CITTA' DI VENEZIA

REGOLAMENTO PER L'UTILIZZO DELLE DOTAZIONI INFORMATICHE E DI TELECOMUNICAZIONE

Appendice al Regolamento sull'ordinamento degli uffici e dei servizi
Approvato dalla Giunta comunale con deliberazione n. 229 del 24 luglio 2019

Indice

1 Premessa e scopo

1. Il Comune di Venezia (di seguito "Comune") adotta il presente Regolamento per l'utilizzo delle dotazioni informatiche e di telecomunicazione (di seguito "Regolamento") per fornire un quadro preciso di indicazioni in merito ai criteri e alle modalità d'assegnazione e d'utilizzo delle stesse.

2. Per dotazioni informatiche e di telecomunicazione (di seguito anche "Dotazioni") si intendono tutte le strumentazioni hardware centrali e periferiche, i sistemi di rete e telecomunicazioni, compresi i dispositivi di telefonia fissa e mobili, e il relativo software di base ed applicativo di proprietà del Comune messo a disposizione degli utenti. Per Sistemi Informativi si intende la struttura del Comune di Venezia preposta alla direzione del sistema informativo comunale. Per Esecuzione Logistica si intende la struttura del Comune di Venezia preposta all'effettuazione degli spostamenti delle Dotazioni. Venis S.p.A. (di seguito anche "Venis") è la società strumentale affidataria della gestione del sistema informativo comunale, nominata dal Comune Responsabile del trattamento dati personali con nota p.g. 2018/0247104.

3. L'utilizzo delle Dotazioni deve sempre ispirarsi ai principi di massima diligenza, buona fede e correttezza, che devono costantemente uniformare e caratterizzare la condotta generale ed i singoli comportamenti di tutti i soggetti autorizzati al loro utilizzo

4. Il presente Regolamento persegue i seguenti scopi:
a) garantire la sicurezza, la disponibilità e l'integrità dei sistemi informatici e dei dati del Comune prodotti e archiviati digitalmente;
b) mantenere in efficienza, ottimizzare l'uso e prevenire utilizzi indebiti delle Dotazioni;
c) evitare che gli utenti possano esporre sé stessi e/o il Comune a sanzioni pecuniarie o penali, derivanti da un uso scorretto o illecito delle Dotazioni, nonché esporre il Comune a conseguenze pregiudizievoli, in relazione al suo patrimonio e/o alla sua immagine;
d) recepire e dare attuazione alle disposizioni normative e ai principi previsti dal Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 (di seguito anche solo "GDPR"), nonché dei Provvedimenti emanati dal Garante per la protezione dei dati personali (di seguito anche solo "Garante").

5. Non rientra tra gli scopi del presente Regolamento il controllo a distanza e/o in forma occulta delle opinioni, abitudini e/o dell'attività dei suoi dipendenti, che rimangono strettamente vietati e non consentiti. Pertanto, nel rispetto delle previsioni di cui agli artt. 4 e 8 della Legge 20 maggio 1970, n. 300 (di seguito anche solo "Statuto dei Lavoratori"), il Comune intende anche disciplinare, con il Regolamento, le modalità di raccolta ed utilizzo delle informazioni e dei dati trattati tramite le Dotazioni, informando circa l'esercizio dell'eventuale potere disciplinare del Comune nei confronti dei dipendenti, qualora si verificasse ed accertasse - secondo le procedure e nel rispetto delle garanzie e tutele oggetto delle previsioni che seguono - un uso improprio e/o non autorizzato delle Dotazioni.

6. Il Regolamento e le previsioni ed indicazioni in esso contenute sono richiamate all'interno dei seguenti atti:
a) informativa resa dal Comune, ai sensi e per gli effetti dell'art. 4 dello Statuto dei Lavoratori, quanto agli utenti, e in ogni caso dell'art. 13 del GDPR, in ordine alle modalità, finalità, procedure e relative tutele con riferimento al trattamento dei loro dati personali nel caso in cui si procedesse ad eventuali attività di controllo, anche attraverso strumenti di registrazione degli accessi e delle presenze (ad esempio badge, rilevatori magnetici o elettronici) o mediante verifiche sull'utilizzo

delle Dotazioni adottate per motivi professionali (ad esempio PC, tablet, smartphone aziendali), nonché della rete internet e della posta elettronica aziendale;
b) lettera di designazione del personale del Comune tra i "Soggetti Autorizzati al Trattamento", con riferimento alle relative istruzioni.

2 Ambito di applicazione

1. Il Regolamento si applica ai seguenti soggetti di seguito complessivamente denominati "utenti":
a) tutti coloro ai quali il Comune fornisce una "matricola" personale, ovvero:
a.a) tutti i dipendenti, indipendentemente dalla modalità di svolgimento dell'attività lavorativa (solo a titolo d'esempio: telelavoro, smart working, ecc.),
a.b) i titolari di cariche politiche;
b) tutti coloro che svolgono attività per il Comune, quali:
b.a) collaboratori e prestatori di lavoro autonomo a prescindere dal rapporto intrattenuto con l'amministrazione;
b.b) in generale, a chiunque sia autorizzato all'utilizzo delle Dotazioni del Comune nello svolgimento delle proprie funzioni istituzionali.

2. Rimane ferma, in ogni caso, l'inapplicabilità agli utenti che non rientrano nella categoria dei dipendenti di cui al precedente punto 2.1.a.a) di ogni riferimento relativo ai profili disciplinari e, più in generale, di ogni ulteriore previsione e/o normativa richiamata nel Regolamento che presupponga lo svolgimento di attività in regime di subordinazione.

3 Riferimenti normativi

a) Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 ("GDPR");
b) Decreto legislativo 10 agosto 2018, n. 101, "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016";
c) Opinion 2/2017 del cd. "Article 29 Data Protection Working Party" dell'8 giugno 2017, "on data processing at work";
d) Provvedimento del Garante del 1° marzo 2007, "Lavoro: le linee guida del Garante per posta elettronica e Internet", pubblicato in Gazzetta Ufficiale n. 58 del 10 marzo 2007;
e) Provvedimento del Garante del 27 novembre 2008 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema", pubblicato in Gazzetta Ufficiale n. 300 del 24 dicembre 2008;
f) Legge 20 maggio 1970, n. 300 "Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale, nei luoghi di lavoro e norme sul collocamento" ("Statuto dei Lavoratori");
g) Legge 22 aprile 1941 n. 633 "Protezione del diritto d'autore e di altri diritti connessi al suo esercizio" (di seguito anche solo "Legge sul Diritto d'Autore");
h) Decreto Legislativo 10 febbraio 2005, n. 30 (di seguito anche solo "Codice della proprietà industriale");
i) I vigenti Contratto Collettivo Nazionale di Lavoro e Contratto Collettivo Decentrato Integrativo.

4 Definizioni

1. Ferme le definizioni già previste nei paragrafi precedenti, le parole e le espressioni di seguito indicate hanno il seguente significato:

Amministratore di sistema: figura professionale dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui vengano effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i sistemi software complessi utilizzati dall'ente, le reti locali e gli apparati di sicurezza. Tale figura professionale è individuata da Venis.

Antivirus: un software atto a rilevare ed eliminare virus informatici o altri programmi dannosi.

Back Up: operazione tesa a creare una copia di sicurezza delle informazioni (dati o programmi).

Chat line: servizio che mette in contatto due o più utenti per una comunicazione in tempo reale.

Codice identificativo: codice che consente l'individuazione delle Dotazioni; gli elementi hardware delle postazioni di lavoro sono individuati con il codice SICOM.

Coworking: condivisione di una postazione tra più utenti, non necessariamente appartenenti allo stesso servizio, messa a disposizione per agevolare il lavoro al di fuori dell'abituale sede di lavoro dell'utente.

Data Breach: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

Data Breach Team: struttura del Comune deputata all'analisi degli eventi di potenziale data breach.

Dati Personali: qualsiasi informazione riguardante una persona fisica identificata o identificabile; si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un dato come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

Domain Controller: sistema che, nell'ambito del Sistema Informativo Comunale, gestisce le richieste di autenticazione per la sicurezza (login, controllo dei permessi, ecc.) e organizza la struttura del sistema in termini di utenti, gruppi e risorse di rete definendo i livelli di accesso alle risorse applicative.

Dotazioni informatiche e di telecomunicazione o Dotazioni: tutte le dotazioni hardware centrali e periferiche, i sistemi di rete e telecomunicazioni, compresi i dispositivi di telefonia fissa e mobili, e il relativo software di base ed applicativo di proprietà del Comune messo a disposizione degli utenti.

File di Log: file nel quale vengono registrate cronologicamente tutte le informazioni relative alle operazioni effettuate dagli utenti in un certo ambito (ad es. sistema, applicazioni, base dati);

File Server: sistemi di archiviazione informatica centralizzati adottati dal Comune e messi a disposizione degli utenti.

Hardware: parte fisica di dispositivi informatici o di telecomunicazione (personal computer, tablet, smartphone, ecc.).

Hard Disk: dispositivo di memoria di massa che utilizza uno o più dischi magnetici per l'archiviazione dei dati.

Interessati: persone fisiche, identificate o identificabili, alle quali si riferiscono i Dati Personali.

Log-in: attività volta ad identificare una utenza per l'accesso ad un computer o ad una applicazione informatica tramite inserimento di User ID e Password.

Log-out: attività volta a disconnettere una utenza dall'accesso ad un computer o ad una applicazione informatica.

Mailing list o *Liste di distribuzione o Caselle postali:* sistema organizzato per la condivisione via mail di messaggi a più persone.

Normativa Applicabile: normativa elencata al precedente punto 3 e tutti gli ulteriori provvedimenti e linee guida del Garante comunque applicabili.

Password: parola segreta associata ad un User ID.

Personal computer (di seguito "PC"): personal computer da tavolo o portatile.

Peer-to-Peer: tipologia di rete informatica caratterizzata da condivisione diretta di risorse tra i nodi della stessa che sono organizzati in modo non gerarchico; essa garantisce ridotti livelli di protezione.

Postazione: postazione di lavoro costituita da un personal computer - desktop, thin client o pc portatile – e da dispositivi e periferiche, a seconda delle specifiche esigenze lavorative, quali ad esempio: monitor, mouse, tastiera, cavi di alimentazione, cavi di rete, cavi usb, webcam, cuffie, microfoni, lettori smart card.

Responsabile del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo, esterno al Comune, che tratta dati personali per conto della stessa, ai sensi dell'art. 28 GDPR.

Responsabile della Protezione dei Dati (di seguito anche "RPD"): Responsabile della protezione dei dati previsto dall'art. 37 del GDPR nonché figura di contatto per il Garante.

Responsabile della struttura: dipendente dell'ente con qualifica dirigenziale o a cui è assegnato un incarico di responsabile di posizione organizzativa.

Server: componente informatica che fornisce servizi ad altre componenti (tipicamente chiamate client) attraverso una rete.

Sistema informativo comunale: consiste nell'insieme composto dalle risorse software, dall'infrastruttura hardware centrale e periferica, dall'infrastruttura di telecomunicazione (fonia e dati) locale e cittadina ed è finalizzato alla gestione (raccolta, registrazione, elaborazione, conservazione, comunicazione) del patrimonio informativo del Comune per l'esercizio dell'azione amministrativa e l'erogazione di servizi a utenti interni ed esterni.

Smart Card: dispositivo hardware ad alta sicurezza delle dimensioni di una carta di credito che possiede potenzialità di elaborazione e memorizzazione di dati.

Software: programma o un insieme di programmi in grado di funzionare su un elaboratore.

Titolare del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento dei dati personali.

Trattamento: qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica,

l'estrazione, la consulenza, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

User ID: codice identificativo associato ad una persona.

Virus: un software che è in grado, una volta eseguito, di infettare dei file in modo da riprodursi facendo copie di sé stesso, potendo provocare danni sia al software che all'hardware.

WiFi: sistema di comunicazione tra dispositivi elettronici che non fa uso di cavi.

5 Disposizioni riguardanti l'assegnazione delle Dotazioni e l'abilitazione per l'accesso al Sistema Informativo Comunale

Le assegnazioni delle Dotazioni e l'accesso al Sistema Informativo Comunale sono effettuate agli utenti sulla base delle esigenze generali espresse dal Comune o da esigenze specifiche espresse dai Responsabili di Struttura.

5.1 Accesso al Sistema Informativo Comunale

1. Contestualmente all'inizio del rapporto di lavoro (per gli utenti di cui al precedente punto 2.1.a) o alla data indicata nella richiesta di abilitazione (per gli utenti di cui al precedente punto 2.1.b) viene creata un'utenza nel Domain Controller.

2. In funzione delle specifiche esigenze di servizio sono configurabili le abilitazioni relative a:
a) alla rete comunale;
b) alla casella di posta elettronica personale (nome.cognome@comune.venezia.it);
c) alla posta elettronica istituzionale (liste di distribuzione o caselle postali);
d) ai file server relativi alle cartelle personali;
e) ai file server relativi alle cartelle di servizio;
f) alla intranet comunale;
g) ai software applicativi.

Di norma per gli utenti di cui al precedente punto 2.1.a sono configurate le abilitazioni per i servizi di cui a precedenti punti a), b), d), f). Ulteriori abilitazioni avvengono su richiesta del Responsabile della Struttura. Le abilitazioni per gli utenti di cui al precedente punto 2.1.b sono effettuate su richiesta del Dirigente.

5.2 Postazione di lavoro

1. Di norma a ciascun utente viene assegnata una sola postazione. Richieste di ulteriori assegnazioni, in quanto deroganti al suddetto principio, devono essere motivate e vanno autorizzate dai Sistemi Informativi.

2. L'assegnazione della postazione, o di un suo componente, ad un utente viene effettuata direttamente dal Responsabile della struttura se l'attrezzatura è già presente presso l'ufficio. Nel caso sia necessaria l'assegnazione di nuova postazione, il Responsabile della struttura ne fa richiesta ai Sistemi informativi tramite il sistema gestionale "4900web" disponibile nella intranet comunale.

3. A seguito dell'assegnazione ad un utente di una postazione o suo componente, è fatto obbligo:
a) all'utente di aggiornare tempestivamente, tramite l'apposito applicativo disponibile nella intranet dell'ente, l'elenco delle attrezzature informatiche utilizzate;

b) al responsabile della struttura di validare l'assegnazione di tali attrezzature, mantenendo assegnate a sé le postazioni di lavoro condivise e le attrezzature in uso comune ai propri uffici (es. pc portatili).

4. L'utilizzo della postazione da parte di più utenti è consentito e gestito a livello centrale tramite profilazione degli utenti; l'assegnazione di una postazione ad un utente non implica quindi l'esclusività di utilizzo della stessa.

5. Gli utenti che svolgono funzioni che non richiedono un'assegnazione puntuale della postazione (ad esempio: agenti di Polizia Municipale, docenti Nidi e Materne, ispettori del Servizio Ispettivo Casa da Gioco, ecc.) utilizzano postazioni in condivisione con altri utenti sulla base dell'organizzazione definita dalle rispettive strutture; tali postazioni sono formalmente assegnate al responsabile della struttura.

6. Presso alcune sedi lavorative possono essere realizzati spazi di coworking, attrezzati con postazioni di lavoro utilizzabili da qualsiasi utente per favorire il lavoro in mobilità.

7. In caso di trasferimento dell'utente ad altro ufficio o ad altra sede dell'ente, di norma la postazione viene trasferita contestualmente. Nel caso in cui la postazione di lavoro abbia caratteristiche tecniche particolari legate alle specifiche funzioni delle strutture coinvolte, i Sistemi informativi valutano, sentite le strutture stesse, soluzioni differenti.

8. La movimentazione delle postazioni tra le diverse sedi o uffici viene disposta da Venis, su indicazione dei Sistemi informativi, ed effettuata dall'Esecuzione Logistica.

9. In caso di cessazione del rapporto di lavoro, di assenza o trasferimenti temporanei di lunga durata ad altri enti, e in qualsiasi caso di sostituzione della postazione, la postazione precedentemente assegnata all'utente ritorna nella disponibilità dei Sistemi informativi che decidono in merito al suo riutilizzo o dismissione. In tali casi è compito del Responsabile della struttura comunicare tempestivamente la dismissione delle Dotazioni tramite apertura di ticket al servizio informatico online "4900web" nella intranet comunale.

5.3 Dispositivi di stampa

1. Ai fini del contenimento dei costi e in considerazione degli obblighi di dematerializzazione in atto nella Pubblica Amministrazione, nonché dell'inquinamento ambientale derivante dalle stesse, le stampanti locali assegnate a singoli utenti vengono progressivamente dismesse a vantaggio dell'utilizzo delle stampanti di rete dipartimentali collocate in aree comuni e utilizzabili da gruppi definiti di utenti (non legate a singole strutture organizzative). Possono essere previste casistiche particolari di volta in volta autorizzate dai Sistemi Informativi.

5.4 Dispositivi di telefonia fissa

1. La postazione di lavoro è di norma corredata da un dispositivo di telefonia fissa. Le assegnazioni di linee telefoniche, utenze, apparati e abilitazioni, vengono attribuite dai Sistemi informativi sulla base di motivate esigenze espresse dagli utenti, approvate dai Dirigenti, secondo le modalità indicate nella intranet comunale.

2. I dispositivi di telefonia fissa in uso a più utenti sono formalmente assegnati al responsabile della struttura.

5.5 Dispositivi di telefonia mobile

1. I dispositivi di telefonia mobile si compongono di SIM e apparati (cellulare, smartphone, router wifi, tablet, ecc.).

2. I dispositivi assegnabili sono esclusivamente quelli disponibili nell'ambito del contratto di fornitura del servizio di telefonia mobile in vigore, approvati da Venis e dai Sistemi informativi in quanto compatibili con le funzioni del Sistema Informativo Comunale.

3. I dispositivi di telefonia mobile sono assegnati dai Sistemi informativi sulla base di richieste degli utenti approvate dai Direttori delle relative strutture, secondo le procedure previste nella intranet comunale. Nel caso di dispositivi di telefonia mobile destinati a cariche politiche, la richiesta viene formulata o approvata dal Direttore responsabile della struttura di coordinamento amministrativo delle stesse.

4. Per particolari esigenze di servizio, gli apparati possono essere messi a disposizione di più utenti e sono formalmente assegnate al Responsabile della struttura, il quale ne risponde dell'utilizzo.

5.6 File server

1. I sistemi di file server centralizzati prevedono spazi di memorizzazione dedicati al singolo utente e spazi condivisi tra gli utenti di strutture e progetti.

2. Le abilitazioni all'utilizzo degli spazi di memorizzazione condivisi rispecchiano generalmente la struttura organizzativa di appartenenza di ciascun utente o la partecipazione a progetti trasversali o comunque sono configurati su richiesta dei Responsabili di struttura.

6 Disposizioni riguardanti le modalità d'uso delle Dotazioni

6.1 Norme generali di comportamento

1. Costituisce regola generale che l'utilizzo delle Dotazioni deve essere limitato esclusivamente all'esercizio delle proprie funzioni lavorative; non è ammesso l'uso a scopi privati.

2. Gli utenti sono tenuti ad utilizzare le Dotazioni messe a loro disposizione con diligenza, adottando comportamenti idonei a non causare danni alle stesse.

3. Gli utenti dovranno osservare gli obblighi specifici di seguito riportati:

a) è fatto divieto di cedere a terzi le Dotazioni, o loro componenti, e comunque di consentirne l'utilizzo da parte di terzi non autorizzati dal Comune;

b) è fatto divieto di manomettere in qualsiasi modo sia l'hardware che il software delle Dotazioni assegnate;

c) è fatto divieto di rimuovere o rendere illeggibile il codice identificativo delle Dotazioni; per le postazioni di lavoro tale codice è denominato SICOM;

d) è fatto divieto di impiegare le Dotazioni per finalità diverse da quelle per le quali sono state progettate o utilizzare i sistemi informativi per compiere azioni illecite nei confronti di altri sistemi, sia interni che esterni, all'organizzazione;

e) è fatto obbligo di segnalare eventuali furti o smarrimenti come indicato al paragrafo 6.2. lett. i);

f) è fatto obbligo di segnalare ogni anomalia o malfunzionamento riguardante le Dotazioni secondo le procedure previste nell'intranet comunale;

g) ai fini del contenimento della spesa energetica, della riduzione dell'inquinamento, della necessità di prolungare la vita dei dispositivi, è fatto obbligo di: spegnere il monitor in caso di temporanea inattività, spegnere la postazione al termine della giornata di lavoro, limitare al minimo indispensabile la produzione di stampe.

6.2 Norme generali per la sicurezza e la protezione dei dati personali

1. L’integrità e la disponibilità delle informazioni e dei dati, ivi inclusi i dati personali, sono garantite solo quando gli stessi sono memorizzati nei file server messi a disposizione dal Comune, oggetto di sistemi di protezione, monitoraggio e backup.

2. Per garantire la sicurezza e la riservatezza dei dati è fatto obbligo agli utenti di:

a) mantenere la riservatezza delle proprie credenziali d'accesso alle Dotazioni, al sistema informativo comunale nel suo complesso e ai singoli applicativi;

b) salvare documenti e dati su file server relativo alla struttura di appartenenza; eventuali dati strettamente personali, inerenti comunque all'attività lavorativa, possono essere salvati nella cartella riservata a ciascun utente presente su file server. Non è consentito il salvataggio di dati su dischi interni alle postazioni di lavoro né su memorie esterne rimovibili (hard disk esterni, chiavette usb, ecc.); qualora per specifiche eccezionali esigenze sia autorizzato dai Sistemi informativi l’utilizzo di memorie esterne, è fatto obbligo all’utente di conservare tali dispositivi in luoghi protetti (ad es. armadi e cassettiere chiusi a chiave), verificare il loro contenuto informativo prima della loro eventuale consegna a terzi e prima della loro eliminazione/distruzione o sostituzione, nonché procedere alla cancellazione dei dati in essi contenuti quando non più necessari;

c) archiviare le informazioni e i dati esclusivamente necessari all’attività lavorativa. Costituisce buona regola la pulizia periodica degli archivi, da eseguirsi almeno ogni 6 (sei) mesi, con cancellazione dei file obsoleti o inutili. Particolare attenzione va prestata alla duplicazione dei dati, al fine di evitare un’archiviazione ridondante;

d) effettuare il log-out dalla propria postazione di lavoro al termine della giornata lavorativa e bloccarla in caso di allontanamento dalla stessa;

e) bloccare l'accesso ai dispositivi mobili con PIN o altro sistema disponibile;

f) eliminare nei dispositivi mobili l'anteprima nelle notifiche del contenuto di messaggi ricevuti di qualsiasi tipo;

g) presidiare l’intero processo di stampa, fotocopia, scansione o trasmissione via fax di documenti, al fine di impedire la volontaria o accidentale diffusione di dati personali o la perdita di riservatezza sulle informazioni contenute nei documenti stessi, anche utilizzando ove disponibili il PIN di protezione per le stampe; allo stesso scopo, è dovere degli utenti prelevare immediatamente i fogli riprodotti da stampanti, fotocopiatrici e fax;

h) in caso di trasferimento ad altra struttura, eliminare dalla postazione, dalle cartelle di rete personali e dalla posta elettronica eventuali file contenenti dati che non è più autorizzato a trattare; il Responsabile di struttura è tenuto a revocare le abilitazioni all'uso dei software gestionali e delle risorse condivise (cartelle di rete, liste di distribuzione, ecc.) dell'utente;

i) qualora si verificasse il furto o lo smarrimento di una dotazione informatica o di telecomunicazione, comunicare immediatamente e comunque entro 24 ore dalla scoperta l’accaduto al Data Breach Team, fornendo tutte le opportune informazioni e chiarimenti in merito, sporgere denuncia alle autorità competenti inviandone copia al Data Breach Team stesso.

3. Più in generale, si ricorda inoltre l’obbligo, al termine dell’orario di lavoro, di:

a) garantire che materiale o documenti cartacei contenenti informazioni relative al Comune siano conservati in appositi cassetti e/o armadi;

b) ove possibile, chiudere a chiave cassetti, porte degli uffici o di aree ad accesso limitato;

c) raccogliere tutti i documenti stampati e i documenti che non sono più richiesti/necessari e provvedere alla loro definitiva eliminazione. In ogni caso, tali documenti non devono essere depositati integralmente nei normali cestini da ufficio.

6.3 Norme per l’utilizzo della postazione di lavoro

1. L’assegnazione delle Dotazioni è finalizzata allo svolgimento dell’attività lavorativa; l’utilizzo di queste apparecchiature ai fini privati non è consentito. In caso di utilizzo difforme, l’utente sarà ritenuto esclusivo responsabile per ogni eventuale danno che dovesse derivarne.

2. Le Dotazioni vengono installate, configurate e aggiornate da Venis secondo configurazioni predefinite. Installazioni di hardware e software diverse dalla configurazione iniziale sono autorizzate dai Sistemi Informativi ed eseguite da Venis, anche per gli applicativi per i quali non sono richiesti i privilegi di amministratore di sistema.

3. L’accesso alle postazioni gestite centralmente in dominio active directory è configurato nominativamente per ciascun utente e non prevede la concessione di privilegi di amministratore di sistema. Le credenziali coincidono con quelle d’accesso al sistema informativo comunale di cui al successivo punto 6.5.

4. Nel caso sia necessario portare qualsiasi dotazione informatica fuori della sede di lavoro (ad es. in caso di eventi, corsi, laboratori formativi, ecc.) è fatto obbligo agli utenti di prendere tutte le precauzioni affinché non venga smarrita, danneggiata o rubata, nonché di prestare assoluta attenzione a non lasciarla mai incustodita e di conservarla in luoghi protetti.

5. Le seguenti attività sono espressamente proibite agli utenti:
a) modificare la configurazione hardware in dotazione, aggiungendo o rimuovendo componenti; l'installazione da parte degli utenti di schede di espansione, memorie aggiuntive interne, schede audio, video o altri dispositivi hardware viene considerata come manomissione del sistema;
b) utilizzare e/o installare apparati di rete e modem sui PC connessi alla rete comunale;
c) qualora le Dotazioni informatiche siano dotate di modem, antenna wifi, o possano connettersi a reti internet tramite altro dispositivo per trasmissione dati, anche USB, o tramite rete cellulare, è severamente vietato l’utilizzo di questi dispositivi quando contemporaneamente connessi alla rete dell’ente; l’accesso con tali modalità dovrà avvenire disattivando ogni altro dispositivo di connessione alla rete comunale;
d) modificare la configurazione software in dotazione, installare/effettuare download di software/applicativi non autorizzati. L'installazione di software non autorizzato dai Sistemi Informativi viene considerato come manomissione del sistema;
e) eliminare un programma o file installato legalmente in modo tale da impedire od ostacolare le normali operazioni, ivi inclusa la disattivazione dei sistemi di sicurezza;
f) acquisire, utilizzare, duplicare software illegalmente.

6. Nel caso in cui i Destinatari vengano a conoscenza di una qualsiasi vulnerabilità derivante da difetti di configurazione o difetti intrinseci ai programmi e/o ai sistemi, dovranno darne tempestivamente comunicazione ai Sistemi informativi.
7. È proibita ogni attività finalizzata a collaudare la sicurezza del sistema informatico, salvo esplicita autorizzazione fornita dall’Amministratore di Sistema.

6.4 Norme per l’utilizzo delle Dotazioni di telefonia fissa e mobile

1. L’assegnazione delle Dotazioni di telefonia è finalizzata allo svolgimento dell’attività lavorativa. L’utente sarà ritenuto esclusivo responsabile per ogni eventuale danno nei confronti del Comune che dovesse derivare dall’utilizzo dei dispositivi. Ogni utilizzo non inerente all’esercizio delle funzioni assegnate all’utente può infatti contribuire a generare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza; pertanto nel caso in cui il Comune dovesse sostenere costi dovuti a un uso improprio del dispositivo di telefonia mobile assegnato o all'inosservanza del presente Regolamento, essi saranno addebitati all’assegnatario.

2. L'utilizzo dell'apparato di telefonia mobile di servizio per telefonate personali è consentito esclusivamente quando l'assegnatario accetta la fatturazione separata a proprio carico di tali telefonate, con un contratto di tipo "dual billing", qualora disponibile nel profilo tariffario della SIM assegnata e dal contratto con l'operatore di telefonia.

3. Nell'utilizzo delle dotazioni di telefonia è fatto divieto all'utente:

a) di chiamare numeri a pagamento, salva preventiva autorizzazione del Dirigente e dei Sistemi Informativi;

b) di attivare servizi di deviazione da numerazione fissa a numerazione esterna e da numerazione fissa a numerazione mobile. Eventuali deroghe vanno motivate e devono essere autorizzate dai Sistemi informativi;

c) di utilizzare le SIM assegnate dal Comune su apparati diversi da quelli assegnati;

d) di utilizzare SIM personali in apparati mobili forniti dall'Amministrazione.

4. Nell'utilizzo delle Dotazioni di telefonia mobile è fatto obbligo di configurare l'apparecchio secondo quanto stabilito al precedente punto 6.2., ovvero:

a) bloccare l'accesso ai dispositivi mobili con PIN o altro sistema disponibile;

b) eliminare nei dispositivi mobili l'anteprima nelle notifiche del contenuto di messaggi ricevuti di qualsiasi tipo.

6.5 Norme per l'accesso al sistema informativo comunale e la gestione delle credenziali

1. L'accesso al sistema informativo comunale è sottoposto a procedure di identificazione personale (log-in) tramite Domain Controller basate sull'utilizzo di credenziali composte da un identificativo univoco (User ID) e di una parola segreta (Password) necessari al riconoscimento della identità degli utenti da parte del sistema installato sulle Dotazioni e/o dell'applicazione in uso.

2. L'accesso al sistema informativo del Comune è consentito:

a) a tutti gli utenti muniti di matricola personale, di cui al precedente punto 2.1.a.;

b) agli ulteriori utenti, di cui al precedente punto 2.1.b., su richiesta del Dirigente della struttura organizzativa con cui essi collaborano; tale richiesta deve precisare: nome, cognome, data di nascita, data di inizio e conclusione del rapporto con l'amministrazione, sistemi cui l'utente deve essere autorizzato ad accedere.

3. È vietato il rilascio di credenziali d'accesso al sistema informativo comunale associate ad utenti generici (ufficio, progetto) e non nominativo.

4. Le credenziali consentono l'accesso al proprio profilo sulla postazione, ai sistemi centrali di file server (cartelle di rete e personali), alla intranet comunale e ai servizi collegati (posta elettronica, protocollo, applicativi, ecc.), nonché consentono il riconoscimento dell'utente da parte del proxy per l'accesso ad internet.

5. Qualora sistemi applicativi aziendali richiedano ulteriori credenziali d'accesso, gli utenti devono astenersi dall'utilizzare le medesime credenziali utilizzate per il sistema informativo comunale.

6. Le credenziali sono segrete e strettamente personali; l'utente è tenuto:

a) a modificare la password al momento del primo utilizzo e ogniqualvolta richiesto dalle procedure automatiche di cambio password impostate con scadenza almeno trimestrale, nonché tutte le volte ritenga siano venuti meno i requisiti di riservatezza;

b) a non comunicarle in alcun caso ad altri soggetti;

c) a non inserirle in messaggi di posta elettronica o trasmetterle attraverso qualsiasi altra forma di comunicazione elettronica;
d) a non salvarle su strumenti o documenti informatici che non siano protetti a loro volta da apposite credenziali;
e) a non trascriverle su fogli, biglietti, post-it o su oggetti, soprattutto se posti nelle vicinanze del PC;
f) a prestare attenzione che non siano attivi sistemi di memorizzazione automatica delle credenziali.

7. Nella scelta delle password l'utente è tenuto a rispettate le seguenti regole:
a) la password dev'essere composta da almeno 8 caratteri, contenere almeno una lettera minuscola, una lettera maiuscola, un numero e un carattere speciale (!, £, %, $, &, ?, ecc.);
b) la password non deve contenere riferimenti personali, anche se in forma parziale, come il proprio nome, la data di nascita, il numero di matricola e qualsiasi altro dato riconducibile all'utente o alla sua storia personale;
c) i sistemi di autenticazione dei sistemi applicativi possono implementare ulteriori regole che l'utente è obbligato a rispettare.

8. L'utente è responsabile di qualsiasi azione o attività svolta tramite l'utilizzo delle credenziali personali a lui assegnate.

9. Per ragioni di sicurezza Venis può disattivare temporaneamente l'accesso alla postazione e/o l'accesso alla rete di una o più postazioni fino al ripristino delle condizioni di sicurezza.

6.6 Norme generali per l'utilizzo della rete intranet e internet

1. La rete del Comune si basa su un'infrastruttura in fibra ottica e wifi proprietaria e su linee di operatori privati. La rete è gestita da Venis che configura le postazioni per l'utilizzo della stessa. Il collegamento alla rete comunale avviene tramite infrastruttura fisica costituita dagli impianti LAN predisposti presso le sedi adibite ad ufficio; in alcune di esse possono essere attivi anche servizi WiFi che consentono il collegamento alla rete comunale. Inoltre presso alcune sedi così come in alcune zone della città è disponibile la rete WiFi "VeniceConnected" che consente invece solamente il collegamento alla rete internet, previa autenticazione.

2. È vietato collegare alla rete comunale apparati non di proprietà dell'amministrazione, salvo l'esplicita e preventiva autorizzazione dei Sistemi Informativi.

3. Non è consentito dalla postazione l'accesso contemporaneo alla rete informatica del Comune di Venezia e alle reti esterne se non attraverso il proxy.

6.7 Norme per l'utilizzo di Internet

1. Il Comune di Venezia consente agli utenti l'accesso alla rete internet per esclusivi scopi lavorativi. L'accesso ad internet avviene attraverso un proxy server, il quale regola e registra ogni accesso tenendo traccia delle attività di ciascun utente. Le credenziali sono le medesime previste per l'accesso al sistema informativo.

2. Al fine di garantire un appropriato utilizzo della rete internet, gli utenti devono rispettare le seguenti regole:
a) è consentita la navigazione in internet solo su siti contenenti informazioni necessarie o utili all'attività lavorativa o, comunque, all'acquisizione di notizie utili alla propria formazione/informazione professionale;

b) l’utente non è mai autorizzato all’installazione di programmi o software particolari per la fruizione di servizi e contenuti e non è altresì autorizzato ad effettuare il download di software, file musicali, video etc. con finalità estranee all’attività lavorativa;

c) deve rispettare le norme in materia di diritto di autore e altri diritti connessi e di utilizzo della rete;

d) non è autorizzato ad accedere a servizi di condivisione di file in modalità peer-to-peer;

e) non deve utilizzare sistemi per l'offuscamento della connessione con la finalità di rendere nascosta la propria identità nella rete, in particolare è vietato l'utilizzo di servizi/software di anonimizzazione;

f) durante il servizio non è permesso, salvo che per motivi lavorativi, professionali, formativi, partecipare a forum, utilizzare chat line o bacheche elettroniche, social network (quali facebook, instagram, twitter, ecc.), anche usando pseudonimi;

g) l’utente è personalmente responsabile della propria condotta nell'utilizzo delle reti e dei servizi di telecomunicazione.

3. Il Comune può prevedere modalità di filtraggio del traffico internet bloccando la navigazione su siti e/o categorie di siti i cui contenuti sono ritenuti dall’ente come estranei alle proprie attività.

6.8 Norme per l’utilizzo della Posta elettronica

1. Il Comune di Venezia consente agli utenti l’utilizzo della posta elettronica per esclusivi scopi lavorativi. Gli utenti assegnatari delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse, nonché di garantire la riservatezza delle credenziali di accesso. Ad ogni e-mail inviata viene automaticamente aggiunta una nota finale riportante un’adeguata informativa relativa alle informazioni confidenziali.

2. Ad ogni utente cui viene assegnata una casella di posta elettronica personale, la stessa di regola è denominata: nome.cognome@comune.venezia.it.

3. Su richiesta dei Responsabili di struttura, tramite apertura di ticket al servizio informatico online “4900web” nella intranet comunale, vengono generate “liste di distribuzione” o “caselle postali” per la gestione condivisa di indirizzi di posta istituzionali, di regola denominati: ufficio@comune.venezia.it o progetto@comune.venezia.it. Al fine di evitare che si vengano a creare situazioni di accesso esclusivo ad informazioni rilevanti ai fini della gestione dei procedimenti dell'ente è opportuno che l’invio di email - in particolare se rivolte all’esterno dell’ente – sia effettuato utilizzando come mittente, ove disponibili, le liste di distribuzione anziché le caselle di posta personali.

4. Gli indirizzi istituzionali di posta elettronica certificata del Comune di Venezia sono pubblicati nel sito internet istituzionale; per il loro utilizzo si fa riferimento al Manuale di gestione dei documenti del Comune di Venezia.

5. Per un corretto utilizzo della posta elettronica vanno rispettate le seguenti indicazioni:

a) Spam: i messaggi di posta elettronica ricevuti possono contenere informazioni o richieste anche non veritiere, e anche l’indirizzo stesso del mittente può essere falsificato. Il Comune di Venezia protegge i propri servizi di posta con un sistema antispam. È fatto comunque obbligo agli utenti di non aprire documenti, eseguire programmi, seguire link a siti internet, contenuti in messaggi di provenienza incerta, ed è fatto divieto di rispondere a tali messaggi, che vanno invece segnalati come spam. In caso di dubbi sull'autenticità di messaggi richiedere il supporto tramite inoltro della mail sospetta a sosvirus@venis.it;

b) Allegati: va controllata la dimensione degli allegati, inviando allegati di grandi dimensioni (superiori a 5 MB) solo quando effettivamente necessario e dopo aver verificato se non sia

possibile un loro "alleggerimento", effettuando delle compressioni delle immagini, o convertendo l'intero documento in formato .pdf. Se possibile utilizzare per la condivisione di documenti le cartelle dei file server;

c) Firme e Conferme di lettura: non vanno impostate automaticamente per tutti i messaggi, ma inserite al bisogno in fase di composizione del singolo messaggio;

d) Manutenzione: è necessario verificare periodicamente l'archivio della propria casella di posta elettronica conservando solo la corrispondenza strettamente necessaria alla propria attività;

e) Invio "massivo": i messaggi di posta elettronica vanno inviati solo ai destinatari oggettivamente interessati alla comunicazione cercando di limitarne il più possibile il numero, in particolare è vietata la diffusione di "catene" di ogni genere e tipo; si informa che invii massivi possono causare il blocco, per motivi di sicurezza, dell'account di posta elettronica;

f) al fine di limitare l'occupazione di spazio è necessario evitare l'invio documenti di rilevante dimensione a una pluralità di destinatari, preferendo sistemi di condivisione dei documenti;

g) liste di distribuzione esterne: evitare di iscriversi a mailing list esterne salvo che queste non siano utili per l'espletamento della propria attività lavorativa ed in ogni caso dopo aver accuratamente verificato in anticipo se tali servizi siano affidabili;

h) non utilizzare l'indirizzo di posta elettronica comunale per la partecipazione a dibattiti, chat, forum, social network o mailing-list o per l'iscrizione a servizi di qualunque genere per uso privato;

i) gli utenti sono tenuti a mantenere in ordine la propria casella di posta elettronica, cancellando documenti inutili ed e-mail non necessarie, in modo tale da razionalizzare l'impiego delle risorse informatiche.

6. Al fine di assicurare la disponibilità del contenuto della casella di posta elettronica in caso di improvvisa o prolungata assenza degli utenti o di un loro impedimento, l'accesso alla predetta casella di posta elettronica potrà essere effettuato dall'Amministratore di Sistema. Sarà cura dell'Amministratore di Sistema realizzare report di tali attività al fine di informare l'utente interessato alla prima occasione utile.

7. Una volta disattivato l'account di posta elettronica, copia dei messaggi di posta elettronica sarà conservata entro i termini previsti dal presente Regolamento e/o dalla Retention Policy, salvo che vi siano elementi che inducano il Comune a ritenere necessario un periodo di conservazione più lungo (ad esempio, per finalità di difesa di un diritto in sede giudiziaria), anche in seguito ad un'eventuale valutazione di impatto ai sensi e per gli effetti dell'art. 35 del GDPR.

6.9 Antivirus

1. Le postazioni sono dotate di software antivirus, aggiornato centralmente con strumenti di distribuzione automatica del software.

2. È vietato disattivare il sistema antivirus presente sulla postazione, modificarne la configurazione o usare software antivirus differenti da quello fornito dall'Amministrazione.

3. Qualora si rilevino comportamenti anomali della propria postazione, deve essere tempestivamente aperto un ticket al servizio informatico online "4900web" nella intranet comunale Altana per assistenza tecnica.

7 Disposizioni riguardanti la revoca dell'assegnazione delle Dotazioni e dell'accesso al sistema informativo comunale

1. Alla conclusione del rapporto di lavoro o allo scadere del rapporto di collaborazione cessano l'assegnazione delle Dotazioni, l'accesso al sistema informativo comunale e ai software applicativi.

I dispositivi mobili (ad es. cellulari, tablet, notebook, ecc.) devono essere contestualmente riconsegnati ai Sistemi informativi.

2. Le abilitazioni dell'utente di cui al punto 5.1 vengono disattivate con riferimento: alla data di cessazione resa evidente dai sistemi di gestione del personale (per gli utenti di cui al precedente punto 2.1.a) o alla data indicata nella richiesta di abilitazione (per gli utenti di cui al precedente punto 2.1.b) e comunque in qualsiasi caso di cessazione del rapporto con l'ente o su richiesta del Dirigente. Per la casella di posta elettronica personale verrà attivato un servizio di risposta automatica per i successivi 30 giorni.

3. Non è consentito ad alcuno l'accesso ai dati dell'utente salvati su file server relativi a cartelle personali o posta elettronica, fatte salve le richieste dell'autorità giudiziaria e le esigenze dell'amministrazione nel rispetto di quanto previsto dai provvedimenti del Garante della Privacy e dalle norme vigenti.

4. Quando il rapporto di lavoro o collaborazione venga a cessare, è fatto divieto all'utente di conservare, duplicare, comunicare o diffondere informazioni e dati.

5. In qualunque momento è facoltà dei Direttori disporre la revoca dell'assegnazione dei dispositivi di telefonia mobile.

8 Disposizioni in merito ai controlli

1. Il Comune, per motivi organizzativi o di sicurezza si riserva la facoltà di effettuare, attraverso Venis, controlli saltuari e occasionali, garantendo agli utenti il rispetto dei principi di liceità, pertinenza e non eccedenza previsti dalla Normativa Applicabile, di quanto previsto dai provvedimenti del Garante della Privacy, nonché il rispetto del divieto dei controlli a distanza dei lavoratori dipendenti.

2. Su richiesta dell'Autorità giudiziaria il Comune, tramite Venis, è tenuto ad effettuare qualsiasi controllo sull'utilizzo delle Dotazioni.

3. Il Comune si riserva, in particolare, di monitorare le reti e le Dotazioni nei seguenti casi:
a) necessità di effettuare verifiche sulla funzionalità e sulla sicurezza dei sistemi;
b) constatazione di utilizzo indebito della posta elettronica e della rete Internet;
c) necessità di effettuare verifiche tese alla protezione del patrimonio del Comune;
d) presenza di casi di abusi da parte di singoli o reiterati;
e) presenza di indizi relativi alla fuga di informazioni riservate o confidenziali.

4. Segnatamente, controlli periodici possono essere effettuati su: volume dei messaggi scambiati, formato e dimensione dei file allegati, durata dei collegamenti ad Internet (globale, per funzione, per gruppi o tipologia di utenti), siti visitati più frequentemente (globale, per funzione, per gruppi o tipologia di utenti), informazioni raccolte dai dispositivi di sicurezza (firewall, antivirus, IDS, IPS, ecc.).

5. Le informazioni relative ai file log vengono conservati per un periodo di 12 mesi e funzionalmente alla capienza dei server.

6. Le modalità con cui verranno effettuati i controlli saranno le seguenti:
a) i controlli, ove possibile, verranno effettuati preventivamente su informazioni appartenenti a gruppi collettivi di utenti, su dati aggregati e anonimi tramite l'analisi di statistiche generali;
b) successivamente, verranno inoltrati avvisi collettivi di diffida al compimento di operazioni non consentite o, a seconda della gravità, verranno prese misure di tipo individuale, specialmente in caso di abuso e/o anomalie reiterate;

c) nei casi in cui si debba far fronte a particolari esigenze tecniche o di sicurezza oppure si debbano utilizzare i dati registrati con riferimento all'esercizio o alla difesa di un diritto in sede giudiziaria (azioni da parte di terzi verso il Comune o viceversa, o in caso di verifiche relative ad un presunto comportamento illecito), oppure si ottemperi all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria, tale periodo verrà prolungato secondo le necessità del caso e nel pieno rispetto delle finalità descritte;

d) in ogni caso verranno esclusi controlli prolungati, costanti o indiscriminati o comunque preordinati al controllo a distanza dei lavoratori. A tal riguardo si precisa che: in ogni caso non si fa luogo alla lettura e alla registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio e-mail ivi inclusi i salvataggi periodici dei dati (c.d. "back up"); inoltre, non si procede alla riproduzione o memorizzazione sistematica delle pagine web visualizzate dall'utente, né alla lettura e alla registrazione dei caratteri inseriti tramite tastiera o analogo dispositivo.

7. L'Amministratore di Sistema può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericoloso per la sicurezza, sia sul PC degli utenti che sulle unità di rete.

8. L'effettuazione di tali controlli, che non hanno lo scopo di monitorare l'attività degli utenti, bensì di verificare la sicurezza del sistema e per effettuare la manutenzione, avverranno nel pieno rispetto della Normativa Applicabile.

9. Con particolare riferimento all'utilizzo dei telefoni, il Comune effettua verifiche periodiche volte a verificare la coerenza dei costi derivanti dalle utenze telefoniche associate con i suddetti apparecchi, nel pieno rispetto della Normativa Applicabile: a tal proposito verranno segnalati agli utenti eventuali discrepanze o problemi che dovessero essere riscontrati nel corso di tali controlli.

10. Con il presente Regolamento è fornita informativa agli utenti, anche ai sensi dell'art. 13 del GDPR, in merito ai controlli e al relativo trattamento dati; l'eventuale conservazione di tali dati avverrà per il tempo strettamente limitato al perseguimento lecito di finalità organizzative e di sicurezza.

9 Conservazione dei dati

1. Quotidianamente vengono salvati su sistemi esterni al data center tutti i dati relativi a: cartelle di rete, posta elettronica, file di Log. I supporti esterni, conservati per almeno 180 giorni, possono essere accessibili solo all'Amministratore di Sistema.
2. I file di Log contengono le informazioni relative ad almeno gli ultimi 180 giorni. I dati contenuti nei Log possono essere trattati in via eccezionale e tassativamente nelle seguenti ipotesi: per corrispondere ad eventuali richieste della polizia giudiziaria e/o dell'autorità giudiziaria, allorquando sia necessario un intervento – espressamente richiesto dall'utente – volto al recupero di dati contenuti in file o e-mail accidentalmente andati persi.
3. Il contenuto dei dispositivi di memorizzazione, delle cartelle dei file server, degli account di posta elettronica saranno conservati sul server centrale e/o sui backup del Comune per dieci anni, fatte salve eventuali esplicite richieste delle Autorità competenti e/o salvo che vi siano elementi che inducano il Comune stesso a ritenere necessario un periodo di conservazione più lungo (ad esempio, per finalità di giustizia), anche in seguito ad un'eventuale valutazione di impatto ai sensi e per gli effetti dell'art. 35 del GDPR.
4. Il traffico internet sarà cancellato dal Comune periodicamente, ogni dodici mesi, fatte salve eventuali esplicite richieste delle Autorità competenti e/o salvo che vi siano elementi che

inducano il Comune stesso a ritenere necessario un periodo di conservazione più lungo (ad esempio, per finalità di giustizia), anche in seguito ad un'eventuale valutazione di impatto ai sensi e per gli effetti dell'art. 35 del GDPR.

10 Disposizioni ulteriori

1. La sicurezza dei sistemi informatici è soggetta a costante evoluzione dovuta al continuo mutare delle minacce informatiche, il che comporta l'adozione di contromisure sempre differenti e specifiche al verificarsi di attacchi o eventi particolari. A tal fine i Sistemi Informativi e Venis informano gli utenti tramite la intranet comunale e/o tramite altri canali circa le ulteriori prescrizioni da osservare da parte degli utenti.

11 Pubblicità

1. Viene data diffusione ai dipendenti dell'approvazione del Regolamento tramite intranet comunale e/o posta elettronica.

12 Osservanza del Regolamento

1. Il mancato rispetto o la violazione delle regole contenute nel Regolamento è perseguibile con provvedimenti disciplinari previsti dal CCNL, ed altresì con le azioni civili e penali previste dalle leggi vigenti, qualora si verifichino gli estremi per la sussistenza della responsabilità civile o penale.