazione di sistema.
Le password non devono essere trascritte; per questo è importante che siano facili da ricordare. È consigliabile utilizzare tecniche di memorizzazione (es. Mi_P1@c3_l4_P1zz@).
È fondamentale utilizzare password diverse per scopi, piattaforme o applicativi diversi. L'eventuale violazione di un sistema potrebbe comportare effetti indesiderati anche su tutti gli altri sistemi utilizzati, dell'organizzazione e personali riconducibili allo stesso soggetto.
Le password devono essere modificate ad intervalli regolari per ridurre l'eventuale finestra temporale di esposizione e comunque almeno ogni 3 mesi (cd. *Password aging*).
Le password non devono mai far riferimento a termini di senso compiuto poiché già contenute nei dizionari utilizzati dai sistemi di violazione, oppure essere troppo ovvie (es. 'P@ssword').
Le password non devono essere in alcun modo collegate alla vita privata o lavorativa dell'utilizzatore. Sono quindi da escludere i nominativi dei familiari, la data di nascita, il codice identificativo, la targa dell'auto, la squadra del cuore, il soprannome, ecc. (il precedente elenco non è esaustivo).
Le password devono contenere combinazioni di caratteri maiuscoli, minuscoli, numeri e caratteri speciali (!, £, $, %, &, /, =, ?, §, @, #, …) anche quando non specificatamente richiesto dal sistema utilizzato (criteri di complessità).
Le password non devono essere riutilizzate a breve distanza di tempo; la rotazione minima prevista è almeno pari a 5 password diverse consecutive (cd. *Password history*);
Le password degli account di accesso ai sistemi non sottoposti alle politiche di complessità, di invecchiamento o di rotazione impostate nel sistema di autenticazione centrale, devono comunque rispettare le medesime regole, agendo manualmente.

Le password e i PIN non devono essere comunicate a nessuno, per nessun motivo, con nessun mezzo (ad esclusione del primo accesso o primo invio). In caso di problemi di accesso alle risorse fare riferimento al supporto tecnico.

La digitazione delle password deve avvenire in massima sicurezza evitando di mostrare a terzi la sequenza dei tasti premuti.

I colleghi impegnati in attività condivise al computer sono tenuti a voltarsi nel caso sia richiesta l'autenticazione al sistema o alla piattaforma software utilizzati.

È vietata la memorizzazione delle password nei browser o tramite applicativi di gestione password (es. Pocket Password) se non direttamente autorizzati/distribuiti dai Sistemi Informativi. Sono comunque esclusi sistemi o applicativi software di memorizzazione delle credenziali nel cloud.

Non utilizzare strumenti web per la generazione o il controllo del livello di sicurezza (utilizzare eventualmente password con costruzione simile al solo fine di verificarne la robustezza; es. https://password.kaspersky.com/it).

Per l'invio delle password di criptazione dei file e della documentazione non utilizzare mai lo stesso canale (es. file criptato inviato via posta elettronica e password comunicata a voce, via telefono).

Non seguire le mode del momento, utilizzare acronimi, pattern, ripetizioni e sequenze ('11111Paperin0000' oppure 'QWERTY12345') o parole presenti nei dizionari.

Nel caso di perdita (o anche solo il sospetto di perdita) della segretezza della password è necessario:

a) modificare immediatamente la password in uso (sui sistemi Windows CTRL+ALT+CANC e Cambia password; verificare le modalità per i singoli applicativi con autenticazione locale);
b) comunicare l'accaduto ai Sistemi Informativi dell'organizzazione, al proprio Responsabile e al DPO per la valutazione della gravità della situazione e l'attivazione delle procedure di emergenza per incidente alla sicurezza, al fine di attivare tutti i controlli e le contromisure del caso.

Nei casi di particolare emergenza oppure in presenza di comportamenti che possano comportare problemi di sicurezza, i Sistemi Informativi sono autorizzati alla momentanea disattivazione dell'account e del sistema utilizzato. Risolta la problematica evidenziata sarà cura dei Sistemi Informativi ripristinare le precedenti autorizzazioni.

Le richieste di cambiamento o reset password dell'account di accesso ai sistemi dell'organizzazione non sono mai inviate tramite e-mail. Eventuali e-mail che richiedano tramite link la modifica della password devono essere marcate come spam e cestinate.

È tassativamente vietato memorizzare account di accesso ai sistemi e servizi dell'organizzazione in documenti salvati in sistemi o dispositivi al di fuori del perimetro dell'organizzazione e ad accesso pubblico, inclusi sistemi di file hosting (come Google Drive, Dropbox, Wetransfer etc etc).

Gli account di amministrazione di dominio possono essere utilizzati soltanto nei client assegnati al personale dei Sistemi Informativi o posizionati nel data center; questo al fine di evitare problemi di registrazione delle password attraverso *keylogger* hardware o software.

Art. 15 - Utilizzo della rete e accessi da remoto

Per l'accesso alla Rete dell'Ente ciascun Utente deve essere in possesso delle specifiche credenziali descritte nell'art. 16.
È assolutamente vietato accedere alla rete informatica e/o nei programmi con un codice d'identificazione Utente di un altro operatore.
Si ricorda che tutti i dischi rigidi o altre unità di memorizzazione locali (es. dischi fissi interni o esterni al PC) non sono soggette a salvataggio da parte del personale incaricato **del Servizio CED dell'Ente**. La responsabilità del salvataggio dei dati ivi contenuti è pertanto a carico del singolo Utente.

Il personale tecnico del Servizio CED dell'Ente può in qualunque momento, senza preavviso, procedere alla rimozione dai computer in rete di ogni file e/o applicazione che riterrà essere pericolosi per la sicurezza dei dati e della rete.

Il Servizio CED dell'Ente si riserva la facoltà di negare o interrompere l'accesso alla rete informatica comunale mediante dispositivi non adeguatamente protetti e/o aggiornati, che possano costituire una concreta minaccia per la sicurezza informatica dell'Ente.

Non è consentito collegare alle prese di rete apparecchiature non autorizzate da parte del Responsabile dei sistemi informativi dell'Ente quali: hub, switch, access point o similari. Non è inoltre consentito installare o utilizzare qualsiasi altra apparecchiatura atta a gestire comunicazioni, salvo specifica autorizzazione rilasciata dal Responsabile dei sistemi informativi dell'Ente, quali a titolo esemplificativo: modem, router, Internet key.

I tecnici delle ditte esterne (fornitori applicativi, sistemisti etc.) dovranno richiedere l'autorizzazione del Responsabile dei sistemi informativi dell'Ente prima di collegarsi fisicamente alla rete informatica con dispositivi personali. Quest'ultimi saranno sottoposti alle politiche di sicurezza di questo Ente, al fine di garantire la sicurezza generale della rete informatica.
Gli accessi da remoto verso la rete informatica dell'Ente potranno essere effettuati solo previa autorizzazione del Responsabile dei sistemi informativi dell'Ente che rilascerà apposite credenziali per l'autenticazione sicura. Tutti gli accessi saranno monitorati e registrati. Non sono ammessi accessi di tipologia differente da quella VPN (Ipsec o SSL) gestita dal Responsabile dei sistemi informativi dell'Ente MFA. Ai fini della richiesta di autorizzazione all'accesso da remoto in VPN è necessario protocollare la richiesta da indirizzare al Responsabile dei sistemi informativi dell'Ente.

Art. 16 - Credenziali di accesso ai programmi gestionali

È possibile ottenere l'assegnazione di specifiche credenziali di autenticazione a programmi gestionali specifici, attraverso richiesta protocollata e sottoscritta dal Dirigente Responsabile del Settore presso il quale l'Utente dovrà operare indirizzare al Responsabile del Ced.
La richiesta dovrà essere compilato a cura del Dirigente Responsabile del Settore anche in caso di trasferimento del dipendente ad altro Settore o eventuale cessazione del rapporto di lavoro con l'Ente, per la conseguente comunicazione di disattivazione dei profili di accesso.

Art. 17 - Supporti rimovibili

Le porte USB, in ottemperanza alle policy adottate con le Misure Minime di Sicurezza, sono chiuse indistintamente a tutti gli utenti, salvo motivate ragione ai Dirigenti. Pertanto, eventuali supporti magnetici contenenti dati sensibili devono essere adeguatamente custoditi dall'Utente in armadi o cassetti chiudibili a chiave. È vietato l'utilizzo di supporti rimovibili personali (dischi rigidi e penne USB) compreso qualsiasi altro punto di memorizzazione tramite internet (c.d. "remote storage" quali Dropbox, GoogleDrive, OneDrive, etc.) nel caso si voglia trattare dati dell'Ente, personali, sensibili e/o giudiziari. In caso di trasferimento di dati sensibili tra computer in rete, si dovrà contattare il Responsabile del ced per l'attività di che trattasi.

Art. 18 - Posta elettronica convenzionale

Il servizio di posta elettronica è un mezzo istituzionale di comunicazione e il suo utilizzo deve avvenire nel rispetto delle norme in materia di protezione dei dati personali.
La casella di posta elettronica istituzionale assegnata all'Utente è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica istituzionale sono responsabili del corretto utilizzo delle stesse.
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 ordinaria e certificata per:

- l'invio e/o il ricevimento di allegati contenenti filmati o brani musicali (es. mp3) non legati all'attività lavorativa;
- l'invio e/o il ricevimento di messaggi personali o per la partecipazione a dibattiti, sondaggi e aste on-line;
- la partecipazione a catene di Sant'Antonio; non si dovrà in alcun caso procedere all'apertura degli allegati a tali messaggi.

La casella di posta elettronica deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti (in termini di centinaia di MB e, ancor più di GB). Il contenuto della mail deve essere mantenuto sotto i 5GB.
È obbligatorio porre la massima attenzione nell'aprire i file allegati alle e-mail prima del loro utilizzo.
In linea di massima non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti, altrimenti, se obbligati sottoporre necessariamente detti file ad una "scansione approfondita" dell'antivirus prima del loro utilizzo.

La posta elettronica è erogata esclusivamente in modalità web, con accesso tramite browser. Sono tassativamente escluse altre modalità considerate non sicure come client locali di posta elettronica (es. Outlook o Mozilla Thunderbird).
La posta elettronica ordinaria o e-mail secondo la recente giurisprudenza, rispetto a quanto previsto dal Regolamento (UE)2014/910 eIDAS (*electronicIDentification Authentication and Signature*) e dalle conseguenti modifiche al D.lgs. n. 82/2005 CAD (Codice dell'Amministrazione Digitale) ha validità giuridica e rilevanza probatoria, è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità.
Alla fine della sessione di lavoro è necessario effettuare sempre la disconnessione (Log out) dal sistema di posta.
I sistemi di sicurezza come firewall e antispam garantiscono con discreta probabilità che le e-mail consegnate siano esenti da pericoli. È sempre a carico dell'utilizzatore la verifica ultima di:

- **Mittente**: deve essere conosciuto (da verificare l'indirizzo effettivo e non la semplice denominazione); esempio da evitare e marcare come spam è il mittenteservice145@mail.145.com;
- **Link**: i link devono essere verificati prima di essere lanciati anche nel caso appaiano a prima vista del tutto familiari (soprattutto come aspetto grafico) al fine di evitare attacchi di tipo phishing; la verifica può essere fatta posizionando il cursore del mouse sul link per visualizzare la reale destinazione (ad esempio evitare di fare click su link del tipo http://amazon.net.ru);

- **Allegati**: diffidate dei file con estensione multipla o senza estensione o con denominazione estranea alle attività o mansioni svolte abitualmente (es. 'Si allega fattura');
- **Contenuti**: scrittura con errori grossolani (traduzione da sistemi automatici), riferimenti alla chiusura di un conto o di un servizio, parole come URGENTE, richieste di dati personali o di password, file che non sono mai stati richiesti o con estensioni sospette.

Nei casi dubbi non aprire le e-mail o i contenuti e contattare il supporto tecnico che provvederà alla verifica secondo le procedure di sicurezza.
È vietato il forward o rilancio della posta sui dispositivi mobili (es. smartphone e tablet) personali. Il forward dei messaggi è permesso solamente sui dispositivi mobili di proprietà dell'organizzazione, agli utilizzatori specificatamente autorizzati.
L'invio di file tramite link ai sistemi di hosting è permesso solo se i file sono criptati e le chiavi di criptazione sono condivise su altro media. Le procedure di criptazione sono disponibili nella intranet istituzionale.
Non consultare la posta elettronica dell'organizzazione presso Internet point, Wi-Fi pubblici o sistemi di connettività condivisa (es. alberghi, ristoranti, bar).
Marcare come spam le e-mail che appaiono come*scam* ovvero tentativi di truffa pianificata con metodi di ingegneria sociale (in genere nella e-mail si promettono enormi guadagni in cambio di somme di denaro da anticipare).
Le e-mail che richiedono l'attivazione delle macro di MS-Word o MS-Excel prima del download degli allegati devono essere immediatamente marcate come spam.
Non attivare mai i link presenti nelle cosiddette e-mail di reset della password, né fornire mai le credenziali di autenticazione per nessun motivo.
Gli allegati inviati via e-mail contenti dati personali o riservati devono essere criptati adottando le procedure e le modalità previste in questi casi. La password di decriptazione deve essere comunicata al destinatario con altro mezzo (es. via telefono).
La ricezione di eventuali messaggi che rappresentano istanze o dichiarazioni da parte di terzi, presentate nelle modalità, così come previste all'art. 65 del CAD (es. richiesta con allegata copia di un documento di identità), devono essere girate al sistema di protocollo per la dovuta procedura di registrazione e assegnazione. Tutto ciò che costituisce patrimonio informativo dell'Ente non può risiedere nella casella di posta elettronica ordinaria ma va protocollato e fascicolato come previsto dal manuale di gestione documentale.

L'Utente assegnatario della casella di posta elettronica istituzionale è il diretto responsabile del corretto utilizzo della stessa e risponde personalmente dei contenuti trasmessi. In particolare l'Utente è tenuto a rispettare quanto segue:

- non utilizzare il servizio per scopi illegali o non conformi al presente Regolamento o in maniera tale da recar danno o pregiudizio all'Ente o a terzi;
- non utilizzare il servizio in modo da danneggiare, disattivare, sovraccaricare, pregiudicare o interferire con la fruibilità del servizio da parte degli altri utenti;
- non utilizzare la posta elettronica per inviare, anche tramite collegamenti o allegati in qualsiasi formato (testo, fotografico, video, grafico, audio, codice, ecc.), messaggi che contengano o rimandino ad esempio a: pubblicità non istituzionale, manifesta o occulta.

In nessun caso l'Utente potrà utilizzare la posta elettronica per diffondere codici dannosi per i computer quali virus e simili.
Di seguito si elencano alcune norme di comportamento che ciascun Utente è tenuto ad osservare al fine di preservare l'efficienza del servizio di posta elettronica e delle comunicazioni con esso veicolate:

- l'Utente è tenuto a visionare regolarmente la casella di posta elettronica di propria competenza;
- i messaggi devono essere preferibilmente di solo testo, evitando ove possibile ogni formattazione e inserzione di immagini;
- è buona norma inviare messaggi sintetici che descrivano in modo chiaro il contenuto;
- è necessario indicare sempre chiaramente l'oggetto, in modo tale che il destinatario possa immediatamente individuare l'argomento del messaggio ricevuto, facilitandone la successiva ricerca per parola chiave;
- non superare la dimensione complessiva di 10 Megabyte degli allegati inviati con un singolo messaggio;
- limitare l'invio di messaggi di posta elettronica a indirizzi plurimi (decine di destinatari) e trasmetterli solo in casi motivati da esigenze di servizio.

L'Utente, infine, si impegna a non inviare messaggi di natura ripetitiva (*c.d.* catene di Sant' Antonio) anche quando il contenuto sia volto a segnalare presunti o veri allarmi (esempio: segnalazioni di virus).
In caso di assenza prolungata programmata del dipendente, si consiglia e si raccomanda al dipendente di attivare il sistema di risposta automatica ai messaggi di posta elettronica ricevuti indicando, nel messaggio di accompagnamento, le coordinate di un collega o della struttura di riferimento che può

essere contattata in sua assenza e/o altre modalità utili di contatto del Settore/Servizio presso cui presta la propria attività lavorativa.

Nell'ipotesi di assenza o impossibilità, temporanea o protratta nel tempo, del dipendente, qualora per ragioni di sicurezza o comunque per garantire l'ordinaria operatività istituzionale sia necessario accedere a informazioni o documenti di lavoro presenti sul personal computer del dipendente, inclusi i messaggi di posta elettronica in entrata ed in uscita, il dipendente può delegare un altro dipendente a sua scelta (fiduciario) il compito di verificare il contenuto di messaggi e inoltrare al responsabile del Settore in cui lavora, quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa.

Di tale attività deve essere redatto apposito verbale e informato il dipendente interessato alla prima occasione utile. In caso di assenza o impossibilità, temporanea o protratta nel tempo, del dipendente, qualora per ragioni di sicurezza o comunque per garantire l'ordinaria operatività istituzionale sia necessario accedere a informazioni o documenti di lavoro presenti sul personal computer del dipendente, inclusi i messaggi di posta elettronica in entrata e in uscita, e il dipendente non abbia delegato un altro dipendente (fiduciario), secondo quanto sopra specificato, il responsabile del Settore cui afferisce il dipendente può chiedere al Responsabile dei sistemi informativi dell'Ente di accedere alla postazione e/o alla casella di posta elettronica istituzionale del dipendente assente mediante apposita istanza protocollata in cui si evinca la richiesta.

Sarà onere del Responsabile del Settore informare celermente il dipendente al suo rientro, fornendo adeguata spiegazione e redigendo apposito verbale.

Le caselle di posta elettronica istituzionale nominative hanno validità pari alla durata della permanenza in servizio del dipendente, fatte salve eventuali situazioni di congedo, distacco e comando. Nel caso in cui il dipendente non presti più la sua attività lavorativa presso questo Ente, la casella di posta elettronica sarà prontamente disattivata, cancellata e il contenuto distrutto.

Art. 19 - Posta Elettronica Certificata (PEC)

La Posta Elettronica Certificata (PEC) è un sistema di posta elettronica nel quale è fornita al mittente documentazione elettronica attestante l'invio e la consegna di documenti informatici, ed è garantita la tracciabilità della casella mittente; il circuito è certamente più sicuro della posta elettronica convenzionale ma non è esente da rischi. Per questo motivo valgono le stesse regole e indicazioni fornite per la posta elettronica convenzionale.
L'invio tramite PEC di documentazione riservata o contenente dati personali particolari deve avvenire sempre attraverso allegati criptati con comunicazione delle chiavi attraverso altro media.
La gestione/invio/ricezione delle PEC di enti è consentita esclusivamente attraverso il software gestione del protocollo informatico, al fine di garantire la corretta archiviazione sostitutiva, profilazione degli accessi da parte del personale. Eventuali eccezioni nella gestione dovranno essere indicati nel manuale di gestione di gestione documentale.

Art. 20 – Firma Elettronica

Le Firme Elettroniche, ai sensi del Regolamento UE n. 910/2014 (eIDAS, Electronic IDentification Authentication and Signature) e del CAD possono essere di 4 tipi:

Tipologia Firma	Definizione	Esempi	Valore Probatorio
Elettronica semplice [art. 3, comma 10 eIDAS]	Dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare	Messaggio di posta elettronica ordinaria o una Sottoscrizione (scansione firma apposta al Documento) che non ha tutti i requisiti delle altre Sottoscrizioni elettroniche di livello superiore	Liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità (art.21 del CAD)
Avanzata [art. 3, comma 11 eIDAS] [Requisiti previsti all'art 26 eIDAS]	a)è connessa unicamente al firmatario; b) è idonea a identificare il firmatario; c) è creata mediante dati per la creazione di una firma elettronica che il firmatario può, con un elevato livello di sicurezza, utilizzare sotto il proprio	Firma grafometrica utilizzata su tablet in molti contesti tra i quali le banche e le assicurazioni	Garantisce l'identità dell'autore, l'integrità e l'immodificabilità del documento, ha l'efficacia prevista dall'art. 2702 del Codice civile. L'utilizzo del dispositivo di firma qualificata o digitale si presume riconducibile al titolare, salvo che questi dia prova contraria

	esclusivo controllo; d) è collegata ai dati sottoscritti in modo da consentire l'identificazione di ogni successiva modifica di tali dati.		
Qualificata [art. 3, comma 12 eIDAS]	Firma elettronica avanzata creata da un dispositivo per la creazione di una firma elettronica qualificata e basata su un certificato qualificato per firme elettroniche	Smart card, Token (sicurezza)	Garantisce l'identità dell'autore, l'integrità e l'immodificabilità del documento, ha l'efficacia prevista dall'art. 2702 del Codice civile. L'utilizzo del dispositivo di firma qualificata o digitale si presume riconducibile al titolare, salvo che questi dia prova contraria.
Digitale [art. 24 CAD]	Particolare tipo di firma qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare di firma elettronica tramite la chiave privata e a un soggetto terzo tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici	Smart card, Token (sicurezza), Firma digitale remota.	Garantisce l'identità dell'autore, l'integrità e l'immodificabilità del documento, ha l'efficacia prevista dall'art. 2702 del Codice civile. L'utilizzo del dispositivo di firma qualificata o digitale si presume riconducibile al titolare, salvo che questi dia prova contraria.

L'utilizzatore dotato di strumenti di firma è responsabile della conservazione in sicurezza di tutte le componenti (hardware come la Smart card, PIN e Password). La perdita degli strumenti di firma o il semplice sospetto della perdita di segretezza della password o del PIN, deve essere immediatamente comunicata al supporto tecnico dei Sistemi Informativi.

È fondamentale conservare separati i dispositivi di firma (Smart card) dal PIN e dalla password (è preferibile provare a ricordare, senza dover trascrivere le credenziali).
La firma di atti o documenti dell'organizzazione è responsabilità diretta dell'intestatario della firma elettronica (di qualsiasi tipologia sopra riportata). È vietato firmare per conto di altri soggetti anche nel caso di autorizzazione verbale o scritta; sono escluse dal divieto le sole firme cosiddette automatiche (es. attraverso il sistema SDI).
I documenti firmati digitalmente, per definizione, non sono ripudiabili a meno di querela di parte.
È possibile firmare atti o documenti dell'organizzazione solo se in formato PDF, PDF/A (progettato per la conservazione dei documenti amministrativi) o XML. Gli altri formati sono vietati, a meno di specifica autorizzazione.
Le tipologie di firme accettate sono P7M (CAeDES) e PDF (PAeDES). Altri formati non sono accettati.
Il rinnovo dei certificati di prossima scadenza è in carico al fornitore del servizio di firma.
L'aggiornamento dei certificati del software di verifica delle firme è a carico del singolo utilizzatore. Le regole per la sicurezza delle password riportate nel presente regolamento sono valide anche nella definizione della password e PIN/PUK di firma.
Nel caso il software di verifica delle firme segnali delle anomalie è necessario:
a. Verificare che la lista delle Certification Authority(CA) sia aggiornata;
b. Verificare il firmatario;
c. Eventualmente richiedere di nuovo il documento firmato al firmatario.
La conservazione sostitutiva dei documenti firmati digitalmente segue quanto previsto dalla regolamentazione in materia. Si faccia riferimento alla specifica documentazione a cura del Responsabile della conservazione e della transizione al digitale.
La documentazione firmata deve seguire un percorso di archiviazione in base al Regolamento dell'organizzazione in materia, a cura del responsabile della conservazione.

Art. 21 - Navigazione internet

Il Personal computer assegnato all'Utente ed abilitato alla navigazione in Internet costituisce uno strumento 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, all'interno dell'Ente.

In questo senso, a titolo puramente esemplificativo, l'Utente non potrà utilizzare Internet per:

- l'upload o il download di software gratuiti se non espressamente autorizzati dal Responsabile dei sistemi informativi dell'Ente ;
- l'utilizzo di documenti (filmati e musica) provenienti da siti web o http, se non strettamente attinenti all'attività lavorativa;
- l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, fatti salvi i casi autorizzati e comunque nel rispetto delle normali procedure di acquisto;
- ogni forma di registrazione a siti i cui contenuti non siano strettamente legati all'attività lavorativa;
- la partecipazione a forum non professionali, a giochi on-line, l'utilizzo di chat line, di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames).

Al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa, l'Ente con logica preventiva, adotta uno specifico sistema di filtro automatico che impedisce determinate operazioni quali l'upload, download (illeciti o illegali) o l'accesso a determinati siti ludici (black-list). I filtri sopracitati limitano l'accesso ai siti Internet che presentano i seguenti contenuti: illegali o non etici, stupefacenti, razzismo e odio, estremismo, violenza, occultismo, plagio; materiale per adulti, nudità, pornografia; giochi, scommesse, intermediazione e trading, download software freeware; social network, radio e tv via Internet; peer to peer; malware, spyware, hacking, proxy anonimi, bypass proxy, phishing, file hosting, remote control.

Qualsiasi altra tipologia di contenuti o siti che il Dirigente o il Responsabile dei sistemi informativi dell'Ente riterrà di non dover rendere accessibile dalla rete informatica, verrà preventivamente comunicata agli utenti.
I file contenenti le registrazioni della navigazione sul web sono conservati per il tempo strettamente necessario, determinato dalle norme in vigore e da esigenze di sicurezza.

Si informa che l'Ente, per il tramite del Servizio CED, non effettua la memorizzazione sistematica delle pagine web visualizzate dal singolo Utente, né controlla con sistemi automatici i dati di navigazione dello stesso.
Si informa tuttavia che al fine di garantire il Servizio Internet e la sicurezza dei sistemi informativi, nonché per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del

patrimonio dell'Ente, il Comune di Trani registra i dati di navigazione (file di log riferiti al traffico web) con modalità inizialmente volte a precludere l'immediata e diretta identificazione di Utenti, mediante opportune aggregazioni. Solo in casi eccezionali e di comprovata urgenza rispetto alle finalità sopra descritte, l'Ente può trattare i dati di navigazione riferendoli specificatamente ad un singolo nome utente.

Gli eventuali controlli per motivi di sicurezza informatica, compiuti dal personale tecnico **del Servizio CED dell'Ente**, potranno avvenire mediante un sistema di controllo dinamico dei contenuti o mediante "file di log" della navigazione svolta. Il controllo sui log, i quali sono cancellati periodicamente ed automaticamente, non è sistematico e le informazioni vengono conservate temporaneamente per finalità di sicurezza di questo Ente. Il prolungamento dei tempi di conservazione dei log potrà aver luogo solo nei seguenti casi:

- esigenze tecniche o di sicurezza del tutto particolari;
- indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;
- su specifica richiesta dell'autorità giudiziaria.

Art. 22 - Protezione da virus

Le postazioni di lavoro collegate alla rete informatica dell'Ente sono protette da uno stesso software antivirus che viene aggiornato automaticamente grazie ad una gestione centralizzata per mezzo di soluzione in cloud centralizzata antivirus. **Non è ammesso l'utilizzo di sistemi antivirus differenti da quello fornito dall'Ente.**

Ogni Utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico. Questa fattispecie può accadere mediante virus o malware, proveniente da dati e/o software importati/installati dall'Utente, che si auto-installano, all'insaputa dell'Utente, all'interno del Pc, infettandolo e diffondendosi nella rete informatica dell'Ente.

Nel caso in cui il software antivirus rilevi e non disinfetti la presenza di un virus, l'Utente dovrà immediatamente sospendere ogni elaborazione in corso e segnalare l'accaduto al personale tecnico utorizzato **del Servizio CED dell'Ente.**

Ogni dispositivo di memorizzazione esterna dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, dovrà essere prontamente consegnato al personale tecnico autorizzato che provvederà ad effettuare le dovute operazioni di disinfezione.

Art. 23 - Salvataggio dati

Ogni Utente è responsabile della corretta conservazione dei dati e dei documenti elettronici che utilizza sul Pc per motivi lavorativi, di qualsiasi tipo, formato e natura essi siano. Per questo motivo la tutela della gestione dei dati sulle postazioni di lavoro (Personal computer e Pc portatili) è demandata all'Utente finale.
Costituisce buona regola la pulizia periodica (almeno ogni mese) 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.

Art. 24 Tele-assistenza

Per lo svolgimento di normali attività di assistenza e manutenzione su personal computer connessi alla rete, il personale tecnico **del Servizio CED dell'Ente** potrà utilizzare specifici software di connessione remota. Tali programmi sono utilizzati per assistere l'Utente al fine di effettuare interventi di assistenza informatica e di manutenzione su applicativi e hardware in uso. L'attività di assistenza e manutenzione avviene previa autorizzazione da parte dell'Utente e mediante visualizzazione di un indicatore visivo sul monitor che segnala la connessione in remoto del tecnico informatico.
Gli Amministratori di Sistema esterni e il responsabile dei sistemi informativi possono accedere ai dispositivi informatici dell'Ente sia direttamente, sia mediante software sicuro di accesso remoto, per i seguenti scopi:

- verifica e risoluzione di problemi sistemistici ed applicativi, su segnalazione dell'utente finale;
- verifica del corretto funzionamento dei singoli dispositivi in caso di problemi rilevati nella rete;
- richieste di aggiornamento software e manutenzione preventiva hardware e software.

Gli interventi tecnici posso avvenire previo consenso dell'utente, quando l'intervento stesso richiede l'accesso ad aree personali dell'utente stesso. Qualora l'intervento tecnico in loco o in remoto non necessiti di accedere mediante credenziali utente, gli Amministratori di sistema esterni e il responsabile dei sistemi informativi sono autorizzati ad effettuare gli interventi senza il consenso dell'utente cui la risorsa è assegnata.

L'accesso in teleassistenza sui computer della rete informatica dell'Ente richiesto da terzi (fornitori e consulenti) deve essere autorizzato dal Responsabile dei sistemi informativi, per le verifiche delle modalità di intervento per il primo accesso. Le richieste successive, se effettuate con la medesima modalità, possono essere gestite autonomamente dall'utente finale.

Art. 25 - Cloud computing e servizi IT esterni

L'acquisizione di servizi basati su tecnologia cloud come IaaS, PaaS e SaaS devono essere conformi alla normativa nazionale e alle Politiche di approvvigionamento che prevedono per servizitecnologici l'autorizzazione da parte dei Sistemi Informativi dell'organizzazione.
L'utilizzo di sistemi basati su tecnologia cloud o web non autorizzati e tracciati è considerato un data breach con tutti i risvolti sanzionatori ed eventualmente risarcitori a carico dell'utilizzatore.
Ai sensi di quanto previsto dalle Circolari 2 e 3 2018 di AgID non è possibile acquisire servizi in modalità SaaS se non qualificati dalla stessa AgID e pubblicati nel rispettivo Marketplace ACN.

Art. 26 - Monitoraggio

Il Responsabile dei sistemi informativi dell'Ente effettuerà monitoraggi periodici su dati anonimi allo scopo di verificare l'attuazione del presente Disciplinare, i possibili rischi alla sicurezza informatica e le possibili problematiche inerenti l'utilizzo degli strumenti informatici.

Questi monitoraggi si possono classificare in:

- analisi del traffico di rete: effettuati attraverso specifici log dei dispositivi di rete;
- analisi del traffico Internet: effettuati attraverso specifici log dei dispositivi di connessione ad Internet;
- inventario Hardware e Software: effettuati attraverso procedure prevalentemente automatiche per le apparecchiature collegate in rete e in maniera semiautomatica per le macchine non appartenenti al dominio.

Il monitoraggio delle risorse hardware e software non coinvolge in alcun modo i dati personali e i documenti presenti sulle singole postazioni di lavoro e viene effettuato per finalità organizzative e gestionali.

I dati del traffico telematico verranno gestiti secondo le modalità e le tempistiche previste dalla normativa vigente in materia di sicurezza dei dati del traffico telefonico e telematico.

Art. 27 – Controlli

L'Ente si riserva di effettuare controlli per verificare il rispetto del presente Disciplinare che costituisce preventiva e completa informativa nei confronti dei dipendenti.
In base al principio di correttezza, l'eventuale trattamento deve essere ispirato ad un canone di trasparenza, come prevede anche la disciplina di settore.

I controlli sono effettuati nel rispetto dei seguenti principi:

- **Proporzionalità**: il controllo e l'estensione dello stesso dovrà rivestire, in ogni caso, un carattere adeguato, pertinente e non eccessivo rispetto alla/alle finalità perseguite, ma resterà sempre entro i limiti minimi;
- **Trasparenza**: l'adozione del presente Disciplinare ha l'obiettivo di informare gli utenti sui diritti ed i doveri di entrambe le parti;
- **Pertinenza e non eccedenza**: ovvero evitando un'interferenza ingiustificata sui diritti e sulle libertà fondamentali dei lavoratori, così come la possibilità di controlli prolungati, costanti o indiscriminati.

Nel caso in cui emerga un evento dannoso, una situazione di pericolo o utilizzi non aderenti al presente Disciplinare, che non siano stati impediti con preventivi accorgimenti tecnici o rilevati durante i monitoraggi o da attività di gestione degli strumenti informatici il Responsabile dei sistemi informativi dell'Ente potrà adottare le eventuali misure che consentano la verifica di tali comportamenti preferendo, per quanto possibile, un controllo preliminare su dati aggregati riferiti all'intero Settore o a sue articolazioni.
Il controllo su dati anonimi si concluderà con una comunicazione al Responsabile del Settore analizzato che si preoccuperà di inviare un avviso generalizzato relativo a un utilizzo non corretto degli strumenti informatici, invitando i destinatari ad attenersi scrupolosamente al presente Disciplinare.
Qualora le anomalie e irregolarità dovessero persistere, si procederà circoscrivendo l'invito al personale afferente al Settore in cui è stata rilevata l'anomalia.
In caso di reiterate anomalie o irregolarità, saranno effettuati controlli su base individuale.
In nessun caso, a eccezione di specifica richiesta da parte dell'Autorità Giudiziaria, verranno poste in essere azioni sistematiche quali:

- la lettura e la registrazione dei messaggi di posta elettronica (al di là di quanto tecnicamente necessario per lo svolgimento del servizio di gestione e manutenzione della posta elettronica);
- la riproduzione ed eventuale memorizzazione delle pagine web visualizzate dal lavoratore;
- la memorizzazione di quanto visualizzato sul monitor.

Oltre a ciò l'Ente si riserva di effettuare specifici controlli sui software caricati sui personal computer utilizzati dai dipendenti al fine di verificarne la regolarità sotto il profilo delle autorizzazioni e delle licenze, nonché, in generale, la conformità degli stessi alla normativa vigente e, in particolare, alle disposizioni in materia di proprietà intellettuale.
Oltre a tali controlli di carattere generale, questo Ente si riserva comunque le facoltà previste dalla normativa vigente di effettuare specifici controlli ad hoc nel caso di segnalazioni di attività che hanno causato danno all'Ente, che ledono diritti di terzi o che, comunque, sono illegittime.

Qualora risulti necessario l'accesso alle risorse informatiche e relative informazioni su risorse informatiche di un Utente (quali file salvati, posta elettronica, pec etc..) che non sia reperibile, in quanto ad esempio assente, temporaneamente irreperibile ovvero cessato, il Responsabile del Settore, per il tramite del Servizio CED dell'Ente, si atterrà alla procedura descritta qui di seguito:
a. Redazione di un atto da parte del Responsabile del Settore che comprovi le necessità produttive e di organizzazione che richiedano l'accesso allo Strumento;
b. Incarico al responsabile dei sistemi informativi di accedere alla risorsa con credenziali di Amministratore ovvero tramite l'azzeramento e la contestuale creazione di nuove credenziali di autenticazione dell'Utente interessato, con avviso che al primo accesso alla risorsa, lo stesso dovrà inserire nuove credenziali;
c. Redazione di un verbale che riassuma i passaggi precedenti;
d. In ogni caso l'accesso ai documenti presenti nella risorsa è limitato a quanto strettamente indispensabile alle finalità produttive e di organizzazione del lavoro;
e. Qualora indirettamente si riscontrino file o informazioni anche personali, esse potranno essere altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, considerato che il presente Regolamento costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli, sempre nel rispetto di quanto disposto dal Regolamento Europeo 2016/679.

Art. 28 - Conservazione dei dati

In applicazione ai principi di diritto di accesso, legittimità, proporzionalità, sicurezza ed accuratezza e conservazione dei dati, le informazioni relative all'accesso ad Internet e dal traffico telematico (log di sistema e del server proxy), la cui conservazione non sia necessaria, saranno cancellati entro i termini indicati nel presente Regolamento, comunque per un massimo di 12 mesi, salvo esigenze ulteriori tecniche o di sicurezza; o per l'indispensabilità dei dati rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria o, infine, all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria.

Art. 29 - Social Media

L' eventuale utilizzo a fini promozionali di Facebook, Twitter, LinkedIn, Whatsapp, dei blog e dei forum, anche professionali (ed altri siti o social media) è gestito ed organizzato esclusivamente dall'Ente attraverso specifiche direttive ed istruzioni operative al personale a ciò espressamente addetto, rimanendo escluse iniziative individuali da parte dei singoli utenti o collaboratori.
Fermo restando il diritto della persona alla libertà di espressione, l'Ente ritiene comunque opportuno indicare agli utenti alcune regole comportamentali, al fine di tutelare tanto la propria immagine ed il patrimonio dell'Ente, anche immateriale, quanto i propri dipendenti, i propri fornitori oltre che gli stessi cittadini utilizzatori dei social media, fermo restando che è vietata la partecipazione agli stessi social media durante l'orario di lavoro.
Il presente articolo deve essere osservato dall'Utente sia che utilizzi dispositivi messi a disposizione dall'Ente, sia che utilizzi propri dispositivi, sia che partecipi ai social media a titolo personale, sia che lo faccia per finalità professionali, come dipendente dell'Ente.
La condivisione dei contenuti nei social media deve sempre rispettare e garantire la segretezza sulle informazioni dell'Ente, nel rispetto del segreto d'ufficio, segreto professionale e della protezione dei dati.
È vietato l'utilizzo di strumenti di condivisione, quali whatsapp, Telegram etc.. per la trasmissione tra colleghi di documenti istituzionali attraverso dispositivi di proprietà personale. Infatti detti strumenti non sono in alcun modo idonei alla formazione e trasmissione dei documenti informatici dell'Ente ex DLgs. 82/2005.

Art. 30 - Sanzioni

È fatto obbligo a tutti i dipendenti ed utenti del sistema informativo/informatico dell'Ente di osservare le disposizioni portate a conoscenza con il presente Disciplinare. Il mancato rispetto o la violazione delle regole sopra ricordate è perseguibile con provvedimenti disciplinari e/o risarcitori previsti dalla vigente normativa, nonché con tutte le azioni civili e penali consentite.

Art. 31 - Aggiornamento e revisione

Il presente Disciplinare è stato redatto tenendo conto del Regolamento UE 2016/679, del Codice in materia di protezione dei dati personali, delle Linee guida dell'Autorità Garante per la protezione dei dati personali, emanate con delibera n. 13 del 1° marzo 2007 e della Direttiva n.2/2009 del Ministro per la Pubblica Amministrazione e Innovazione.
Il presente Disciplinare è soggetto a revisione come per Legge o qualora se ne ravveda la necessità.

Copia del presente documento verrà consegnata a ciascun dipendente ovvero messo a disposizione per ogni Utente autorizzato all'utilizzo della rete informatica dell'Ente.

Con l'entrata in vigore del presente Disciplinare tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi sostituite dalle presenti.

Città di Trani

Medaglia d'Argento al Merito Civile

Provincia Barletta Andria Trani

DELIBERAZIONE DELLA GIUNTA COMUNALE N° 93 del 02/10/2025

OGGETTO: APPROVAZIONE AGGIORNAMENTO REGOLAMENTO IT DEL COMUNE DI TRANI

L'anno 2025 il giorno 02 del mese di Ottobre alle ore 17:00, nella sala delle adunanze del Comune di Trani, appositamente convocata, si è riunita la Giunta Comunale. Alla seduta risultano presenti:

N°	Nome	Qualifica	Presente	Assente
1	BOTTARO AMEDEO	Sindaco		X
2	FERRANTE FABRIZIO	Assessore	X	
3	LAURORA CARLO	Assessore	X	
4	LIGNOLA LUCA	Assessore	X	
5	DI LERNIA CECILIA	Assessore		X
6	RONDINONE ALESSANDRA	Assessore		X
7	VALENTE PAOLA	Assessore		X
8	CAPONE ALESSANDRO	Assessore	X	
9	DI LERNIA COSIMO DAMIANO	Assessore	X	
10	DE MARI LUCIA	Assessore	X	

PRESENTI: 6 ASSENTI: 4

Con l'assistenza del Il Segretario Dott. Francesco Angelo Lazzaro

Il Vice Sindaco Ferrante Fabrizio, constatato il numero legale degli intervenuti e la regolarità della seduta dichiara aperta la seduta e invita la Giunta Comunale a trattare l'argomento in oggetto sulla cui proposta sono stati acquisiti i prescritti pareri ai sensi del TUEL riportati in allegato al presente verbale quale parte integrante e sostanziale.

LA GIUNTA COMUNALE

Acquisita la proposta di deliberazione predisposta dal Dirigente proponente, all'esito dell'istruttoria dallo stesso condotta, con il supporto delle articolazioni amministrative di riferimento e previa verifica della regolarità tecnico amministrativa ai sensi dell'articolo 147 bis, comma 1, del d.lgs. 18 agosto 2000, n. 267, come da parere reso ai sensi dell'articolo 49, del d. lgs. 18 agosto 2000, n. 267, e preso atto dei fatti e delle circostanze, nonché dei contenuti dei riferimenti documentali, come dal Dirigente stesso rappresentati.

PREMESSO che:

- con Deliberazione di Giunta Comunale n. 46 del 23.05.2025 avente ad oggetto: "APPROVAZIONE DEL MANUALE DI GESTIONE DOCUMENTALE DEL COMUNE DI TRANI AGGIORNATO AI SENSI DELLE LINEE GUIDA AGID SULLA FORMAZIONE, GESTIONE E CONSERVAZIONE DEI DOCUMENTI INFORMATICI è stato approvato il "Manuale di Gestione Documentale" aggiornato alle Linee Guida Agid sulla formazione, gestione e conservazione dei documenti informatici;
- con Deliberazione di Giunta Comunale n. 58 del 13.06.2025 avente ad oggetto: "APPROVAZIONE PIANO TRIENNALE PER L'INFORMATICA NELLA PUBBLICA AMMINISTRAZIONE EDIZIONE 2024-2026 - AGGIORNAMENTO 2025" è stato approvato il Piano triennale per l'informatica 2024- 2026 (aggiornamento 2025);

CONSIDERATO che:

- il Comune di Trani dispone di una rete informatica e telematica, costituita da un insieme di strumenti e mezzi informatici quali le componenti hardware e software e dei necessari collegamenti telematici che veicolano le informazioni da e verso le banche dati comunali;
- con l'emanazione della circolare AGID 2/2017 del 18/04/2017, venivano fornite indicazioni operative per la verifica delle condizioni minime di sicurezza ICT e del trattamento dei dati;

VISTI i Decreti direttoriali ACN prot. N. 29 del 2 gennaio 2023, n. 5489 dell'8 febbraio 2023 e n. 20610 del 28 luglio 2023;

DATO ATTO che l'utilizzo della rete informatica e telematica, di internet e della posta elettronica, sono strumenti ormai indispensabili per perseguire con efficienza, efficacia ed economicità le funzioni istituzionali e gestionali dell'Ente come imposto dalle normative vigenti, che sempre più tendono alla globalità delle informazioni telematiche;

RITENUTO pertanto necessario aggiornare il Regolamento che disciplina la gestione e l'utilizzo degli strumenti informatici e telematici comunali, utilizzata dai dipendenti e dagli amministratori comunali, al fine di diminuire il rischio di intrusione nei sistemi informativi dell'Ente ed altresì evitare il furto, l'accesso non autorizzato, la distruzione o perdita di dati;

CONSIDERATO che:

- è compito del Comune assicurare la piena funzionalità del sistema informatico e promuovere ogni opportuna misura, organizzativa e tecnologica, volta a prevenire il rischio di utilizzi impropri delle strumentazioni e delle banche dati;
- risulta fondamentale individuare il complesso delle misure che configurano il livello minimo di protezione del sistema informatico comunale e del patrimonio informativo digitale dell'Ente;
- per dare attuazione a tali esigenze è necessario fornire agli utenti (amministratori, responsabili di servizio, dipendenti e collaboratori) specifiche disposizioni circa le modalità da seguire per un corretto utilizzo degli strumenti e delle risorse informatiche messe loro a disposizione per lo svolgimento delle proprie mansioni istituzionali, in modo che ciascun utente possa collaborare attivamente alle politiche di sicurezza poste in atto dall'Amministrazione;
- risulta, altresì, necessario disciplinare le misure con le quali il Comune può eventualmente accertare e inibire le condotte illecite sull'utilizzo delle predette risorse, ponendo in essere adeguati e commisurati sistemi di controllo sul corretto utilizzo degli strumenti informatici, senza che ciò possa in alcun modo invadere e violare la sfera personale del lavoratore e quindi il suo diritto alla riservatezza ed alla dignità, come sancito dallo Statuto dei Lavoratori (L. 20/05/1970 n. 300);
- ogni utente è responsabile, civilmente e penalmente, del corretto utilizzo delle risorse informatiche, dei servizi a cui ha accesso e dei dati trattati a fini istituzionali;
- per rispondere alle suddette esigenze operative è stato elaborato uno specifico "Regolamento IT";
- tale regolamento è conforme alle indicazioni del Garante per la Protezione dei dati personali, nonché alle altre disposizioni normative in materia;
- tali prescrizioni si aggiungono ed integrano le specifiche istruzioni che vanno fornite a tutti gli incaricati in attuazione del Regolamento Europeo 679/16 "General Data Protection Regulation" (d'ora in avanti Reg. 679/16 o GDPR);

VISTO lo schema del "Regolamento IT" (Allegato A), il quale costituisce parte integrante, formale e sostanziale della presente;

VISTO il T.U. delle leggi sull'ordinamento degli enti locali, approvato con D.Lgs. 267/2000 e s.m.i.;

ACQUISITO il parere favorevole di regolarità tecnica, espresso ai sensi dell'art. 49, comma 1, del D.Lgs. n. 267/2000, il quale costituisce parte integrante, formale e sostanziale della presente;

DATO ATTO che il presente provvedimento non necessità del parere di regolarità contabile, atteso che lo stesso non ha riflessi né diretti né indiretti sulla situazione economico finanziaria o sul patrimonio dell'Ente;

Con votazione favorevole ed unanime espressa nei modi e nelle forme di legge

DELIBERA

Per le motivazioni di cui in premessa, che si intendono integralmente riportate e trascritte:

1. **DI APPROVARE** il "Regolamento IT del Comune di Trani", allegato alla presente come parte integrante, formale e sostanziale (Allegato A) ;
2. **DI DISPORRE** al Servizio Personale affinché copia del Regolamento sia consegnato e fatto sottoscrivere ai nuovi assunti, contestualmente alla sottoscrizione del contratto di lavoro;
3. **DI DISPORRE**, altresì, la trasmissione copia del presente provvedimento a tutti i Dirigenti, a tutto il personale dipendente, alle RR.SS.UU., nonché di provvedere alla pubblicazione della stessa sul sito istituzionale nell'ambito della sezione "Amministrazione Trasparente";
4. **DI DICHIARARE** la presente deliberazione immediatamente eseguibile ai sensi dell'art 134 comma 4 del D.Lgs 267/2000.

Il presente verbale viene letto, confermato e sottoscritto nei modi di legge.

Vice Sindaco	Il Segretario
Ferrante Fabrizio	Dott. Francesco Angelo Lazzaro

(*Il presente documento è sottoscritto con firma digitale - ai sensi degli art .20 e 21 D.lgs 82/2005*)