



Comune di Farra di Soligo

Allegato 12 - PIANO DI SICUREZZA RELATIVO ALLA FORMAZIONE, ALLA GESTIONE, ALLA TRASMISSIONE, ALL'INTERSCAMBIO, ALL'ACCESSO, ALLA CONSERVAZIONE DEI DOCUMENTI INFORMATICI

Indice generale

Premessa.....	1
Elementi di rischio cui sono soggetti i documenti informatici e i dati contenuti nel Sistema di Gestione Informatica dei Documenti	2
Sicurezza della rete di accesso al servizio	2
Accesso al Sistema di Gestione Informatica dei Documenti e ai documenti e dati in esso contenuti da parte di utenti interni all'AOO	2
Trattamento dei dati personali e delle categorie particolari di dati di cui agli artt. 9-10 del Regolamento EU 2016/679 senza l'ausilio di strumenti elettronici	3
Formazione dei documenti.....	4
Sicurezza delle registrazioni di protocollo.....	4
Gestione dei documenti e sicurezza logica del Sistema.....	4
Backup e ripristino dell'accesso ai dati.....	5
Trasmissione e interscambio dei documenti	5
Conservazione dei documenti	6
Sicurezza fisica e infrastrutturale del Sistema	6
Accesso di Utenti esterni al Sistema.....	6
Piani formativi del personale	7
Monitoraggio periodico dell'efficacia e dell'efficienza delle misure di sicurezza	7
Misure di tutela e garanzia	7

Premessa

Il presente piano di sicurezza, adottato ai sensi dei punti 3.1.6 e 3.9 delle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici garantisce che:

- i documenti e le informazioni trattati dal Comune di Farra di Soligo siano resi disponibili, integri e riservati;
- i dati personali e le categorie particolari di dati di cui agli artt. 9-10 del Regolamento EU 2016/679 vengano custoditi mediante l'adozione di idonee e preventive misure di sicurezza, 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.

Il sistema garantisce inoltre:

- l'univoca identificazione ed autenticazione degli utenti;

- la garanzia di accesso alle risorse esclusivamente agli utenti abilitati e/o a gruppi di utenti secondo la definizione di appositi profili;
- il tracciamento permanente di qualsiasi evento di modifica delle informazioni trattate e l'individuazione del suo autore.

Il piano di sicurezza, che si basa sui risultati dell'analisi dei rischi a 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 dell'Ente;
- 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 ICT emanate dall'AgID con circolare del 18 aprile 2017, n. 2/2017 e adottate dal Comune di Farra di Soligo;
- i piani di formazione del personale;
- 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 SGID 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 dei dati personali, eccedente rispetto allo scopo o comunque non in linea con la normativa vigente.

Per prevenire tali rischi e le conseguenze da essi derivanti, l'Ente 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 dell'Ente non è esposto all'accesso attraverso la rete internet, ma opera all'interno di un sistema installato nella rete locale dell'Ente, ereditando dalla stessa tutti i meccanismi previsti per la sicurezza e la protezione, salvo l'accesso attraverso VPN protetto da crittografia.

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 identificazione; i profili di abilitazione alle funzionalità del Sistema stesso sono attribuiti a ciascun utente sulla base di quanto stabilito dal presente manuale di gestione. L'accesso ai documenti e ai dati presenti sul Sistema è definito in base al livello di riservatezza degli stessi.

Le credenziali di identificazione consistono in un codice (Userid), per l'identificazione dell'incaricato, associato ad una parola chiave riservata (Password), conosciuta solamente dal medesimo; tali credenziali vengono verificate in tempo reale dal 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'Userid corrispondente.

Agli incaricati è prescritto di adottare le necessarie cautele volte ad assicurare la segretezza della Password; la complessità relativa alla password viene stabilita dal sistema di gestione documentale in sede di inserimento ed è in linea con le Misure di sicurezza adottate e gli standard internazionali (come NIST, OWASP). La Password è modificata dall'incaricato al suo primo utilizzo e, successivamente, con cadenza prestabilita (ad esempio, semestrale o trimestrale).

L'Userid non può essere assegnato ad altri incaricati neppure in tempi diversi.

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.

Il personale del servizio 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.

Trattamento dei dati personali e delle categorie particolari di dati di cui agli artt. 9-10 del Regolamento EU 2016/679 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, fascicolo, sottofascicolo o inserto, secondo quanto stabilito dal manuale di gestione documentale; 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.

Le persone autorizzate al trattamento vengono formate in merito alle misure di sicurezza organizzativa, fisica e informatica per assicurare un corretto trattamento.

Trattamento dei dati personali e delle categorie particolari di dati di cui agli artt. 9-10 del Regolamento EU 2016/679 senza l'ausilio di strumenti elettronici

Ai fini del trattamento dei dati personali e delle categorie particolari di dati di cui agli artt. 9-10 del Regolamento EU 2016/679, sono impartite alle persone autorizzate istruzioni scritte da parte del Titolare del trattamento o di suo soggetto designato ai sensi dell'art. 2-quaterdecies del d.lgs. 196/2003 come novellato dal d.lgs 101/2018, relative alle modalità delle operazioni, del controllo e della custodia di atti e documenti.

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 suddetti documenti, sono controllati e custoditi dalle persone autorizzate per tutto il tempo di svolgimento dei relativi compiti, trascorso il quale provvederanno alla restituzione; nell'arco di tale periodo gli incaricati medesimi 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 dell'AOO sono prodotti utilizzando i formati previsti dal presente manuale di gestione documentale.

L'apposizione della firma digitale, volta a garantire l'attribuzione certa della titolarità del documento e la sua integrità, avviene, qualora sia necessario, previa conversione in un formato, tra quelli previsti, che garantisca la leggibilità, l'interscambiabilità, la non alterabilità, l'immutabilità nel tempo del contenuto e della struttura del documento medesimo; l'acquisizione mediante scansione dei documenti analogici avverrà in uno dei formati avente le medesime caratteristiche.

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 dalla normativa europea ed italiana vigenti.

Sicurezza fisica e infrastrutturale del Sistema

L'Ente si è dotato di una procedura di Disaster Recovery/Business Continuity in grado di assicurare la continuità delle operazioni indispensabili per il servizio e il ritorno alla normale operatività. La procedura di Disaster Recovery dell'Ente prevede che le copie di sicurezza siano localizzate in un secondo sito, posto comunque all'interno del territorio dell'Unione Europea. In caso di perdita dei dati il servizio di Disaster Recovery prevede il ripristino degli stessi e dell'accesso ad essi entro il quanto definito nel medesimo piano.

Sicurezza delle registrazioni di protocollo

L'accesso al registro di protocollo al fine di effettuare le registrazioni o di apportare modifiche è consentito soltanto al personale abilitato alla protocollazione.

L'accesso in consultazione all'intero registro di protocollo è consentito soltanto al personale del Servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi; i dipendenti che operano nell'ambito di altre UOR, uffici o servizi sono abilitati ad accedere esclusivamente ai dati di protocollo dei documenti da essi prodotti, ad essi assegnati o, comunque, di competenza della propria UOR 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 del manuale di gestione documentale, vengono registrate per mezzo di log di sistema che mantengano 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 SGID 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, al termine della giornata lavorativa, genera il registro giornaliero delle registrazioni di protocollo, in formato digitale; tale registro, formato nel rispetto di quanto previsto dalla normativa vigente, viene inviato nell'arco della giornata lavorativa successiva, al soggetto conservatore di cui l'Ente si serve.

Gestione dei documenti e sicurezza logica del Sistema

I documenti informatici, una volta registrati sul Sistema di Gestione Informatica dei Documenti, risultano immutabili 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 fornitore del software di gestione documentale assicura il corretto funzionamento del sistema e dei trattamenti eseguiti secondo i principi contenuti nel Regolamento UE 2016/679, in particolare agli artt. 24, 25 e 32.

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 malware mediante l'attivazione dei seguenti strumenti elettronici e/o dei seguenti software in esecuzione nel perimetro informatico dell'Ente ed interamente ai sistemi operativi:

- Unified Threat Management con funzionalità di deep packet inspection
- Sistemi di rilevamento delle intrusioni (HIDS e NIDS)
- Sistemi di analisi e notifica degli eventi di sicurezza (SIEM)
- Antivirus, Antimalware installati in tutte le postazioni di lavoro e nei sistemi server
- Politiche di gruppo volte a minimizzare i rischi di accesso abusivo e cancellazione non autorizzata e ad una corretta individuazione delle anomalie

Backup e ripristino dell'accesso ai dati

Il Backup dei dati contenuti nel Sistema di Gestione Informatica dei Documenti avviene nelle modalità descritte nel piano di Disaster Recovery e Business Continuity.

L'ente garantisce la corretta esecuzione giornaliera delle copie dati che vengono effettuate automaticamente:

- sui supporti SDD ove presenti;
- in sistemi di replica;
- sui NAS del sistema di backup dell'Ente;

I supporti di memorizzazione su cui sono memorizzati i dati sono custoditi a cura dell'Amministratore di Sistema dell'Ente (o del Responsabile del trattamento dei dati personali, qualora l'Ente affidi il servizio esternamente) al fine di evitare accessi non autorizzati e trattamenti non consentiti.

Il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici avviene secondo quanto previsto dalla procedura di Disaster Recovery e di Continuità operativa.

Nel caso di utilizzo di supporti rimovibili contenenti dati sensibili o giudiziari, cessato lo scopo per cui sono stati memorizzati, se non riscrivibili vengono distrutti, se riscrivibili possono venire cancellati e riutilizzati esclusivamente nel caso in cui le informazioni in essi contenute non siano intelligibili e in alcun modo ricostruibili.

Trasmissione e interscambio dei documenti

La trasmissione e l'interscambio di documenti e fascicoli informatici all'interno dell'Ente 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 dall'Ente sono compatibili con il protocollo SMTP definito nelle specifiche pubbliche RFC 821, 822, 2045, 2049, 2822, 5321 e S/MIME definito negli RFC 5750 e 5751.

Le informazioni relative alla segnatura di protocollo sono strutturate in un file conforme alle specifiche XML, compatibile con un file XML Schema, secondo quanto previsto nell'allegato 6 delle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici.

Conservazione dei documenti

I documenti informatici registrati sul SGID sono affidati per la conservazione digitale ad un soggetto conservatore accreditato ai sensi delle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici. Il trasferimento in conservazione avverrà mediante la produzione di pacchetti di versamento, basati su uno schema XML conforme a quanto previsto nel Manuale operativo del Portale della Conservazione a norma dei documenti digitali di Accatre. L'Ente prende atto delle misure di sicurezza adottate dal soggetto conservatore.

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, l'Ente predispone le apposite attività formative per il personale, con particolare riferimento ai seguenti temi:

- informatica, utilizzo del personal computer e della rete;
- utilizzo applicativi software per la produzione dei documenti informatici;
- utilizzo della posta elettronica certificata;
- utilizzo del Sistema di Gestione Informatica dei Documenti;
- politiche e aspetti organizzativi previsti nel manuale di gestione;
- legislazione e tematiche relative alla gestione documentale;
- legislazione, buone pratiche e misure tecniche ed organizzative in materia di protezione dei dati personali;
- aggiornamento sui temi suddetti.

Monitoraggio periodico dell'efficacia e dell'efficienza delle misure di sicurezza

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.

Misure di tutela e garanzia

Qualora l'Ente adotti misure di sicurezza avvalendosi di soggetti esterni, prima di provvedere all'applicazione delle stesse, riceve dal fornitore una descrizione scritta dell'intervento che ne attesti la conformità alle disposizioni di cui alle misure minime di sicurezza ICT emanate dall'AgID con circolare del 18 aprile 2017, n. 2/2017, nonché agli artt. 24, 25 e 32 del Regolamento UE 2016/679.

Qualora il contratto preveda la delega della gestione del monitoraggio della sicurezza delle informazioni, il fornitore sottoscriverà contestualmente al contratto la designazione a Responsabile del trattamento in conformità all'art. 28 del Regolamento UE 2016/679.