ALLEGATO O

al Manuale di gestione del protocollo informatico, dei flussi documentali, del sistema di conservazione digitale dei documenti informatici e degli archivi

Comune di Poggibonsi

Provincia di Siena

PIANO DI SICUREZZA RELATIVO ALLA FORMAZIONE, ALLA GESTIONE, ALLA TRASMISSIONE, ALL'INTERSCAMBIO, ALL'ACCESSO E ALLA CONSERVAZIONE DEI DOCUMENTI INFORMATICI

SOMMARIO

Art. 1 - Premessa

1) Il presente *Piano di Sicurezza relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso e alla conservazione dei documenti informatici* (di seguito denominato per semplicità *Piano di Sicurezza Informatica*) è adottato in conformità delle nuove *"Linee Guida sulla formazione, gestione e conservazione dei documenti informatici"* redatte a cura dell'Agenzia per l'Italia Digitale – AgID in vigore dal 01/01/2022 e alla precedente normativa;
2) Scopo del presente documento è descrivere la strategia che il Comune intende adottare per poter soddisfare i seguenti requisiti di sicurezza:

   a) **Confidenzialità**: l'accesso e la divulgazione delle informazioni presenti nel sistema, indipendentemente dal formato in cui si trovano, deve poter essere effettuato solo da entità autorizzate. Devono essere ridotte al minimo, compatibilmente con i limiti delle tecnologie e risorse impiegate, la probabilità che un'informazione riservata sia resa pubblica.

   b) **Integrità**: la modifica o la distruzione di informazioni presenti nel sistema, indipendentemente dal formato in cui si trovano, devono poter essere effettuate solo da entità autorizzate. Devono essere ridotte al minimo, compatibilmente con i limiti delle tecnologie e risorse impiegate, le 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).

   c) **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.

   d) **Accountability** (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.
3) Il presente Piano di Sicurezza Informatica si conforma ai requisiti minimi di sicurezza dei sistemi di protocollo informatico indicati dalle nuove *"Linee Guida sulla formazione, gestione e conservazione dei documenti informatici"* in vigore dal 01/01/2022 (all'Art. 3.1.6).
4) In base al Piano di Sicurezza Informatica i dati personali comuni, sensibili e/o giudiziari vengono custoditi in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.
5) Il presente Piano di Sicurezza Informatica, che si basa sui risultati dell'analisi dei rischi a cui sono esposti i dati (personali e non), e/o i documenti trattati, definisce:

   a) le politiche generali e particolari di sicurezza da adottare all'interno dell'Ente;

   b) le modalità di accesso al Sistema di Gestione Informatica dei Documenti;

   c) gli interventi operativi adottati sotto il profilo organizzativo, procedurale e tecnico, con particolare riferimento alle misure minime di sicurezza in caso di trattamento di dati personali (vedi comma precedente);

   d) la formazione degli addetti;

   e) le modalità con le quali deve essere effettuato il monitoraggio periodico dell'efficacia e dell'efficienza delle misure di sicurezza.

6) Tale Piano di Sicurezza Informatica è soggetto a revisione con cadenza almeno biennale; a seguito di particolari esigenze, determinate da sopravvenienze normative o evoluzioni tecnologiche, potrà essere modificato anticipatamente:

Art. 2 - Elementi di rischio cui sono soggetti i documenti informatici e i dati contenuti nel Sistema di Gestione Informatica dei Documenti

1) I principali elementi di rischio cui sono soggetti i documenti informatici e i dati trattati con l'ausilio delle tecnologie informatiche sono essenzialmente riconducibili alle seguenti tipologie:

- accesso non autorizzato, sia esso inteso come accesso al Sistema di Gestione Informatica dei Documenti; o come accesso ai documenti, dati e unità archivistiche in esso contenuti;
- cancellazione o manomissione dei documenti e dei dati, includendo a tale proposito tutti i dati presenti sul Sistema di Gestione Informatica dei Documenti;
- perdita dei documenti e dei dati contenuti nel Sistema;
- trattamento illecito, eccedente rispetto allo scopo o comunque non in linea con la normativa vigente, dei dati personali.

2) Per prevenire tali rischi e le conseguenze da essi derivanti, il Comune di Poggibonsi adotta gli accorgimenti e le politiche per la sicurezza di seguito descritte.

Art. 3 - Sicurezza della rete di accesso al servizio

1) Il Sistema di Gestione Informatica dei Documenti del Comune di Poggibonsi è ospitato nella server farm del TIX di Regione Toscana e l'accesso da parte dell'ente avviene attraverso la connessione RTRT Estesa.

Art. 4 - Accesso al Sistema di Gestione Informatica dei Documenti e ai documenti e dati in esso contenuti da parte di utenti interni all'AOO

1) L'accesso ai documenti e ai dati presenti sul Sistema è definito in base al livello di riservatezza degli stessi.
2) L'accesso al Sistema di Gestione Informatica dei Documenti, da parte degli utenti interni all'AOO, avviene attraverso l'utilizzo di credenziali di autenticazione.
3) Le credenziali di autenticazione consistono in un codice (User-Id), per l'identificazione dell'incaricato, associato ad una parola chiave riservata (Password), conosciuta solamente dal medesimo.
4) Agli incaricati è prescritto di adottare le necessarie cautele volte ad assicurare la segretezza della Password; quest'ultima è composta da almeno dieci caratteri, tra cui almeno un numero e un carattere speciale e non contiene riferimenti agevolmente riconducibili al titolare. La Password è modificata dall'incaricato al suo primo utilizzo e, successivamente, con cadenza trimestrale.
5) L'User-Id non può essere assegnato ad altri incaricati neppure in tempi diversi.
6) Le credenziali di autenticazione non utilizzate da almeno sei mesi vengono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica; tali credenziali sono altresì disattivate anche nel caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.
7) Il Responsabile della sicurezza informatica dell'Ente non è in grado di conoscere la Password dell'utente; qualora l'utente medesimo dimenticasse la propria Password si

procederà all'assegnazione di una nuova chiave di accesso.

Art. 5 - Accesso al trattamento di dati personali sensibili o giudiziari e politiche di sicurezza espressamente previste

1) L'accesso ai documenti contenenti dati personali, sensibili o giudiziari e ai dati medesimi avviene per mezzo dell'individuazione di specifici profili di autorizzazione stabiliti sulla base del livello di riservatezza di ciascun documento, fascicolo, sotto fascicolo o inserto; tali profili, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento.
2) Periodicamente, e comunque con cadenza almeno annuale, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.
3) Gli incaricati del trattamento di dati personali, sensibili o giudiziari non possono lasciare incustodita e accessibile la propria postazione di lavoro durante il trattamento degli stessi.

Art. 6 - Formazione dei documenti

1) I documenti dell'AOO sono prodotti utilizzando i formati indicati nell'Allegato N.3 del *Manuale di Conservazione dei Documenti Informatici del Comune di Poggibonsi*.
2) L'apposizione della firma digitale, volta a garantire l'attribuzione certa della titolarità del documento e la sua integrità, avviene previa conversione in un formato, tra quelli previsti dal suddetto DPCM, che garantisca la leggibilità, l'interscambiabilità, la non alterabilità, l'immutabilità nel tempo del contenuto e della struttura del documento medesimo (ad esempio il formato PDF); l'acquisizione mediante scansione dei documenti analogici avverrà in uno dei formati avente le medesime caratteristiche.
3) L'apposizione delle varie tipologie di sottoscrizioni elettroniche, l'apposizione della firma digitale, nonché la validazione temporale del documento sottoscritto digitalmente avverranno in conformità di quanto sancito dalle regole tecniche contenute nel DPCM 22/02/2013, emanate ai sensi dell'art. 71 del D. Lgs. 82/05.
4) La sottoscrizione del documento con firma digitale avverrà prima dell'effettuazione della registrazione di protocollo.

Art. 7 - Sicurezza delle registrazioni di protocollo

1) L'accesso in consultazione al registro di protocollo è consentito sulla base dell'organizzazione dell'Ente; ciascun operatore è abilitato ad accedere esclusivamente ai documenti e ai dati di protocollo dei documenti che ha prodotto, che gli sono stati assegnati o comunque di competenza del proprio ufficio di riferimento.
2) Ogni registrazione di protocollo viene memorizzata dal Sistema di Gestione Informatica dei Documenti, unitamente all'identificativo univoco dell'autore che l'ha eseguita e alla data e all'ora della stessa.
3) Il Sistema non consente la modifica del numero e della data di protocollo; in tal caso l'unica possibile modifica è l'annullamento della registrazione stessa di cui, analogamente al caso precedente, il Sistema manterrà traccia. L'annullamento di una registrazione di protocollo deve essere richiesto con specifica funzione del sistema di protocollazione, adeguatamente motivata, al Responsabile dell'Ufficio Protocollo, che è l'unico soggetto autorizzato ad effettuare l'annullamento, come previsto dall'Art.37 del *Manuale di gestione del protocollo informatico, dei flussi documentali, del sistema di conservazione digitale dei documenti informatici e degli archivi del Comune di Poggibonsi.*

4) L'impronta digitale del documento informatico associata alla registrazione di protocollo del medesimo è generata utilizzando una funzione di hash conforme a quanto previsto dalla normativa vigente.
5) Al fine di garantire l'immodificabilità delle registrazioni di protocollo il Sistema permette, al termine della giornata lavorativa, la produzione del registro giornaliero delle registrazioni di protocollo, in formato digitale; tale registro, formato nel rispetto di quanto previsto nel *Manuale di gestione del protocollo informatico, dei flussi documentali, del sistema di conservazione digitale dei documenti informatici e degli archivi del Comune di Poggibonsi* e nel *Manuale di Conservazione dei documenti informatici del Comune di Poggibonsi*, sarà trasferito nell'arco della giornata lavorativa successiva al Delegato alla Conservazione digitale a norma accreditato di cui l'Ente si serve.

Art. 8 - Gestione dei documenti e sicurezza del Sistema di Gestione Informatica dei Documenti

1) I documenti informatici, una volta registrati sul Sistema di Gestione Informatica dei Documenti, risultano immodificabili e non eliminabili; l'accesso ad essi, da parte degli utenti interni all'AOO, avviene soltanto attraverso il Sistema medesimo, previa la suddetta procedura di identificazione informatica e nel rispetto dei profili di autorizzazione di ciascun utente.
2) Il Sistema consente l'effettuazione di qualsiasi operazione su di esso o sui dati, documenti, fascicoli e aggregazioni documentali in esso contenuti, esclusivamente agli utenti abilitati per lo svolgimento di ciascuna attività; il Sistema effettua inoltre il tracciamento di qualsiasi evento di accesso e/o modifica delle informazioni trattate e di tutte le attività rilevanti ai fini della sicurezza svolte su di esso da ciascun utente, in modo da garantirne l'identificazione; tali registrazioni sono protette al fine di non consentire modifiche non autorizzate.
3) Il Sistema e tutti i documenti e dati in esso contenuti sono protetti contro i rischi di intrusione non autorizzata.

Art. 9 - Conservazione dei documenti

1) I documenti registrati sul Sistema di Gestione Informatica dei Documenti sono conformi ai requisiti e contengono i metadati previsti ai fini della conservazione permanente.
2) Il trasferimento in conservazione avverrà mediante la produzione di pacchetti di versamento basati su uno schema XML conforme a quanto previsto nel *Manuale di Conservazione dei documenti informatici del Comune di Poggibonsi*.

Art. 10 - Accesso di Utenti esterni al Sistema di Gestione Informatica dei Documenti

1) Non è consentito l'accesso al Sistema da parte di utenti esterni.
2) L'esercizio del diritto di accesso agli atti da parte di utenti esterni viene effettuato nel rispetto di quanto sancito dalla legge 241/90 e del D. Lgs. 196/03.

Art. 11 - Piani formativi del personale

1) Ai fini di una corretta gestione dell'intero ciclo dei documenti informatici, dalla formazione degli stessi fino alla loro trasmissione al sistema di conservazione, l'Ente predispone apposite attività formative per il personale, con particolare riferimento ai seguenti temi:

- utilizzo del Sistema di Gestione Informatica dei Documenti;
- fascicolazione dei documenti informatici;
- politiche e aspetti organizzativi previsti nel manuale di gestione;
- legislazione e tematiche relative alla gestione documentale;
- legislazione in materia di protezione dei dati personali;
- aggiornamento sui temi suddetti.

Art. 12 - Aggiornamento del Piano di Sicurezza Informatica

1) Il Responsabile dei Sistemi Informativi cura l'aggiornamento del presente Piano di Sicurezza Informatica, in collaborazione con il Responsabile del Protocollo, con il Responsabile della Gestione Documentale ovvero con il Coordinatore della Gestione Documentale, se e ove nominato, con il Responsabile della Conservazione e con il Responsabile per la Transizione al Digitale.