COMUNE DI GALLIO

Provincia di Vicenza

REGOLAMENTO PER LA GESTIONE E L'UTILIZZO DEGLI STRUMENTI INFORMATICI E PRECAUZIONI GENERALI DA ADOTTARE CON RIFERIMENTO PARTICOLARE AL TRATTAMENTO DI DATI PERSONALI CONTENUTI IN ARCHIVI E DOCUMENTI CARTACEI

con allegato **"Piano della sicurezza informatica"**

approvato con deliberazione di Giunta comunale n. 140 del 25.10.2018

INDICE

Premessa

Il presente Regolamento intende fornire ai dipendenti e collaboratori, denominati anche incaricati o utenti, del Comune di Gallio le indicazioni per una corretta e adeguata gestione delle informazioni personali, in particolare attraverso l'uso di sistemi, applicazioni e strumenti informatici dell'Ente (PC, notebook, tablet, smartphone, risorse di rete, e-mail ed altri strumenti con relativi software e applicativi di seguito più semplicemente definiti "Strumenti") messi a disposizione dall'Ente per espletare la prestazione lavorativa. Gli Strumenti, nonché le relative reti dell'Ente a cui è possibile accedere tramite gli stessi, sono domicilio informatico del Comune di Gallio.
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 679/16 sulla protezione dei dati personali.
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 altresì 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.
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.

1 - Oggetto e finalità

Il presente Regolamento è redatto:

- alla luce della 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";
- in attuazione del Regolamento Europeo 679/16 sulla protezione dei dati personali (d'ora in avanti Reg. 679/16 o GDPR);
- ai sensi delle "Linee guida del Garante per posta elettronica e internet" in Gazzetta Ufficiale n. 58 del 10 marzo 2007;
- alla luce dell'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».

La finalità è quella di promuovere in tutto il personale dell'Ente una corretta "cultura informatica" affinché l'utilizzo degli Strumenti informatici e telematici forniti dall'Ente, quali la posta elettronica, internet e i personal computers con i relativi software, sia conforme alle finalità dell'Ente e nel pieno rispetto della legge. Si vuole fornire a tutto il personale le indicazioni necessarie con l'obiettivo principale di evitare il verificarsi di qualsiasi abuso o uso non conforme, muovendo dalla convinzione che la prevenzione dei problemi sia preferibile rispetto alla loro successiva correzione.

2 - Principi generali e riservatezza nelle comunicazioni

2.1 I principi che sono a fondamento del presente Regolamento sono gli stessi espressi nel GDPR, e, precisamente:

a) **Liceità e correttezza**, secondo cui il trattamento di dati personali è lecito solo quando previsto da procedimenti amministrativi che rientrano nelle funzioni istituzionali dell'Ente, quando il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte, o ancora quando il trattamento è necessario per adempiere un obbligo legale a cui è soggetto l'Ente. In tutti gli altri casi l'interessato dovrà aver espresso il proprio consenso (un consenso informato) al trattamento dei propri dati.
b) **Trasparenza**, secondo cui devono essere trasparenti le modalità con cui sono raccolti e utilizzati i dati personali e devono essere facilmente accessibili e comprensibili le informazioni e comunicazioni relative al trattamento (identità del titolare del trattamento, finalità del trattamento, diritti degli interessati…).
c) **Limitazione delle finalità**, secondo cui i dati personali devono essere raccolti per finalità determinate, esplicite e legittime e successivamente devono essere trattati in una modalità che sia compatibile con tali finalità. Il trattamento dei dati per finalità diverse da quelle per le quali sono stati inizialmente raccolti è consentito solo se compatibile con tali iniziali finalità.
d) **Minimizzazione dell'uso**, secondo cui i dati personali devono essere sempre adeguati, pertinenti e limitati a quanto necessario per il perseguimento delle finalità per cui sono raccolti e trattati.
e) **Esattezza**, secondo cui i dati personali devono essere sempre esatti e aggiornati. Eventuali inesattezze devono essere tempestivamente rettificate ovvero i dati inesatti devono essere cancellati.
f) **Limitazione della conservazione**, secondo cui i dati devono essere conservati per il tempo necessario al raggiungimento delle finalità per le quali sono trattati. Valgono in ogni caso le disposizioni legislative e regolamentari in materia di documentazione amministrativa ed è poi possibile l'ulteriore trattamento ai fini di archiviazione nel pubblico interesse o di ricerca scientifica o storica o a fini statistici.

2.2 Il dipendente si attiene alle seguenti **regole di trattamento**:

a) È vietato comunicare a soggetti non specificatamente autorizzati i dati personali, gli elementi e le informazioni dell'Ente dei quali il dipendente/collaboratore viene a conoscenza nell'esercizio delle proprie funzioni e mansioni all'interno dell'Ente. In caso di dubbio, è necessario accertarsi che il soggetto cui devono essere comunicati i dati sia o meno autorizzato a riceverli, mediante richiesta preventiva al proprio Responsabile di settore.
b) È vietata l'estrazione di originali e/o copie cartacee ed informatiche per uso personale di documenti, manuali, fascicoli, lettere, data base e quant'altro.
c) È vietato lasciare incustoditi documenti, lettere, fascicoli, appunti e quant'altro possa contenere dati personali e/o informazioni dell'Ente quando il dipendente/collaboratore si allontana dalla postazione di lavoro. È vietato lasciare sulla postazione di lavoro (scrivania, bancone ecc.) materiali che non siano inerenti la pratica che si sta trattando in quel momento. Ciò vale soprattutto nel caso di lavoratori con mansioni di front office.
d) Per le riunioni e gli incontri con utenti, cittadini, fornitori, consulenti e collaboratori dell'Ente è necessario porre particolare attenzione alla riservatezza, utilizzando apposite sale dedicate e/o evitando la presenza di soggetti non interessati.

3 - Tutela del lavoratore

3.1 Alla luce dell'art. 4, comma 1, L.n. 300/1970, la regolamentazione della materia indicata nell'art. 1 del presente Regolamento, 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 sistemi informativi per fare fronte ad esigenze produttive od organizzative e di sicurezza nel trattamento dei dati personali.
3.2 È garantito al singolo lavoratore il controllo sui propri dati personali secondo quanto previsto dagli articoli 15-16-17-18-20-21-78 del Reg. 679/16.

4 - Campo di applicazione

4.1 Il presente regolamento si applica a tutti i dipendenti, senza distinzione di ruolo e/o di livello, nonché a tutti i collaboratori dell'Ente a prescindere dal rapporto contrattuale con lo stesso intrattenuto.
4.2 Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche e telematiche, per "utente" deve intendersi ogni dipendente e collaboratore in possesso di specifiche credenziali di autenticazione. Tale figura potrà anche venir indicata come "incaricato del trattamento".

5 - Gestione, assegnazione e revoca delle credenziali di accesso

5.1 Le credenziali di autenticazione per l'accesso alle risorse informatiche vengono assegnate dall'Amministratore di Sistema, previa formale richiesta (come da modello di cui all'**Allegato A**) del Responsabile di settore nell'ambito del quale verrà inserito ed andrà ad operare il nuovo utente. Nel caso di collaboratori esterni la richiesta dovrà essere inoltrata direttamente dal Responsabile di settore con il quale il collaboratore si coordina nell'espletamento del proprio incarico. La richiesta di attivazione delle credenziali dovrà essere completa di generalità dell'utente ed elenco dei sistemi informativi per i quali deve essere abilitato l'accesso. Ogni successiva variazione delle abilitazioni di accesso ai sistemi informativi dovrà essere richiesta formalmente all' Amministratore di Sistema dal Responsabile di riferimento.
5.2 Le credenziali di autenticazioni consistono in un codice per l'identificazione dell'utente (altresì nominati username, nome utente o user id), assegnato dall'Amministratore di Sistema, ed una relativa password. La password è personale e riservata e dovrà essere conservata e custodita dall'incaricato con la massima diligenza e non divulgata.
5.3 La password deve essere di adeguata robustezza: deve essere composta da almeno 8 caratteri, formata da lettere maiuscole e minuscole e/o numeri. Non deve contenere riferimenti agevolmente riconducibili all'utente (username, nomi o date relative alla persona o ad un famigliare).
5.4 È necessario procedere alla modifica della password a cura dell'utente al primo accesso e, successivamente, almeno ogni sei mesi. Nel caso in cui l'utente svolga mansioni che, in astratto, possano comportare il trattamento di dati particolari e/o giudiziari, è obbligatorio il cambio password almeno ogni tre mesi.
5.5 Nel caso di cessazione del rapporto di lavoro con il dipendente/collaboratore, il Responsabile dell'Ufficio/area di riferimento dovrà comunicare formalmente e preventivamente all'Amministratore di Sistema la data effettiva a partire dalla quale le credenziali saranno disabilitate utilizzando il medesimo modello di cui all'**Allegato A**.

PASSWORD

Il più semplice metodo per l'accesso illecito a un sistema consiste nell'indovinare la password dell'utente legittimo. In molti casi sono stati procurati seri danni al sistema informativo a causa di un accesso protetto da password "deboli". La scelta di password "forti" è, quindi, parte essenziale della sicurezza informatica.

COSA NON FARE:

NON dite a nessuno la Vostra password. Ricordate che lo scopo principale per cui usate una password è assicurare che nessun altro possa utilizzare le Vostre risorse o possa farlo a Vostro nome.

NON scrivete la password da nessuna parte che possa essere letta facilmente, soprattutto vicino al computer. Quando immettete la password NON fate sbirciare a nessuno quello che state battendo sulla tastiera.

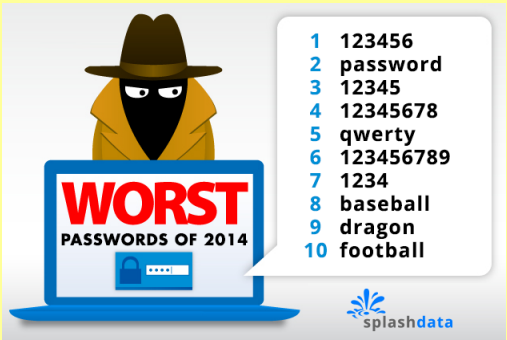
NON usate come password:

a. nomi, cognomi o loro parti;
b. lo username assegnato;
c. un indirizzo di posta elettronica;
d. parole comuni, anche il lingua straniera;
e. date, mesi dell'anno, giorni della settimana, anche il lingua straniera;
f. parole banali e/o di facile intuizione, ad es. pippo, security, password e palindromi (radar);
g. ripetizioni di sequenze di caratteri (es. abcabcabc, qwertyui, 12345678);
h. una password già impiegata in precedenza.

COSA FARE: regole per la corretta gestione delle password

a. La password assegnata è personale e segreta e non va mai comunicata ad altri.
b. Occorre cambiare immediatamente una password non appena si abbia il dubbio che sia diventata poco "sicura".
c. Le password devono essere lunghe almeno 8 caratteri e devono contenere anche lettere maiuscole, caratteri speciali come, ad esempio: | \ ! " £ $ % & / ( ) = ? ^ * + [ ] - _ , ; . : -
d. Le password non devono essere memorizzate su alcun tipo di supporto, quali, ad esempio, post-it (sul monitor o sotto la tastiera) o agende (cartacee, posta elettronica, telefono cellulare).
e. Le password devono essere sostituite almeno nei tempi indicati dalla normativa, a prescindere dall'esistenza di un sistema automatico di richiesta di aggiornamento password.
f. Evitare di digitare la propria password in presenza di altri soggetti che possano vedere la tastiera, anche se collaboratori o dipendenti dell'ente.

La password ideale deve essere complessa, senza alcun riferimento, ma facile da ricordare. Una possibile tecnica è usare una sequenza di caratteri priva di senso evidente, ma con singoli caratteri che formano una frase facile da memorizzare (es: "NlMzz5DlCmm!", Nel Mezzo Del Cammin, più il carattere 5 e il punto esclamativo). Decifrare una parola come questa può richiedere giorni, una come "radar" meno di dieci secondi. Alcuni esempi di password assolutamente da evitare:



a. se Username = "mario.rossi", password = "mario", o ancora peggio, password = "mariorossi";
b. il nome della moglie/marito, fidanzato/a, figli, anche al rovescio;
c. la propria data di nascita, quella del coniuge ecc.;
d. la targa della propria auto;
e. il proprio numero di telefono, quello del coniuge ecc.;
f. parole comuni tipo "Password", "Querty", "12345678", "87654321" (troppo facili);
g. qualsiasi parola del vocabolario di qualsiasi lingua diffusa (italiano, inglese ecc.).

6 - Utilizzo della rete LAN

6.1 Per l'accesso alle risorse informatiche del Comune di Gallio attraverso la rete locale, ciascun utente deve essere in possesso di credenziali di autenticazione secondo l'art. 5.

6.2 È proibito accedere alla rete e nei sistemi informativi utilizzando credenziali di altre persone.

6.3 L'accesso alla rete garantisce all'utente la disponibilità di condivisioni di rete (cartelle area documentale su server) nelle quali vanno inseriti e salvati i files di lavoro, organizzati per area/ufficio o per diversi criteri o per obiettivi specifici di lavoro. Tutte le cartelle di rete, siano esse condivise o personali, possono ospitare esclusivamente contenuti professionali. Pertanto è vietato il salvataggio sui server dell'Ente, ovvero sugli Strumenti, di documenti di carattere personale e non inerenti l'attività lavorativa. Eventuale materiale di carattere personale rilevato dall'Amministratore

di Sistema a seguito di interventi di sicurezza informatica ovvero di manutenzione/aggiornamento su server ed anche su Strumenti potrà essere viene rimosso secondo le regole previste nel successivo punto 12 del presente Regolamento, ferma ogni ulteriore responsabilità civile, penale e disciplinare. Tutte le risorse di memorizzazione, diverse da quelle citate al punto precedente, non sono sottoposte al controllo regolare degli Amministratori di Sistema e non sono oggetto di backup periodici. A titolo di esempio e non esaustivo si citano: il disco C o altri dischi locali dei singoli PC, la cartella "Documenti" o "Desktop" dell'utente, gli eventuali dispositivi di memorizzazione locali o di disponibilità personale come Hard disk portatili o NAS ad uso esclusivo. Pertanto tutti i dati di interesse dell'Ente dovranno essere conservati nelle apposite cartelle di rete condivise dell'area documentale sottoposte a manutenzione periodica e processi di backup pianificati. Sulle restanti risorse di memorizzazione sopra indicate non sono garantite la sicurezza e la protezione contro la eventuale perdita di dati. Pertanto la responsabilità dei salvataggi dei dati ivi contenuti è a carico del singolo utente.

6.4 Senza il consenso del Responsabile di settore, è vietato trasferire documenti elettronici dai sistemi informativi e Strumenti dell'Ente a dispositivi esterni (hard disk, chiavette, CD, DVD e altri supporti).

6.5 Senza il consenso del Responsabile di settore è vietato trasferire documenti elettronici dell'Ente (ad esempio pervenuti via mail o salvati sul Server o sullo Strumento in dotazione) su repository esterne (quali ad esempio Dropbox, GoogleDrive, OneDrive, ecc.) ovvero inviandoli a terzi via posta elettronica o con altri sistemi al di fuori delle normale attività lavorativa.

6.6 Con regolare periodicità (almeno una volta al mese), ciascun utente provvede alla pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati, essendo infatti necessario evitare un'archiviazione ridondante.

6.7 Il Comune di Gallio mette a disposizione dei propri utenti la possibilità di accedere alle proprie risorse informatiche anche dall'esterno dei confini dell'Ente, mediante rete VPN (Virtual Private Network), un canale privato e criptato verso la rete interna. L'accesso mediante VPN viene concesso a consulenti, professionisti, tecnici e fornitori che nell'ambito di un rapporto contrattuale con l'Ente necessitino di accedere a determinate risorse informatiche. Viene concesso, altresì, a dipendenti e funzionari del Comune di Gallio che necessitino di svolgere compiti specifici, pur non essendo presenti in sede. Le richieste di abilitazione all'accesso mediante VPN dovranno seguire le prescrizioni del punto 5 utilizzando il modello apposito di cui all'**Allegato B**.

6.8 All'interno delle sedi del Comune possono essere rese disponibili anche reti senza fili, c.d. "Wi-Fi". Tali reti consentono l'accesso alle risorse dell'Ente e ad internet per i dispositivi non connessi alla rete LAN mediante cavo. L'accesso mediante rete Wi-Fi viene concesso a consulenti, professionisti, tecnici e fornitori che nell'ambito di un rapporto contrattuale con l'Ente necessitino di accedere a determinate risorse informatiche. Viene concesso, altresì, a dipendenti e funzionari del Comune che necessitino di svolgere compiti specifici che non possono essere svolti dalle postazioni fisse. Le richieste di fruizione dei canali "Wi-Fi" interne alle sedi dell'Ente devono essere presentate all'Amministratore di Sistema mediante il modulo di cui all'**Allegato C**, appositamente sottoscritto dal responsabile di settore competente per il dipendente o per il personale esterno.

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

I log relativi all'uso del File System e della intranet dell'Ente, nonché i file salvati o trattati su Server o Strumenti, sono registrati e possono essere oggetto di controllo da parte del Titolare del trattamento, attraverso l'Amministratore di Sistema, per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio dell'Ente.

I controlli possono avvenire secondo le disposizioni previste al successivo punto 12 del presente Regolamento.

Le informazioni così raccolte sono altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, compresa la verifica del rispetto del presente Regolamento, che costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli ai sensi del Regolamento Europeo 679/16 "General Data Protection Regulation".

7 - Utilizzo degli Strumenti elettronici (PC, notebook e altri strumenti con relativi software e applicativi)

7.1 Il dipendente/collaboratore è consapevole che gli Strumenti forniti sono di proprietà del Comune di Gallio e devono essere utilizzati esclusivamente per espletare la prestazione lavorativa. Ognuno è responsabile dell'utilizzo delle dotazioni informatiche assegnate. Ogni utilizzo non inerente all'attività lavorativa è vietato in quanto può comportare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. Ciascun dipendente/collaboratore si deve quindi attenere alle seguenti regole di utilizzo degli Strumenti.

7.2 L'accesso agli Strumenti dell'Ente è protetto da password; per l'accesso devono essere utilizzati Username e password assegnate dall'Amministratore di Sistema (cfr. 5). A tal proposito si rammenta che essi sono strettamente personali e l'utente è tenuto a conservarli nella massima segretezza.

7.3 Tutti gli Strumenti assegnati in uso devono essere custoditi con cura da parte degli incaricati evitando ogni possibile forma di danneggiamento e segnalando tempestivamente al personale dell'Ufficio CED/Responsabile di settore ogni malfunzionamento e/o danneggiamento. Non è consentita l'attivazione della password d'accensione (BIOS), senza preventiva autorizzazione scritta da parte dell'Amministratore di Sistema.

7.4 Non è consentito all'utente modificare le caratteristiche hardware e software impostate sugli Strumenti assegnati, salvo preventiva autorizzazione scritta da parte dell'Amministratore di Sistema.

7.5 L'utente è tenuto a scollegarsi dal sistema, o bloccare l'accesso, ogni qualvolta sia costretto ad assentarsi dal locale nel quale è ubicata la stazione di lavoro (PC) o nel caso ritenga di non essere in grado di presidiare l'accesso alla medesima: lasciare un PC 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.

7.6 Le informazioni archiviate sul PC locale non sono sottoposte a processi di backup e la loro gestione è demandata all'utente

7.7 L'utente utilizzatore dovrà provvedere a memorizzare sulle cartelle condivise dell'Area Documentale dell'Ente dati che possono essere utilizzati anche da altri utenti, evitando di mantenere l'esclusività su di essi.

7.8 Gli operatori dell'Ufficio CED o l'Amministratore di sistema possono in qualunque momento procedere alla rimozione di ogni file o applicazione che riterranno essere pericolosi per la sicurezza dei PC, della rete locale e dei server dell'Ente, nonché tutte le impostazioni eventualmente configurate che possano interferire con il corretto funzionamento dei servizi informatici dell'Ente.

7.9 È obbligatorio consentire l'installazione degli aggiornamenti di sistema che vengono proposti automaticamente, al primo momento disponibile, in modo tale da mantenere il PC sempre protetto.

7.10 È vietato utilizzare il PC per l'acquisizione, la duplicazione e/o la trasmissione illegale di opere protette da copyright.

7.11 È vietato l'utilizzo di supporti di memoria (chiavi USB, CD, DVD o altri supporti) per il salvataggio di dati trattati tramite gli Strumenti Dell'Ente, salvo che il supporto utilizzato sia stato

autorizzato per iscritto dall'Ufficio CED o dall'Amministratore di sistema. In tale caso, il supporto fornito può essere utilizzato esclusivamente per finalità lavorative.
7.12 È vietato connettere al PC qualsiasi periferica esterna senza una preventiva autorizzazione dall'Amministratore di Sistema.
7.13 È vietato connettere alla rete locale qualsiasi dispositivo (PC esterni, router, switch, etc.) senza una preventiva autorizzazione dall'Amministratore di Sistema.
7.14 Nel caso in cui l'utente dovesse notare comportamenti anomali del PC, l'utente stesso è tenuto a comunicarlo tempestivamente all'Ufficio CED o all'Amministratore di sistema.
I log relativi all'utilizzo di Strumenti, reperibili nella memoria degli Strumenti stessi ovvero sui Server o sui router dell'Ente, nonché i file con essi trattati sono registrati e possono essere oggetto di controllo da parte del Titolare del trattamento, attraverso l' Amministratore di sistema, per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio dell'Ente.
I controlli possono avvenire secondo le disposizioni previste al successivo punto 12 del presente Regolamento.
Le informazioni così raccolte sono altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, compresa la verifica del rispetto del presente Regolamento, che costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli ai sensi del Regolamento Europeo 679/16 "General Data Protection Regulation".

8 - Utilizzo di Internet

Le regole di seguito specificate sono adottate anche ai sensi delle "Linee guida del Garante per posta elettronica e internet" pubblicate in Gazzetta Ufficiale n. 58 del 10 marzo 2007.
Ciascun dipendente /collaboratore si deve attenere alle seguenti regole di utilizzo della rete Internet e dei relativi servizi.
8.1 È ammessa solo la navigazione in siti considerati correlati con la prestazione lavorativa.
8.2 È vietato compiere azioni che siano potenzialmente in grado di arrecare danno all'Ente estranee all'attività lavorativa.
8.3 È vietato a chiunque il download di qualunque tipo di software gratuito (freeware) o shareware prelevato da siti Internet senza una preventiva autorizzazione dall'Amministratore di Sistema.
8.4 L'Ente si riserva di bloccare l'accesso a siti "a rischio" attraverso l'utilizzo di blacklist pubbliche in continuo aggiornamento e di predisporre filtri, basati su sistemi euristici di valutazione del livello di sicurezza dei siti web remoti, tali da prevenire operazioni potenzialmente pericolose o comportamenti impropri. In caso di blocco accidentale di siti di interesse dell'Ente, contattare l'Amministratore di sistema per uno sblocco selettivo ed inserimento in white list.
8.5 Nel caso in cui, per ragioni di servizio, si necessiti di una navigazione libera da filtri è necessario richiedere lo sblocco all'Amministratore di sistema, e all'Ufficio CED, nella quale siano indicati chiaramente: motivo della richiesta, utente e postazione da cui effettuare la navigazione libera, intervallo di tempo richiesto per completare l'attività. L'utente, nello svolgimento delle proprie attività, deve comunque tenere presente in modo particolare i punti 13 e 14 del presente regolamento. Al termine dell'attività saranno ripristinarti i filtri nella situazione iniziale.
8.6 È vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, salvo i casi direttamente autorizzati dal Responsabile di settore, con il rispetto delle normali procedure di acquisto.
8.7 È vietato l'utilizzo di abbonamenti privati per effettuare la connessione a Internet tranne in casi del tutto eccezionali e previa autorizzazione scritta dell'Amministratore di Sistema e dell'Ufficio CED.

8.8 È vietata la partecipazione a Forum non professionali, ai Social Network, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames).
8.9 È consentito l'uso di strumenti di messaggistica istantanea, per permettere una efficace e comoda comunicazione tra i colleghi, mediante i soli strumenti autorizzati. Tali strumenti hanno lo scopo di migliorare la collaborazione tra utenti aggiungendo un ulteriore canale comunicativo rispetto agli spostamenti fisici, alle chiamate telefoniche ed e-mail. È consentito un utilizzo legato esclusivamente a scopi professionali. Anche su tali strumenti di messaggistica istantanea è attivo il monitoraggio e la registrazione dell'attività degli utenti, secondo le disposizioni dei punti 13 e 14 del presente regolamento.
8.10 Per motivi tecnici e di buon funzionamento del sistema informatico è buona norma, salvo comprovata necessità, non accedere a risorse web che impegnino in modo rilevante banda, come a titolo esemplificativo: filmati (tratti da youtube, siti di informazione, siti di streaming ecc) o web radio, in quanto possono limitare e/o compromettere l'uso della rete agli altri utenti.
Si informa che l'Ente, per il tramite dell'Amministratore di sistema, 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, l'Ente può registrare per ***180 giorni*** *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 e motivata urgenza rispetto alle finalità sopra descritte, l'Ente può trattare i dati di navigazione riferendoli specificatamente ad un singolo nome utente.
In tali casi i controlli avverranno nelle forme indicate al successivo punto 12 del presente Regolamento.
Le informazioni così raccolte sono altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, compresa la verifica del rispetto del presente Regolamento, che costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli ai sensi del Regolamento Europeo 679/16 "General Data Protection Regulation".

9 - Utilizzo della posta elettronica

Le regole di seguito specificate sono adottate anche ai sensi delle "Linee guida del Garante per posta elettronica e internet" pubblicate in Gazzetta Ufficiale n. 58 del 10 marzo 2007.
Ciascun dipendente/collaboratore si deve attenere alle seguenti regole di utilizzo dell'indirizzo di Posta elettronica.
9.1 Ad ogni utente viene fornito un account e-mail dell'Ente nominativo. L'utilizzo dell'e-mail deve essere limitato esclusivamente a scopi dell'Ente, ed è assolutamente vietato ogni utilizzo di tipo privato. L'utente a cui è assegnata una casella di posta elettronica è responsabile del corretto utilizzo della stessa.
9.2 L'Ente può fornire altresì caselle di posta elettronica associate a ciascuna unità organizzativa, ufficio o gruppo di lavoro (caselle impersonali) che saranno gestite di volta in volta in relazione alle esigenze organizzative dell'ufficio.
9.3 L'iscrizione a mailing-list o newsletter esterne con il proprio indirizzo dell'Ente personale è concessa esclusivamente per motivi professionali. Prima di iscriversi occorre verificare anticipatamente l'affidabilità del sito che offre il servizio.
9.4 Allo scopo di garantire la sicurezza della rete dell'Ente, evitare di aprire messaggi di posta in arrivo da mittenti di cui non si conosce l'identità o con contenuto sospetto o insolito, oppure che

contengano allegati di tipo ***.exe, *.com, *.vbs, *.htm, *.scr, *.bat, *.js e *.pif**. È necessario porre molta attenzione, inoltre, alla credibilità del messaggio e del mittente per evitare casi di phishing o frodi informatiche. In qualunque situazione di incertezza contattare l'Ufficio CED o l'Amministratore di sistema per una valutazione dei singoli casi.

9.5 Non è consentito diffondere messaggi del tipo "catena di S. Antonio" o di tipologia simile anche se il contenuto sembra meritevole di attenzione; in particolare gli appelli di solidarietà e i messaggi che informano dell'esistenza di nuovi virus. In generale è vietato l'invio di messaggi pubblicitari di prodotti di qualsiasi tipo.

9.6 Nel caso fosse necessario inviare allegati "pesanti" (sopra i 10 MB) è opportuno ricorrere prima alla compressione dei file originali in un archivio di formato .zip o equivalenti. Nel caso di allegati ancora più voluminosi è necessario rivolgersi all'Ufficio CED per identificare modalità di trasmissione più adeguate.

9.7 Nel caso in cui fosse necessario inviare a destinatari esterni messaggi contenenti allegati con dati personali o dati personali sensibili, è obbligatorio che questi allegati vengano preventivamente resi inintelligibili attraverso criptazione con apposito software (archiviazione e compressione con password). La password di criptazione deve essere comunicata al destinatario attraverso un canale diverso dalla mail (ad esempio per lettera o per telefono) e mai assieme ai dati criptati. Tutte le informazioni dell'Ente, i dati personali e/o sensibili di competenza dell'Ente possono essere inviati soltanto a destinatari (persone, imprese o Enti) qualificati e competenti.

9.8 Non è consentito l'invio automatico di e-mail all'indirizzo e-mail privato (attivando per esempio un "inoltro" automatico delle e-mail in posta in arrivo)

9.9 In caso di assenza (es. ferie, malattia, infortunio ecc.) è raccomandabile utilizzare un messaggio "Fuori sede" facendo menzione di chi, all'interno dell'Ente, assumerà le mansioni durante l'assenza, oppure indicando un indirizzo di mail alternativo preferibilmente di tipo collettivo. Rivolgersi all'Ufficio CED per tale eventualità o gestirla direttamente tramite la propria Webmail previa comunicazione all'Ufficio Ced

9.10 La diffusione massiva di messaggi di posta elettronica deve essere effettuata esclusivamente per motivi inerenti al servizio, possibilmente su autorizzazione del Responsabile di settore competente. Per evitare che le eventuali risposte siano inoltrate a tutti, generando traffico eccessivo ed indesiderato, i destinatari dovranno essere messi in copia nascosta (Bcc o Ccn) se la tipologia del messaggio lo consente.

9.11 È vietato inviare posta elettronica in nome e per conto di un altro utente, salvo sua espressa autorizzazione;

9.12 La casella di posta elettronica personale deve essere mantenuta in ordine, cancellando messaggi e documenti la cui conservazione non è più necessaria. Anche la conservazione di messaggi con allegati pesanti è da evitare per quanto possibile, preferendo, in alternativa, il salvataggio dell'allegato sulle condivisioni dell'Ente.

9.13 I messaggi in entrata vengono sistematicamente analizzati alla ricerca di virus e malware e per l'eliminazione dello spam. I messaggi che dovessero contenere virus vengono eliminati dal sistema.

Si informa che le comunicazioni anche elettroniche ed i documenti elettronici allegati possono avere rilevanza procedimentale e pertanto devono essere conservate per la durata prevista dalla normativa vigente.

Si informa altresì che l'Ente, per il tramite dell'Amministratore di sistema, non controlla sistematicamente il flusso di comunicazioni mail né è dotato di sistemi per la lettura o analisi sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio e-mail.

Tuttavia, in caso di assenza improvvisa o prolungata del dipendente ovvero per imprescindibili esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio

dell'Ente ovvero per motivi di sicurezza del sistema informatico, l'Ente per il tramite dell'Amministratore di sistema può, secondo le procedure indicate successivo punto 12 del presente Regolamento, accedere all'account di posta elettronica dell'Ente, prendendo visione dei messaggi, salvando o cancellando file.
Si informa che, in caso di cessazione del rapporto lavorativo, la mail dell'Ente affidata all'incaricato verrà sospesa per un periodo di 6 mesi e successivamente disattivata. Nel periodo di sospensione l'account rimarrà attivo e visibile ad un soggetto incaricato dall'Ente solo in ricezione, che tratterà i dati e le informazioni pervenute per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio dell'Ente, trasmettendone il contenuto ad altri dipendenti (se il messaggio ha contenuto lavorativo) ovvero cancellandolo (se il messaggio non ha contenuto lavorativo). Il sistema in ogni caso genererà una risposta automatica al mittente, invitandolo ad inviare il messaggio ad altro indirizzo mail dell'Ente.
Le informazioni eventualmente raccolte sono altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, compresa la verifica del rispetto del presente Regolamento, che costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli ai sensi del Regolamento Europeo 679/16 "General Data Protection Regulation".

SICUREZZA E PRIVACY DELLA POSTA ELETTRONICA

Confidenzialità

La confidenzialità della posta elettronica e della comunicazione attraverso il Web è limitata in quanto i messaggi, transitando nella rete pubblica di Internet, possono essere visionati da terzi non autorizzati. Il livello di confidenzialità di una e-mail si avvicina di più a quello di una cartolina piuttosto che a quello di una lettera. Per questa ragione è fatto divieto assoluto di comunicare informazioni classificate come riservate o dati particolari attraverso l'e-mail o attraverso il Web se non esplicitamente autorizzati dal Titolare del trattamento o da un Responsabile preposto.

Attendibilità

L'attendibilità dell'identità del mittente è molto limitata nella comunicazione via e-mail. E' relativamente facile, infatti, camuffare il mittente di una e-mail. Si richiede pertanto, ogni qual volta sia necessaria la certezza dell'identità del mittente, di verificarla con mezzi appropriati.
L'attendibilità della data ed ora esatta di invio di una e-mail è molto limitata. E' relativamente facile, infatti, modificare questi dati. Si richiede pertanto, ogni qual volta sia necessaria la certezza della data e dell'ora del messaggio, di verificarle con i mezzi appropriati.

Contenuto dei messaggi

Gli utenti devono assicurarsi che nei loro messaggi elettronici non siano inserite inconsapevolmente informazioni su User e Password utilizzate per accedere ad altre applicazioni. In particolare va usata la massima cautela nell'invio a mezzo posta elettronica di pagine internet che potrebbero contenere nell'indirizzo informazioni utili a risalire alla User/Password utilizzata.
Gli utenti sono invitati a nominare correttamente i nomi dei file allegati alle e-mail, specificando, nel caso si procedesse ad inviare documenti soggetti a modifiche e revisioni, la versione corrente del file con dei numeri progressivi.
Gli utenti sono invitati a prestare attenzione nell'utilizzo della funzione "Rispondi" e "Rispondi a tutti" nel caso il messaggio originario sia stato inviato ad un numero elevato di destinatari.
Per la trasmissione di file all'interno è possibile utilizzare la posta elettronica, prestando attenzione alla dimensione degli allegati. È obbligatorio controllare i file attachements di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).
È vietato rispondere ad e-mail di spam, in quanto una eventuale risposta conferma, a specifici programmi, l'esistenza della casella e-mail a ricevere posta, quindi altro spam.

Altri consigli per l'utilizzo della posta elettronica

Gli utenti sono invitati a leggere quotidianamente la posta elettronica e a rispondere in tempi ragionevoli alle e-mail ricevute.
Gli utenti sono invitati a scrivere i propri messaggi di posta elettronica in plain text, qualora non si siano previamente accertati che il destinatario è provvisto di un client di posta in grado di supportare la lettura di altri formati.
Si invitano gli utenti che hanno selezionato l'opzione di completamento automatico dell'indirizzo di prestare molta attenzione nella selezione dei destinatari.
Gli utenti devono periodicamente cancellare o organizzare in opportune cartelle la posta già letta. Una quantità troppo elevata di e-mail nella cartella predefinita di arrivo della nuova posta può compromettere sensibilmente la stabilità del programma di posta.

Gli utenti devono sempre indicare con chiarezza (nel campo oggetto), l'argomento del proprio messaggio. E' possibile richiedere una ricevuta di corretto ricevimento della propria mail. A tale ricevuta va tuttavia assegnata una importanza relativa poiché talvolta la conferma della ricezione avviene ad opera del mail server centrale e non del destinatario ultimo del messaggio.

10 - Utilizzo dei telefoni, fax, fotocopiatrici, scanner e stampanti dell'Ente

Il dipendente è consapevole che gli Strumenti di stampa, così come anche il telefono dell'Ente, sono di proprietà del Comune di Gallio e sono resi disponibili all'utente per rendere la prestazione lavorativa. Pertanto ne viene concesso l'uso esclusivamente per tale fine.

10.1 Il telefono dell'Ente 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.

10.2 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 (cfr. 7 "Utilizzo di Strumenti elettronici"), 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 (cfr. 8), se consentita.

10.3 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 dall'Ufficio CED.

10.4 È vietato l'utilizzo delle fotocopiatrici dell'Ente per fini personali, salvo preventiva ed esplicita autorizzazione da parte del Responsabile di settore.

10.5 Per quanto concerne l'uso delle stampanti gli utenti sono tenuti a:

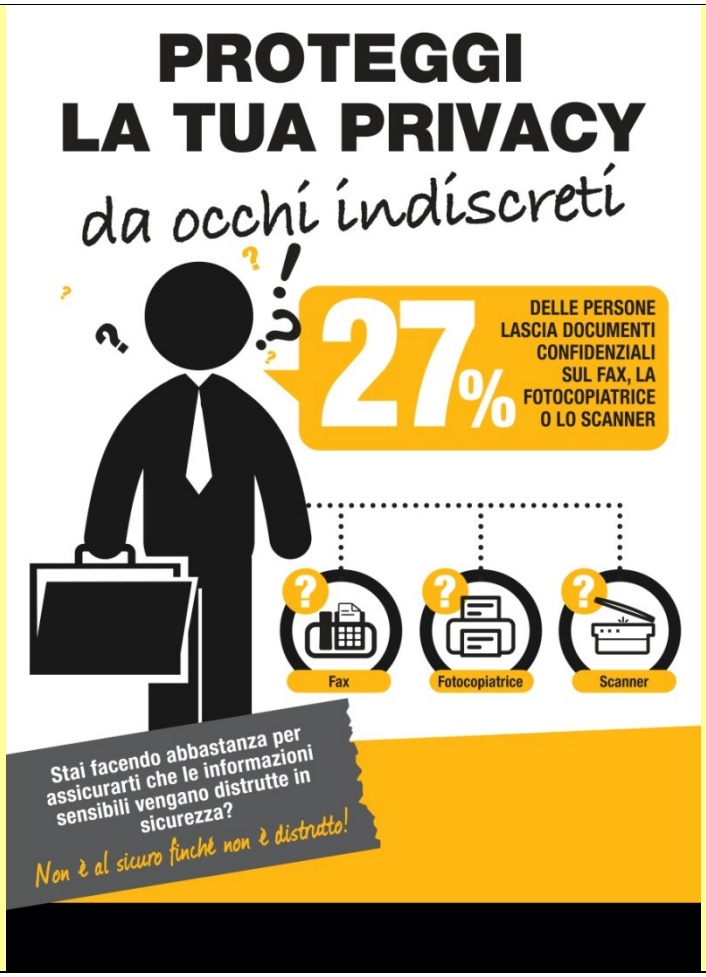
a) Stampare documenti solo se strettamente necessari per lo svolgimento delle proprie funzioni operative,
b) Prediligere le stampanti di rete condivise, rispetto a quelle locali/personali, per ridurre l'utilizzo di materiali di consumo (toner ed altri consumabili),
c) Prediligere la stampa in bianco/nero e fronte/retro al fine di ridurre i costi, se possibile.
d) Le stampanti e le fotocopiatrici dell'Ente devono essere spente in caso di inutilizzo prolungato.

10.6 Nel caso in cui si rendesse necessaria la stampa di informazioni riservate l'utente dovrà presidiare il dispositivo di stampa per evitare la possibile perdita o divulgazione di tali informazioni e persone terze non autorizzate.

PRECAUZIONI SPECIFICHE PER GLI INCARICATI ADDETTI ALLA DUPLICAZIONE DI DOCUMENTAZIONE

Cura nel disporre dei documenti originali
Gli incaricati preposti alla duplicazione di documentazione o alla sostituzione della documentazione cartacea con registrazione ottica devono prestare attenzione a non dimenticare l'originale del documento all'interno della macchina fotocopiatrice e/o dello scanner.

Distruzione:
La distruzione dei supporti magnetici od ottici, contenti dati, deve avvenire per distruzione fisica dello stesso, mediante abrasione o perforazione. Se disponibili, per i CD/DVD, utilizzare gli appositi strumenti di distruzione.



11 - Assistenza agli utenti e manutenzioni

11.1 L'Ufficio CED e l'Amministratore di sistema possono accedere ai dispositivi informatici dell'Ente sia direttamente, sia mediante software di accesso remoto, per i seguenti scopi:

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

11.2 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 sono autorizzati ad effettuare gli interventi senza il consenso dell'utente cui la risorsa è assegnata.

11.3 L'accesso in teleassistenza sui PC della rete dell'Ente richiesto da terzi (fornitori e/o altri) deve essere autorizzato dall'Ufficio CED, 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.

11.4 Durante gli interventi in teleassistenza da parte di operatori terzi, l'utente richiedente deve presenziare la sessione remota, in modo tale da verificare ed impedire eventuali comportamenti non conformi al presente regolamento.

12 - Controlli sugli Strumenti (art. 6.1 Provv. Garante, ad integrazione dell'Informativa ex art. 13 Reg. 679/16)

12.1 Poiché in caso di violazioni contrattuali e giuridiche, sia l'Ente, sia il singolo lavoratore sono potenzialmente perseguibili con sanzioni, anche di natura penale, l'Ente verificherà, nei limiti consentiti dalle norme legali e contrattuali, il rispetto delle regole e l'integrità del proprio sistema informatico. Il datore di lavoro, infatti, può avvalersi legittimamente, nel rispetto dello Statuto dei lavoratori (art. 4, comma2), di sistemi che consentono indirettamente il controllo a distanza (c.d. controllo preterintenzionale) e determinano un trattamento di dati personali riferiti o riferibili ai lavoratori. Resta ferma la necessità di rispettare le procedure di informazione e di consultazione di lavoratori e sindacati in relazione all'introduzione o alla modifica di sistemi automatizzati per la raccolta e l'utilizzazione dei dati, nonché in caso di introduzione o di modificazione di procedimenti tecnici destinati a controllare i movimenti o la produttività dei lavoratori. I controlli devono essere effettuati nel rispetto dell'art. 2.2 del presente Regolamento e 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 Regolamento 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.

12.2 L'uso degli Strumenti Informatici dell'Ente può lasciare traccia delle informazioni sul relativo uso, come analiticamente spiegato nei riquadri di cui ai punti 6 – 7 – 8 – 9 del presente Regolamento. Tali informazioni, che possono contenere dati personali eventualmente anche sensibili dell'Utente, possono essere oggetto di controlli da parte dell'Ente , per il tramite dell'Amministratore di Sistema, volti a garantire esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio dell'Ente, nonché per la sicurezza e la salvaguardia del sistema informatico, per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, etc.). Gli interventi di controllo sono di due tipi (di seguito descritti al punto 12.3 e 12.4) e possono permettere all'Ente di prendere indirettamente cognizione dell'attività svolta con gli strumenti.

12.3 Controlli per la tutela del patrimonio dell'Ente, nonché per la sicurezza e la salvaguardia del sistema informatico. Controlli per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, etc..).

Qualora per le finalità qui sopra descritte risulti necessario l'accesso agli Strumenti e alle risorse informatiche e relative informazioni descritte ai punti 6 – 7 – 8 – 9 il Responsabile del trattamento dei dati personali per il tramite dell'Ufficio CED, si atterrà al processo descritto qui di seguito (se e in quanto compatibile con lo Strumento oggetto di controllo).

I. Avviso generico a tutti i dipendenti della presenza di comportamenti anomali che possono mettere a rischio la sicurezza del sistema informativo e richiamo all'esigenza di attenersi al rispetto del presente Regolamento.
II. Successivamente, dopo almeno 7 giorni, se il comportamento anomalo persiste, l'Ente potrà autorizzare il personale addetto al controllo, potendo così accedere alle informazioni descritte ai punti 6 – 7 – 8 – 9 con possibilità di rilevare files trattati, siti web visitati, software installati, documenti scaricati, statistiche sull'uso di risorse ecc. nel corso dell'attività lavorativa. Tale attività potrà essere effettuata in forma anonima ovvero tramite

controllo dell'indirizzo IP, dell'Utente e con l'identificazione del soggetto che non si attiene alle istruzioni impartite.

III. Qualora il rischio di compromissione del sistema informativo dell'Ente sia imminente e grave a tal punto da non permettere l'attesa dei tempi necessari per i passaggi procedimentali descritti ai punti 1 e 2, il Responsabile del Trattamento, unitamente all'amministratore di sistema, può intervenire senza indugio sullo strumento da cui proviene la potenziale minaccia.

12.4 Controlli per esigenze produttive e di organizzazione. Per esigenze produttive e di organizzazione si intendono – fra le altre – l'urgente ed improrogabile necessità di accedere a files o informazioni lavorative di cui si è ragionevolmente certi che siano disponibili su risorse informatiche di un Utente (quali file salvati, posta elettronica, chat, SMS, ecc) che non sia reperibile, in quanto ad esempio assente, temporaneamente irreperibile ovvero cessato.

Qualora risulti necessario l'accesso alle risorse informatiche e relative informazioni descritte ai punti 6 – 7 – 8 – 9 il Responsabile del trattamento dei dati personali, per il tramite dell'Ufficio CED, si atterrà alla procedura descritta qui di seguito (se e in quanto compatibile con lo Strumento oggetto di controllo).

I. Redazione di un atto da parte del Responsabile di settore che comprovi le necessità produttive e di organizzazione che richiedano l'accesso allo Strumento.
II. Incarico all'Amministratore di sistema 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.
III. Redazione di un verbale che riassuma i passaggi precedenti.
IV. In ogni caso l'accesso ai documenti presenti nella risorsa è limitato a quanto strettamente indispensabile alle finalità produttive e di organizzazione del lavoro.
V. 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 679/16 "GDPR".

Tutti i controlli sopra descritti avvengono nel rispetto del principio di necessità e non eccedenza rispetto alle finalità descritte nel presente Regolamento. Dell'attività sopra descritta viene redatto verbale, sottoscritto dal Responsabile del Trattamento e dall'Amministratore di Sistema che ha svolto l'attività.

In caso di nuovo accesso da parte dell'utente allo Strumento informatico oggetto di controllo, lo stesso dovrà avvenire previo rilascio di nuove credenziali (salvo diverse esigenze tecniche).

13 - Conservazione dei dati

13.1 In riferimento agli articoli 5 e 6 del Reg. 679/16 e 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, salvo esigenze 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.

13.2 L' Ente si impegna ad assumere le misure di sicurezza nel trattamento e nella conservazione di tale tipologia di dati alla luce di quanto stabilito dal Legislatore.

14 - Partecipazioni a Social Media

14.1 L'utilizzo a fini promozionali di Facebook, Twitter, Linkedin, 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.
14.2 Pur garantendo il diritto della persona alla libertà di espressione, l'Ente ritiene comunque opportuno indicare agli utenti alcune regole comportamentali, al fine di tutelare la propria immagine ed il patrimonio, anche immateriale, oltre che gli stessi utenti utilizzatori dei social media, fermo restando che è vietata la partecipazione agli stessi social media durante l'orario di lavoro.
14.3 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.
14.4 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 privacy.

15 - Open Government

15.1 Il Comune di Gallio riconosce ed incoraggia modalità di esercizio delle proprie funzioni basate su modelli, strumenti e tecnologie che consentono all'Amministrazione di essere "aperta" e "trasparente" nei confronti dei cittadini.
15.2 Ferme restando le disposizioni di legge in materia di Open Government l'incaricato dovrà porre particolare attenzione nella pubblicazione e divulgazione di documenti contenenti dati personali, facendo riferimento ai seguenti principi:

- è consentita la diffusione dei soli dati personali la cui inclusione in atti e documenti da pubblicare sia realmente necessaria e proporzionata alla finalità di trasparenza perseguita nel caso concreto (cd. "principi di necessità, pertinenza e non eccedenza"). Di conseguenza, i dati personali che esulano da tale finalità non devono essere inseriti negli atti e nei documenti oggetto di pubblicazione online. In caso contrario, occorre provvedere, comunque, all'oscuramento delle informazioni che risultano eccedenti o non pertinenti.
- è, invece, sempre vietata la diffusione di dati idonei a rivelare lo "stato di salute" (art. 9 del GDPR) e "la vita sessuale" (art. 4, comma 6, del d. lgs. n. 33/2013).

16 - Videosorveglianza

16.1 Il Comune di Gallio utilizza sistemi di videosorveglianza a garanzia dei luoghi pubblici per tutelare persone e beni da aggressioni, furti, rapine, atti di vandalismo etc.
16.2 Ferme restando le disposizioni del Garante della Privacy in materia di Videosorveglianza dovranno essere rispettati i seguenti principi:

- È obbligatorio esporre un avviso ben visibile con un simbolo che segnali la presenza di telecamere ed indichi chiaramente chi effettua la rilevazione delle immagini e per quali scopi.
- Nel caso in cui i sistemi siano attivi durante le ore notturne, i cartelli devono essere opportunamente illuminati.

- Il periodo di conservazione non deve superare le 24 ore, fatte salve esigenze di ulteriore conservazione in relazione a indagini da parte di polizia o magistratura.
- Le immagini possono essere visionate solo da responsabili o incaricati del trattamento dei dati e le forze di polizia.
- Sono vietati la duplicazione e la distruzione ad opera del personale che ha accesso ai dati acquisiti.

17 - Pubblicazione notizie ed eventi sul Portale Web del Comune

17.1 Il Comune di Gallio dispone di un proprio portale web istituzionale per la diffusione di informazioni riguardanti gli Organi di governo dell'Ente, gli Uffici, le Notizie, gli Eventi promossi dall'Amministrazione etc.
17.2 Tutti gli uffici, ognuno per la propria competenza, provvedono a mantenere in efficienza il sito internet del Comune, curandone gli aggiornamenti, i contenuti, la qualità, l'appropriatezza e la correttezza delle informazioni secondo quanto richiesto dall'Amministrazione;

18 - Precauzioni generali da adottare con riferimento particolare al trattamento di dati personali contenuti in archivi e documenti cartacei

18.1 Gli incaricati sono tenuti a custodire e controllare gli atti e i documenti contenenti dati personali, in modo da evitare che persone prive di autorizzazione possano accedere ai dati.
18.2 I documenti contenenti dati personali devono essere conservati in archivi ad accesso controllato e con possibilità di chiusura. Solo il personale autorizzato dovrà averne la possibilità di accesso.
18.3 Tutta la documentazione e le pratiche trattate o da trattare devono essere riposte in armadi chiusi a chiave nel periodo di intervallo meridiano o al termine della giornata lavorativa.
18.4 La protezione dei dati deve essere compiuta dalla loro acquisizione fino all'eventuale distruzione degli stessi e per tutto il ciclo di loro trattamento e conservazione.
18.5 Gli incaricati devono evitare che terzi (non incaricati), possano accedere ai luoghi in cui sono custoditi i dati, quindi devono adottare misure idonee per evitare la visibilità dei dati a terzi.
18.6 Non è possibile effettuare copie su supporti magnetici o trasmissioni non autorizzate di dati oggetto del trattamento.
18.7 Non è possibile effettuare copie fotostatiche o di qualsiasi altra natura, non autorizzate**,** di stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento.
18.8 Non è possibile sottrarre, cancellare, distruggere senza autorizzazione**,** stampe, tabulati, elenchi, rubriche e ogni altro materiale riguardante i dati oggetto del trattamento.
18.9 Sarà cura di ogni incaricato adottare ogni misura possibile al fine di garantire quanto sopra.

TRATTAMENTI SENZA L'AUSILIO DI STRUMENTI ELETTRONICI

1. UTILIZZATE LE CHIAVI!

Il primo livello di protezione di qualunque sistema è quello fisico; è vero che una porta chiusa può in molti casi non costituire una protezione sufficiente, ma è anche vero che pone se non altro un primo ostacolo, e richiede comunque uno sforzo volontario non banale per la sua rimozione. È fin troppo facile per un estraneo entrare in un ufficio non chiuso a chiave e sbirciare i documenti posti su una scrivania; pertanto, chiudete a chiave il vostro ufficio quando l'ultima unità di personale lascia il locale e, comunque, alla fine della giornata e chiudete i documenti a

chiave negli armadi ogni volta che potete.

2. NON COMUNICATE DATI PERSONALI A SOGGETTI NON LEGITTIMATI

L'utilizzo dei dati personali deve avvenire in base al cd "principio di necessità", è cioè essi non devono essere condivisi, comunicati o inviati a persone che non ne necessitano per lo svolgimento delle proprie mansioni lavorative.

I dati non devono essere comunicati all'esterno dell'ente e comunque a soggetti terzi, se non previa autorizzazione.

3. FATE ATTENZIONE A COME DISTRUGGETE I DOCUMENTI

Qualora sia necessario distruggere i documenti contenenti dati personali, questi devono essere distrutti utilizzando gli appositi apparecchi "distruggi documenti" o, in assenza, devono essere sminuzzati in modo da non essere più ricomponibili.

I documenti originali non possono in alcun caso essere distrutti senza la previa autorizzazione della Soprintendenza Archivistica.

4. RADDOPPIATE LE ATTENZIONI SE I DOCUMENTI CONTENGONO DATI PARTICOLARI

I documenti contenenti dati particolari (ex sensibili e/o giudiziari) devono essere controllati e custoditi molto attentamente in modo che non vi accedano persone prive di autorizzazione.

L'archiviazione dei documenti cartacei contenenti dati particolari deve avvenire in locali ad accesso controllato, utilizzando possibilmente armadi o contenitori chiusi a chiave.

Riponete i documenti contenenti dati particolari negli appositi contenitori o armadi al termine delle operazioni affidate e comunque a fine giornata. In ogni caso di allontanamento dal proprio posto di lavoro, documenti devono essere riposti negli armadi o nei cassetti, possibilmente chiusi a chiave.

All'Amministratore di Sistema
Comune di Gallio
Via Roma 2, 36032 Gallio (VI)
E-mail: comune@comune.gallio.vi.it

Il/La sottoscritto/a

Cognome: _____ Nome: _____
Nato/a a: _____ Prov: _____
Nato/a il: _____ Cod.Fiscale: _____

In qualità di *(barrare soltanto **una** delle caselle sotto riportate)*:

- ☐ Dipendente del Comune di Gallio
- ☐ Collaboratore esterno coordinato dal settore/area _____ del _____
- ☐ Dipendente di ditta esterna coordinato dal settore/area _____ del _____

CHIEDE

1) L'assegnazione delle credenziali di accesso per *(barrare le caselle di proprio interesse e riportare nelle note il livello di autorizzazione da assegnare)*:

- ☐ Utente di dominio NOTE:
- ☐ Utente macchina NOTE:
- ☐ E-mail ordinaria istituzionale (@comune.gallio.vi.it) NOTE:
- ☐ Utente GestionePraticheEdilizie NOTE:
- ☐ Utente Halley NOTE:
- ☐ Utente sito istituzionale Comune di Gallio NOTE:
- ☐ Altro *(specificare)*: NOTE:

2) Di ricevere le credenziali richieste:

- ☐ Al seguente indirizzo di posta elettronica ordinaria: _____
- ☐ Al seguente indirizzo di Posta Elettronica Certificata: _____
- ☐ Consegna a mano presso: _____

LUOGO E DATA

FIRMA DEL RICHIEDENTE

_____ _____

LUOGO E DATA

FIRMA DEL RESPONSABILE DEL SETTORE/AREA

_____ _____

La presente richiesta deve essere firmata dal richiedente e dal responsabile del settore/area di riferimento, anche nel caso di collaboratore esterno o Ditta esterna

All'Amministratore di Sistema
Comune di Gallio
Via Roma 2, 36032 Gallio (VI)
E-mail: comune@comune.gallio.vi.it

Il/La sottoscritto/a

Cognome: _____ Nome: _____
Nato/a a: _____ Prov: _____
Nato/a il: _____ Cod.Fiscale: _____

In qualità di (*barrare soltanto **una** delle caselle sotto riportate*)**:**

- ☐ Dipendente del Comune di Gallio
- ☐ Collaboratore esterno coordinato dal settore/area _____ del _____
- ☐ Dipendente di ditta esterna coordinato dal settore/area _____ del _____

CHIEDE

1) L'accesso tramite Virtual Private Network (VPN) ai seguenti servizi/sistemi:

_____
_____
_____
_____

Motivazione: _____

2) Di ricevere le credenziali richieste:

- ☐ Al seguente indirizzo di posta elettronica ordinaria: _____
- ☐ Al seguente indirizzo di Posta Elettronica Certificata: _____
- ☐ A mano presso: _____

DICHIARA DI ESSERE A CONOSCENZA

- che username e la password sono nominali;
- che tutte le operazioni con essi effettuate sono direttamente attribuibili al proprietario delle credenziali stesse;
- che gli accessi e tutte le operazioni effettuate vengono registrati e controllati;
- che utilizzi impropri della suddetta password sono puniti a norma di legge;
- che l'accesso tramite VPN e l'utilizzo del servizio verranno bloccati in caso di utilizzi impropri delle credenziali assegnate, di una loro divulgazione o di un loro smarrimento, come pure in caso di eventuali violazione di legge commesse mediante l'utilizzo delle stesse;
- che il Comune di Gallio non sarà responsabile della divulgazione dei dati e/o delle informazioni o della perdita d'informazioni derivanti da o in qualsiasi modo connessi all'utilizzo non autorizzato dell'infrastruttura del Comune di Gallio;
- che il Comune di Gallio adotta le misure utili a garantire la sicurezza dei dati degli Utenti e che il trattamento dei dati sarà eseguito esclusivamente dai soggetti responsabili del trattamento e/o da Suoi incaricati.

LUOGO E DATA	FIRMA DEL RICHIEDENTE
_____	_____
LUOGO E DATA	FIRMA DEL RESPONSABILE DEL SETTORE/AREA
_____	_____

La presente richiesta deve essere firmata dal richiedente e dal responsabile del settore/area di riferimento, anche nel caso di collaboratore esterno o Ditta esterna

All'Amministratore di Sistema
Comune di Gallio
Via Roma 2, 36032 Gallio (VI)
E-mail: comune@comune.gallio.vi.it

Il/La sottoscritto/a

Cognome: _____ Nome: _____
Nato/a a: _____ Prov: _____
Nato/a il: _____ Cod.Fiscale: _____

In qualità di (*barrare soltanto **una** delle caselle sotto riportate*)**:**

- ☐ Dipendente del Comune di Gallio
- ☐ Collaboratore esterno coordinato dal settore/area _____ del _____
- ☐ Dipendente di ditta esterna coordinato dal settore/area _____ del _____

CHIEDE

1) Di ottenere le credenziali per l'accesso alla connessione wi-fi presente nei locali:

- ☐ _____
- ☐ _____
- ☐ _____

Per il giorno: _____ dalle ore: _____ alle ore: _____

Motivazione: _____

2) Di ricevere le credenziali richieste:

- ☐ Al seguente indirizzo di posta elettronica ordinaria: _____
- ☐ Al seguente indirizzo di Posta Elettronica Certificata: _____
- ☐ Consegna a mano presso: _____

DICHIARA DI ESSERE A CONOSCENZA

- Che le credenziali saranno concesse ed utilizzate dal solo soggetto richiedente limitatamente alla giornata e agli orari sopra indicati e che non saranno cedute a terzi;
- Che il richiedente è direttamente responsabile delle attività svolte durante la connessione in internet tramite il servizio wi-fi;
- In particolare durante l'utilizzo del servizio wi-fi è vietato:
  - Svolgere qualunque attività che sia in contrasto con la normativa italiana ed europea;
  - Accedere a siti che per contenuti ed immagini siano in contrasto con le finalità pubbliche del servizio e/o illegali (ad es. pedofilia, pornografia, violenza, razzismo, ecc.);
  - Inviare messaggi di posta elettronica secondo modalità indiscriminate (spamming)
  - Svolgere qualsiasi attività intesa ad eludere o ingannare i sistemi di controllo di accesso e/o sicurezza di qualsiasi server interno o esterno pubblico o privato;
  - Usare meccanismi o strumenti di qualsiasi natura atti ad eludere i sistemi di protezione da copia abusiva del software, a rivelare password, ad identificare eventuali vulnerabilità della sicurezza dei vari sistemi, a decriptare file crittografati o a compromettere la sicurezza della rete in qualsiasi modo.
- che il richiedente è responsabile di ogni violazione del presente accordo e si impegna a manlevare sostanzialmente e processualmente il Comune di Gallio e a tenerla indenne da qualsiasi pretesa anche di terzi a qualsivoglia titolo, comunque avente causa, dalla violazione del presente accordo e/o dalla violazione di leggi o regolamenti o provvedimenti amministrativi.

- che il servizio di rete wi-fi è fornito mediante l'uso di frequenze in banda condivisa e limitata protezione contro interferenze,e che di conseguenza l'erogazione del servizio e la sua qualità non sono garantite;
- che il gestore del servizio non è in alcun modo responsabile per il contenuto, la qualità, la validità di qualsiasi informazione reperita in rete, né dell'esito di transazioni con particolare riferimento a quelle di natura commerciale con utilizzo di sistemi di pagamento elettronico o tecniche affini che l'utente volesse realizzare;
- di assumersi la responsabilità per le azioni compiute durante l'utilizzo del servizio wi-fi e per il contenuto dei messaggi trasmessi;
- che l'accesso wi-fi prevede una modalità di utilizzo del servizio senza cifratura dei dati. La trasmissione avviene in chiaro e l'accesso non richiede alcuna configurazione particolare. Che tutto ciò determina che gli utenti siano più esposti a pericoli di intercettazione dei dati trasmessi, mettendo potenzialmente a repentaglio la sicurezza e l'integrità degli stessi;
- che l'utente deve adottare le opportune misure di sicurezza e ogni accorgimento atto ad evitare eventuali attacchi alla propria macchina. Nell'ambito dell'utilizzo del servizio, il Comune di Gallio declina ogni responsabilità per qualunque conseguenza derivante dall'utilizzo delle connessioni wifi.

LUOGO E DATA

FIRMA DEL RICHIEDENTE

LUOGO E DATA

FIRMA DEL RESPONSABILE DEL SETTORE/AREA

La presente richiesta deve essere firmata dal richiedente e dal responsabile del settore/area di riferimento, anche nel caso di collaboratore esterno o Ditta esterna

COMUNE DI GALLIO

Provincia di Vicenza

PIANO DELLA SICUREZZA INFORMATICA

allegato al **REGOLAMENTO PER LA GESTIONE E L'UTILIZZO DEGLI STRUMENTI INFORMATICI E PRECAUZIONI GENERALI DA ADOTTARE CON RIFERIMENTO PARTICOLARE AL TRATTAMENTO DI DATI PERSONALI CONTENUTI IN ARCHIVI E DOCUMENTI CARTACEI**

approvato con deliberazione di Giunta comunale n. 140 del 25.10.2018

1 Il piano di sicurezza informatica

1.1 Definizione

Il ricorso alle tecnologie dell'informazione e della comunicazione intrapreso dal Comune per lo snellimento, l'ottimizzazione e una maggiore efficienza dei procedimenti amministrativi comporta una serie di rischi che, se non adeguatamente affrontati, potrebbero comportare gravi conseguenze sull'affidabilità dei dati e dei servizi.
Tali rischi sono imputabili a due fattori caratteristici della tecnologia in questione: la non garanzia di corretto funzionamento sia nelle componenti hardware che in quelle software e l'esposizione alle intrusioni informatiche. In termini più operativi è bene intendere la sicurezza del Sistema Informativo non solo come "protezione del patrimonio informativo da rilevazioni, modifiche o cancellazioni non autorizzate per cause accidentali o intenzionali" ma anche come "limitazione degli effetti causati dall'eventuale occorrenza di tali cause".
Si evidenzia che la sicurezza del Sistema Informativo non dipende solo da aspetti tecnici ma anche, se non principalmente, da quelli organizzativi, sociali e legali. La sicurezza del Sistema Informativo è pertanto vista come caratteristica "globale", in grado di fornire dinamicamente, con l'evolversi temporale delle necessità e delle tecnologie, il desiderato livello di disponibilità, integrità e confidenzialità delle informazioni e dei servizi erogati.
Il presente Piano descrive le misure di sicurezza adottate per la formazione, la gestione, la trasmissione, l'interscambio, l'accesso e la conservazione dei documenti informatici, nel rispetto anche di quanto disposto dal D.Lgs 196/2003, "Codice in materia di protezione dei dati personali", del relativo Allegato B "Disciplinare tecnico in materia di misure minime di sicurezza" e dal Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27.04.2016. Sono elencate inoltre le strategie ed i controlli adottati per assicurare al Sistema Informativo del Comune un adeguato livello di sicurezza.

1.2 Obiettivi

Scopo del presente documento è descrivere la strategia che il Comune intende adottare per poter soddisfare i seguenti requisiti di sicurezza:

- **CONFIDENZIALITÀ**: l'accesso e la divulgazione di informazioni presenti nel sistema, indipendentemente dal formato in cui si trovano, deve poter essere effettuato solo dai soggetti autorizzati. Deve pertanto essere ridotta al minimo la probabilità che un'informazione riservata sia resa pubblica.
- **INTEGRITÀ**: la modifica o la distruzione di informazioni presenti nel sistema, indipendentemente dal formato in cui si trovano, devono poter essere effettuate solo dai soggetti autorizzati. Deve pertanto essere ridotta al minimo la probabilità che l'informazione sia in qualche modo modificata. Devono essere altresì garantiti sia l'origine del dato (non ripudiabilità) che la sua conformità all'originale (autenticità).
- **DISPONIBILITÀ**: l'accesso all'informazione e ai sistemi deve essere sempre affidabile e tempestivo. Una perdita di disponibilità si verifica quando a fronte di un'intrusione un sistema diventa non più accessibile da parte degli utenti.
- **TRACCIABILITÀ**: tutte le azioni che un'entità compie nell'ambito del sistema sono memorizzate in modo tale da poter essere, in tempi successivi, ricondotte in maniera inequivocabile all'entità stessa.

L'adozione di idonee e preventive misure di sicurezza garantisce che il trattamento dei dati personali comuni identificativi, sensibili e/o giudiziari venga effettuato in modo da ridurre al minimo i rischi di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta, in relazione alle conoscenze acquisite in base al progresso tecnico, alla loro natura e alle specifiche caratteristiche del trattamento.
Il Piano per la Sicurezza Informatica si basa attualmente sull'analisi dei rischi a cui è esposto il sistema informatico, i relativi dati e documenti in esso contenuti e sulle direttive strategiche stabilite dal vertice del Comune.
Il presente Piano è soggetto a revisione, in funzione dell'estensione del sistema, dell'evoluzione tecnologica, della variazione degli obiettivi dell'organizzazione e del manifestarsi di nuovi o mutati rischi per la sicurezza. In caso di eventi straordinari il Piano è soggetto ad una revisione estemporanea.

2 Il Sistema Informativo Comunale

2.1 Tipologia di servizi offerti

Il Sistema Informativo del Comune di Gallio è rivolto a soddisfare tutte le esigenze di accesso alle informazioni "interne" cioè provenienti dai servizi interni all'amministrazione stessa sia, quasi sempre indirettamente, provenienti dall'utenza della popolazione residente esterna all'amministrazione.
Nell'uno e nell'altro caso l'esigenza può essere soddisfatta o da un sistema effettivamente interno, fisicamente residente presso sistemi informativi strettamente Comunali, oppure tramite un sistema esterno, reso disponibile da altri enti e al Comune stesso accessibile con le opportune modalità.

2.2 Servizio informativo

2.2.1 Organizzazione

Nel contesto del Sistema Informativo ogni dipendente del Comune di Gallio deve collaborare, secondo le proprie specifiche funzioni, alla gestione del Sistema Informativo e alla gestione generale della sicurezza.

Tipologia Utenti	Compiti/Responsabilità	Note
Addetti società assistenza hardware e software	Attuazione e messa in opera delle politiche di sicurezza informatica (sistemi antivirus, firewalling, backup, politiche relative alle utenze, …). Verifiche sull'attuazione delle politiche.	
Dipendenti Comune (generici)	Rispetto delle norme relative alla Sicurezza Informatica; rispetto delle norme inerenti il trattamento dati.	Vedere incarichi specifici a Responsabile o incaricato del trattamento nei settori specifici

2.3 Infrastruttura tecnologica

2.3.1 Generalità

L'Infrastruttura Tecnologica del Comune di Gallio può essere schematizzata come segue:

Tipologia di apparati	Descrizione
Apparati Server interni	Indichiamo in questa categoria tutti gli ambienti server di proprietà comunale o comunque gestiti direttamente, sia fisici che virtuali; tutti gli apparati server interni sono dislocati presso la Sala Server Comunale
Apparati Server Esterni	Indichiamo in questa categoria tutti gli ambienti server, sia fisici che virtuali, gestiti da società esterne, in virtù di contratti stipulati con il Comune
Apparati di Rete	Indichiamo in questa categoria tutti gli apparati (router, switch, hub, …) che concorrono alla connettività fra le sedi Comunali (connettività interna), da e verso Internet (connettività pubblica verso l'esterno)
Apparati Storage, di Backup e Sicurezza	Indichiamo in questa categoria tutti gli apparati che concorrono specificatamente alla sicurezza (storage per backup, apparati firewall)
Infrastruttura di Comunicazione	Intendiamo con questo termine l'insieme delle cablature che realizzano la connettività LAN, nonché l'infrastruttura di comunicazione fra le sedi (WAN), da e verso Internet
Apparati Client	In questa categoria raggruppiamo tutti gli apparati (PC, Portatili, …) utilizzati dall'utenza interna

2.3.2 Struttura fisica

Il sistema informatico dell'Ente è così costituito:

DCServer23 FUJITSU TX1310M1 – MI5W sn. YLTQ057629
Garanzia e Supporto Fujitsu Italia con intervento entro 48 ore fino al 09/05/2022
Ruolo: Domain Controller Primario – DHCP DNS SERVER

DCServer32 FUJITSU TX120 S3p – PS130-D3049 sn. YLLC001957
Garanzia e Supporto Fujitsu Italia con intervento entro 48 ore fino al 31.12.2019
Ruolo: Domain Controller Secondario – Application Server sw Halley Informatica

FPServer1 FUJITSU TX1330M1 – PS170 - sn. YLXM005462

Garanzia e Supporto Fujitsu Italia con intervento entro 48 ore fino al 31.03.2020
Ruolo: Domain Controller Secondario – File Server Area Documentale – Application Server sw Enginnering

NAS QNAP TS-253A-4G con protocollo I-SCSI per Windows Server backup

L'inventario dei dispositivi connessi alla rete è prodotto ed aggiornato con specifico software di monitoraggio e scansione.
Tutti i sistemi server utilizzano sistemi operativi Windows Server 2008/2012 x64 per i quali sono disponibili i relativi aggiornamenti di sicurezza Windows Update.
Tutti i PC client utilizzano sistemi operativi Windows 7/10 x64 per i quali sono disponibili i relativi aggiornamenti di sicurezza Windows Update.

Caratteristiche Sede Comunale

- Ubicazione: Via Roma 2 (sede principale e palazzina staccata)
- Videosorveglianza: no
- Allarme: no
- Antincendio: estintori al piano

Caratteristiche Uffici

Denominazione	Estintori	Accesso	Armadi chiusi a chiave	Allarme	Cassaforte	Videosorveglianza
Segreteria	Sì (al piano)	Porta chiusa a chiave	Sì	No	No	No
Patrimonio					No	
Segretario c.le					No	
Personale/Commercio					No	
Urbanistica					No	
Manutenzioni					No	
Archivio Urbanistica (piano terra di Via Roma)					No	
Servizi sociali					No	
Servizi demografici					Sì	
Polizia locale					Sì	
Ragioneria					No	
Tributi					No	
Biblioteca					No	

Caratteristiche sala server

- Ubicazione: piano primo
- Accesso: chiuso a chiave
- UPS: gruppi UPS 1500VA per ciascun server/apparato
- Raffreddamento: non necessario
- Videosorveglianza: no
- Allarme: no
- Antincendio: estintori al piano
- Posizione: stanza dedicata

Caratteristiche armadio di rete

- Ubicazione: piano terra
- Accesso: chiuso a chiave
- UPS: gruppo UPS 1500VA
- Raffreddamento: non necessario
- Antincendio: estintori al piano

Caratteristiche connettività

Router dual-wan Cisco serie 800 con gestione delle linee Internet fail-over e funzioni di firewall

Linea primaria (fibra HTTC)

- Gestore: Media Veneto srl
- Tipologia: HTTC

Linea secondaria (wireless)

- Gestore: Media Veneto srl
- Tipologia: WI-FI con antenna esterna

I servizi sono distribuiti fra i tre server e vengono fatti i seguenti backup:

- da ciascun Windows Server Backup completo su Unità i-Scsi **QNAP NAS TS-253A-4G, cadenza giornaliera**
- da server applicativo DCSERVER32 cloud backup in server in DATACENTER BOXXAPPS**, cadenza giornaliera**
- da server applicativo/file server FPSERVER1 cloud backup in server in DATACENTER BOXXAPPS**, cadenza giornaliera**

2.3.4 Sistema di Conservazione

Per quanto concerne il sistema di conservazione si fa rimando a quanto dettagliato nel Manuale di Gestione.

3 Politiche organizzative della sicurezza

3.1 Generalità

La definizione e l'applicazione delle politiche di sicurezza all'interno del Comune richiedono l'individuazione di un insieme di regole che fanno riferimento alle tecnologie usate, alle metodologie, alle procedure d'implementazione e ad altri elementi specifici dell'ambiente e del sistema informativo. L'applicazione delle politiche di sicurezza all'interno del Comune richiede, inoltre, la definizione di processi che descrivano gli specifici passi operativi che le persone devono seguire per raggiungere gli obiettivi che sono stati stabiliti. I processi sono indispensabili per la gestione di tutti gli oggetti legati alla sicurezza.
Attualmente, l'individuazione della politica di sicurezza comunale determina il modello logico della sicurezza fissandone gli obiettivi. L'individuazione degli obiettivi di sicurezza si traduce in obiettivi del sistema informativo, sostanziandosi con la formalizzazione di norme organizzative e standard di riferimento. Inoltre, la sicurezza viene considerata da tutto il personale, una componente integrante dell'attività quotidiana, finalizzata alla protezione delle informazioni e delle apparecchiature da manomissioni, uso improprio o distruzione. Un sistema di sicurezza, per poter raggiungere i migliori risultati funzionali, va visto globalmente, negli aspetti fisici, logici e organizzativi, come un insieme di misure e strumenti hardware, software, organizzativi e procedurali integrati fra loro, volti a ridurre la probabilità di danni a un livello accettabilmente basso e ad un costo ragionevole.

3.1.1 Backup e Disaster Recovery

I dati, in qualunque modo elaborati dal sistema informatico dell'Ente, sono salvati nella memoria centrale dei Server.
È stato attivato un sistema di duplicazione e memorizzazione criptata dei dati informatici presenti sulle strutture *hardware* del Comune di Gallio in modalità remota (backup remoto). Tale servizio è stato realizzato e viene interamente gestito dalla società Boxxapps srl.
Il servizio ha lo scopo di mettere al sicuro i dati dell'Ente e deve dare la possibilità di recuperarli e renderli disponibili in caso di problemi tecnici, atti vandalici, eventi naturali disastrosi.
Il servizio prevede la combinazione di un "local disaster" e di un "cloud disaster". L'invio dei dati presso il Data Center del fornitore avviene attraverso un meccanismo di crittografia di tipo Secure Sockets Layer (SSL).
Il servizio deve prevede, tra l'altro:
1. Piattaforma software presso l'Internet Data Center del fornitore e hosting.
3. Un sistema di gestione per la sicurezza delle informazioni relativa al servizio conforme alle specifiche dettate dalla norma ISO/IEC 27001:2014 e ISO 9001:2008.
4. Servizio giornaliero di "local backup" su dispositivo del fornitore dei dati definiti con l'ente e contenuti sui server:
    a. con retention di:
        1. copia giornaliera degli ultimi 7 giorni;
        2. copia settimanale delle ultime 4 settimane;
    b. spazio disponibile in locale su dispositivo del fornitore;
    c. fornitura di un disco rimovibile crittografato per eseguire una copia dei dati;

5. Servizio giornaliero di “cloud disaster”:
    a. con retention di:
        1. copia giornaliera degli ultimi 7 giorni;
        2. copia settimanale delle ultime 4 settimane;
        3. copia mensile degli ultimi 6 mesi;
        4. copia semestrale dei ultimi 2 semestri (indicativamente giugno e dicembre).

3.2 Sicurezza logica

3.2.1 Introduzione
La sicurezza logica si occupa della protezione dell’informazione, dei dati, dei documenti, delle applicazioni, dei sistemi e reti, sia in relazione al loro corretto funzionamento ed utilizzo, sia in relazione alla loro gestione e manutenzione nel tempo. La realizzazione della sicurezza logica è pensata in termini architetturali e ciò comporta l’individuazione di tutti i sistemi hardware e software che implementano le attività dei vari servizi Comunali, in modo tale da garantirne la fruibilità nel tempo, che deve essere nel contempo aperta a tutti gli operatori necessari, ma limitata alle funzioni ad essi attribuite in un determinato momento.
3.2.2 Sistema di autenticazione
La credenziale di autenticazione consiste in un codice per l’identificazione dell’Incaricato (utente), associato a una parola chiave riservata e conosciuta solamente dal medesimo. La parola chiave è composta da almeno otto caratteri (numeri e lettere) e non contiene riferimenti agevolmente riconducibili all’Incaricato, il quale provvederà a modificarla al primo utilizzo. Le credenziali di autenticazione sono affidate al controllo del *Server DCSERVER23 (domain controller primario)* che garantisce l’applicazione delle politiche di protezione e sicurezza in forma centralizzata ed automatizzata. La politica di centralizzazione del sistema informativo si appoggia al sistema integrato di *active directory* (“insieme di servizi di rete - *account* utente, *account computer*, cartelle condivise, stampanti, *etc*. - adottati dai sistemi operativi organizzati in modo da consentirne la condivisione da parte dei *client*”) tramite apposita profilazione degli utenti (gestione dei profili di autorizzazione). Ad integrare la protezione sul sistema informativo, i *software* dell’Ente e gli applicativi *web* sono dotati di apposite procedure di accesso tramite *username* (“nome con il quale l'utente viene riconosciuto da un *computer*, da un programma o da un *server*”) e *password* (“sequenza di caratteri alfanumerici utilizzata per accedere in modo esclusivo ad una risorsa informatica”). Lo *username* è un identificativo che, insieme alla *password*, rappresenta le credenziali per accedere alle risorse informatiche o ad un sistema.

3.2.2 Antivirus e similari
Il sistema informatico dell’Ente e i dati personali da esso custoditi sono protetti contro il rischio di intrusione e contro l’azione di programmi di cui all’Articolo 615-*quinquies* del Codice Penale (“*Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico*”), mediante l'attivazione:

- software antivirus centralizzato SYMANTEC ENDPOINT PROTECTION – CLOUD EDITION
- protezione antivirus e antispam integrata nel mail server ARUBA (posta ordinaria dominio comune.gallio.vi.it) - protezione antivirus e antispam integrata nel mail server INFOCERT (posta certificata dominio legalmail.it)

4 Documenti e Banche dati

4.1 Sistema di gestione informatica dei documenti
Il DPR 445/2000, all’art. 1, comma 1, lett. r) definisce il Sistema di Gestione Informatica dei Documenti come *“l’insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure informatiche utilizzati dalle amministrazioni per la gestione dei documenti”*. Tale sistema è attivato dal Comune su tutte le postazioni di lavoro degli uffici afferenti all’AOO e le abilitazioni all’utilizzo delle sue funzionalità sono stabilite e aggiornate a cura dei Responsabili individuati all’interno dell’AOO (Responsabile della gestione documentale, Responsabile dei sistemi informativi).
Per quanto concerne i software attraverso i quali viene registrato e gestito il patrimonio documentale dell’ente si fa riferimento alle indicazioni contenute nel manuale di gestione così come anche per i seguenti argomenti:

- Protocollo informatico;
- Formazione dei documenti;
- Formati adottati;
- Sottoscrizioni;

- Validazione temporale;
- Metadati;
- Trasmissione dei documenti;
- Conservazione.

5 Trattamento dei dati personali - Analisi dei rischi

Per quanto concerne le politiche inerenti il trattamento dei dati personali e l'analisi dei rischi incombenti sui dati ed i documenti si fa esplicito rimando alla normativa in materia, al regolamento comunale e al registro dei trattamenti.