ALLEGATO N. 4
PIANO DI SICUREZZA RELATIVO ALLA FORMAZIONE, ALLA GESTIONE, ALLA TRASMISSIONE, ALL'INTERSCAMBIO, ALL'ACCESSO, ALLA CONSERVAZIONE DEI DOCUMENTI INFORMATICI

Premessa

Il presente piano di sicurezza, adottato ai sensi dell'articolo 4, comma 1, lettera c), del D.P.C.M. 3 dicembre 2013 *"Regole tecniche per il protocollo informatico"*, descrive le politiche adottate dal Comune di Treia affinché:

- i documenti e le informazioni trattati dall'Ente siano resi disponibili, integri e riservati;
- i dati personali comuni, sensibili e/o giudiziari vengano 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.

A tali fini, l'articolo 7 del suddetto D.P.C.M. individua i requisiti minimi di sicurezza dei sistemi di protocollo informatico a cui il presente piano si conforma.
Il piano di sicurezza, in base ai rischi cui sono esposti i dati (personali e non) e/o i documenti trattati, definisce:

- le politiche generali e particolari di sicurezza da adottare all'interno del Comune di Treia;
- le modalità di accesso al Sistema di Gestione Informatica dei Documenti;
- gli interventi operativi adottati sotto il profilo organizzativo, procedurale e tecnico, con particolare riferimento alle misure minime di sicurezza, di cui al disciplinare tecnico richiamato nell'allegato b) del decreto legislativo 30 giugno 2003, n. 196 *"Codice in materia di protezione dei dati personali"*, in caso di trattamento di dati personali, sensibili o giudiziari;
- la formazione degli addetti;
- le modalità con le quali deve essere effettuato il monitoraggio periodico dell'efficacia e dell'efficienza delle misure di sicurezza.

Tale piano di sicurezza è soggetto a revisione con cadenza almeno biennale; a seguito di particolari esigenze, determinate da sopravvenienze normative o evoluzioni tecnologiche, potrà essere modificato anticipatamente.

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

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.

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

Sicurezza della rete di accesso al servizio

Il Sistema di Gestione Informatica dei Documenti del Comune di Treia non è esposto all'accesso attraverso la rete internet, ma è installato all'interno di un server che opera nella intranet dell'Ente, ereditando dalla stessa tutti i meccanismi previsti per la sicurezza e la protezione.

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

L'accesso al Sistema di Gestione Informatica dei Documenti, da parte degli utenti interni all'AOO, avviene attraverso l'utilizzo di credenziali di autenticazione; i profili di abilitazione alle funzionalità del Sistema stesso sono attribuiti a ciascun utente sulla base di quanto stabilito dall'allegato n. 2 al presente manuale. L'accesso ai documenti e ai dati presenti sul Sistema è definito in base al livello di riservatezza degli stessi.
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; tali credenziali vengono verificate in tempo reale da un apposito sistema di identificazione, il quale consente l'accesso ai soggetti abilitati e traccia tutti gli accessi di ciascun utente, memorizzando, ai fini di controllo, l'*User-Id* corrispondente, ma non la *Password* dello stesso.
Agli incaricati è prescritto di adottare le necessarie cautele volte ad assicurare la segretezza della *Password*; quest'ultima è composta da almeno otto caratteri alfanumerici (di cui almeno una lettera maiuscola, una lettera minuscola, 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, ogni 3 mesi.
Come ulteriori misure di sicurezza l'*User-Id* non può essere assegnato ad altri incaricati neppure in tempi diversi e, al momento del cambio della *Password*, non possono venir riattivate le ultime due *Password* di ciascun utente.
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.
Qualora il titolare delle credenziali di autenticazione dimenticasse la propria *password*, il responsabile per la sicurezza informatica dell'Ente procederà all'assegnazione di una nuova chiave di accesso.

Accesso al trattamento di dati personali sensibili o giudiziari e politiche di sicurezza espressamente previste

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 o fascicolo, secondo quanto stabilito dall'articolo 27 del presente manuale; tali profili, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento.
Periodicamente, e comunque con cadenza almeno annuale, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.
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. Per quanto riguarda l'accesso al Sistema di Gestione Informatica dei Documenti, le credenziali di autenticazione di ciascun operatore vengono consegnate dai medesimi in busta chiusa e sigillata al Responsabile per il trattamento dei dati personali; in caso di prolungata assenza o impedimento del soggetto incaricato del trattamento dei dati personali, sensibili o giudiziari e, qualora si renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema, il Responsabile per il trattamento dei dati personali è autorizzato ad utilizzare le credenziali contenute nella suddetta busta per procedere al trattamento, comunicandolo al titolare. Il soggetto titolare delle credenziali provvederà, al momento del proprio rientro in servizio, alla sostituzione della *password*, provvedendo all'inserimento della stessa in altra busta sigillata da consegnare nuovamente al suddetto Responsabile.

Trattamento dei dati personali, sensibili o giudiziari senza l'ausilio di strumenti elettronici

Analogamente al trattamento dei medesimi dati svolto per mezzo di strumenti elettronici, sarà verificato il sussistere delle condizioni per l'accesso e il trattamento dei suddetti dati, da parte di ciascun utente o gruppo di utenti, con cadenza almeno annuale.
I documenti, sono controllati e custoditi dagli incaricati del trattamento per tutto il tempo di svolgimento dei relativi compiti; nell'arco di tale periodo gli incaricati si assicureranno che a tali documenti non accedano persone prive di autorizzazione.
L'accesso agli archivi contenenti dati sensibili o giudiziari è consentito solo previa autorizzazione; le persone ammesse sono identificate e registrate.

Formazione dei documenti

I documenti informatici del Comune di Treia sono prodotti utilizzando i formati previsti dal D.P.C.M. 3 dicembre 2013 e dall'allegato n. 5 del presente manuale. 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 D.P.C.M., che garantisca la leggibilità, l'interscambiabilità, la non alterabilità, l'immutabilità nel tempo del contenuto e della struttura del documento medesimo (ad esempio il PDF); l'eventuale acquisizione mediante scansione dei documenti analogici avverrà in uno dei formati avente le medesime caratteristiche.
L'apposizione della firma digitale o di altre eventuali sottoscrizioni elettroniche, nonché la validazione temporale del documento sottoscritto digitalmente avvengono in conformità di quanto sancito dalle regole tecniche contenute nel D.P.C.M. 22 febbraio 2013, emanate ai sensi dell'articolo 71 del D.Lgs. 82/2005.
La sottoscrizione del documento con firma digitale avviene prima dell'effettuazione della registrazione di protocollo.

Sicurezza delle registrazioni di protocollo

Di norma i dipendenti che operano nell'ambito dei vari uffici sono abilitati ad accedere esclusivamente ai dati di protocollo dei documenti da essi prodotti, ad essi assegnati o, comunque, di competenza del proprio ufficio di riferimento.
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.
Eventuali modifiche, autorizzate ai sensi dell'articolo 28 del presente manuale, vengono registrate per mezzo di *log* di sistema che mantengono traccia dell'autore, della modifica effettuata, nonché della data e dell'ora; il Sistema mantiene leggibile la precedente versione dei dati di protocollo, permettendo, in tal modo, la completa ricostruzione cronologica di ogni registrazione.
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 sempre essere accompagnata da autorizzazione scritta del Responsabile della gestione documentale e il Sistema di Gestione Informatica dei Documenti deve recare, in corrispondenza della registrazione annullata, gli estremi del provvedimento di autorizzazione.
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.
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 conservazione, sarà trasferito, nell'arco della giornata lavorativa successiva, alla struttura di conservazione accreditata di cui il Comune si serve, secondo quanto previsto dall'articolo 3 del presente manuale.

Gestione dei documenti e sicurezza logica del Sistema

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.
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 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.
Il Sistema e tutti i documenti e dati in esso contenuti sono protetti contro i rischi di intrusione non autorizzata e contro l'azione di programmi informatici mediante l'attivazione di *software* antivirus e *firewall*, aggiornati periodicamente, ogni qual volta il fornitore renda disponibili gli aggiornamenti dei medesimi e la cui licenza viene annualmente rinnovata.
Ai fini di ridurre la vulnerabilità dei sistemi informativi, il sistema operativo utilizzato dall'AOO e il Sistema di Gestione Informatica dei Documenti vengono costantemente tenuti aggiornati per mezzo dell'istallazione degli aggiornamenti periodici che i fornitori rendono disponibili.

Backup e ripristino dell'accesso ai dati

Il Backup dei dati contenuti nel Sistema di Gestione Informatica dei Documenti di Halley avviene quotidianamente, in modalità totale, su 2 RDX esterni ridondati e mensilmente su un ulteriore RDX.
Per quanto riguarda, invece, i dati contenuti nelle procedure non Halley e nelle varie macchine, viene eseguita una copia su un server di *backup*; di tali dati, salvati su 2 dischi *raid* uno in *mirror*, vengono mantenuti gli ultimi 3 giorni, l'ultimo mese e l'ultimo anno, ai fini di permettere il ripristino dei dati.
Come ulteriore misura di sicurezza e al fine di permettere maggiore facilità nelle operazioni, lo *storage* dei dati avviene in una macchina diversa da quella che esegue il *backup*.
I server e i supporti esterni in cui sono salvati i dati di *backup* ed eventuali altri supporti su cui siano memorizzati dati sensibili o giudiziari sono custoditi, sotto chiave, a cura del Responsabile della sicurezza informatica, d'intesa con il Responsabile della gestione documentale e il Responsabile per il trattamento dei dati personali, al fine di evitare accessi non autorizzati e trattamenti non consentiti.
I supporti riscrivibili, utilizzati dal Comune, contenenti dati sensibili o giudiziari, possono venire cancellati e riutilizzati esclusivamente nel caso in cui le informazioni in essi contenute non siano intelligibili e in alcun modo ricostruibili.
Qualora dati sensibili e giudiziari vengano memorizzati su supporti rimovibili non riscrivibili, una volta che sia cessato lo scopo per cui tali dati sono stati memorizzati, i supporti vengono distrutti.

Trasmissione e interscambio dei documenti

La trasmissione e l'interscambio di documenti e fascicoli informatici all'interno dell'AOO avviene esclusivamente per mezzo del Sistema di Gestione Informatica dei Documenti; nessun'altra modalità è consentita al fine di evitare la dispersione e la circolazione incontrollata di documenti e dati.

La trasmissione di documenti informatici al di fuori dell'Ente avviene tramite PEC o mediante i meccanismi dell'interoperabilità e della cooperazione applicativa di cui al Sistema Pubblico di Connettività, utilizzando le informazioni contenute nella segnatura di protocollo.
I messaggi di posta elettronica certificata prodotti dal Comune di Treia sono compatibili con il protocollo SMTP/MIME definito nelle specifiche pubbliche RFC 821-822, RFC 2045 e 2049 e successive modificazioni.
Le informazioni relative alla segnatura di protocollo sono strutturate in un file conforme alle specifiche XML, compatibile con un file XML Schema e/o DTD, secondo lo schema previsto nella circolare AgID n. 60 del 23 gennaio 2013.

Conservazione dei documenti

I documenti informatici registrati sul Sistema di Gestione Informatica dei Documenti sono affidati per la conservazione digitale ad un soggetto conservatore accreditato ai sensi del D.P.C.M. 3 dicembre 2013 *"Regole tecniche per il sistema di conservazione"*. 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.

***Disaster recovery* e continuità operativa**

Il Comune di Treia, conformemente a quanto disposto dall'articolo 50-*bis* del D.Lgs. 82/2005, prevede di dotarsi di un piano di emergenza in grado di assicurare la continuità delle operazioni indispensabili per il servizio e il ritorno alla normale operatività, definendo a tali fini il piano di continuità operativa e quello di *disaster recovery*, basati su appositi e dettagliati studi di fattibilità tecnica, nel cui ambito viene obbligatoriamente acquisito il parere dell'AgID.
In caso di perdita dei dati il servizio di *Disaster Recovery* prevederà il ripristino degli stessi e dell'accesso ad essi entro il tempo massimo previsto dal disciplinare tecnico di cui all'allegato b) al D.Lgs. 196/2003.

Accesso di Utenti esterni al Sistema

L'esercizio del diritto di accesso da parte di utenti esterni al Sistema viene effettuato nel rispetto di quanto sancito dalla legge 241/1090 e del D.Lgs. 196/2003.
Qualora l'utente esterno decida di esercitare il proprio diritto di accesso rivolgendosi direttamente all'URP o ad altro sportello allo scopo predisposto, la consultazione deve avvenire in modo che siano resi visibili soltanto dati o notizie che riguardino il soggetto interessato ed adottando gli opportuni accorgimenti (ad es. il posizionamento del monitor) volti ad evitare la diffusione di informazioni di carattere personale.

Piani formativi del personale

Ai fini di una corretta gestione dell'intero ciclo dei documenti informatici, dalla formazione degli stessi fino alla loro trasmissione al sistema di conservazione, il Comune predispone le apposite attività formative per il personale, con particolare riferimento ai seguenti temi:
- aspetti normativi relativi alla gestione documentale;
- utilizzo applicativi *software* per la gestione dei documenti informatici;
- utilizzo del Sistema di Gestione Informatica dei Documenti;
- fascicolazione dei documenti informatici;
- gestione dei fascicoli informatici;
- aggiornamento sui temi suddetti.

Monitoraggio periodico del funzionamento del Sistema

Il Responsabile della gestione documentale dell'Ente effettua periodiche verifiche sul corretto funzionamento del Sistema di Gestione Informatica dei Documenti, valutando a tal fine, anche per mezzo di controlli a campione, il corretto svolgimento delle operazioni inerenti la gestione documentale.
Il Responsabile per la sicurezza informatica esegue periodicamente i controlli sul corretto funzionamento dei sistemi informatici in uso nell'Ente.

Misure di tutela e garanzia

Qualora l'Ente adotti misure minime di sicurezza avvalendosi di soggetti esterni alla propria struttura, per provvedere all'esecuzione, riceverà dall'installatore una descrizione scritta dell'intervento che ne attesti la conformità alle disposizioni del disciplinare tecnico di cui all'allegato b) del D.Lgs. 196/2003.

* * * * * *