ALLEGATO N. 1

PIANO DI SICUREZZA DEL SISTEMA DI GESTIONE INFORMATICA DEI DOCUMENTI

Premessa

Il presente piano di sicurezza, descrive le politiche adottate dal A.T.E.R. di Matera affinché:

- i documenti e le informazioni trattati dall'Ente siano resi disponibili, integri e riservati;
- i dati 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 le Linee Guida AgID individuano 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 dell'Ente;
- le modalità di accesso al Sistema di Gestione Informatica dei Documenti;
- gli interventi operativi adottati sotto il profilo organizzativo, procedurale e tecnico, al fine di garantire le misure di sicurezza necessarie alla tutela del patrimonio documentale dell'Ente e alla tutela e garanzia dei 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 sarà soggetto a revisione a seguito di particolari esigenze, determinate da sopravvenienze normative o evoluzioni tecnologiche.

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, 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 A.T.E.R. Matera adotta gli accorgimenti e le politiche per la sicurezza di seguito descritte.

Procedure comportamentali degli operatori ai fini della protezione dei documenti informatici e dei dati in essi contenuti

Le postazioni di lavoro, da tavolo e portatili, o gli strumenti comunque funzionalmente assimilabili, di proprietà del A.T.E.R. di Matera a vario titolo messi a disposizione del personale, sono strumenti di lavoro e il loro utilizzo è finalizzato allo svolgimento delle attività professionali e istituzionali dell'Ente.

Ogni operatore adotta comportamenti corretti, tali da preservare il buon funzionamento degli strumenti e da ridurre i rischi per la sicurezza dei sistemi informativi.

Gli operatori cui sono affidati i dispositivi informatici di proprietà dell'ATER sono tenuti ad avere le seguenti accortezze:

- qualora nei dispositivi e nelle postazioni di lavoro siano memorizzati dati sensibili o giudiziari, l'operatore che li utilizza deve porre in atto comportamenti idonei a garantire la protezione di detti dati;
- ciascun operatore è tenuto a segnalare immediatamente ai referenti informatici ogni sospetto utilizzo non autorizzato, violazione della sicurezza o malfunzionamento relativo ai dispositivi informatici a lui assegnati;
- al momento della cessazione del rapporto di lavoro, ciascun operatore deve restituire all'Ente qualsiasi risorsa informatica a lui assegnata e mettere a disposizione ogni informazione di interesse istituzionale;
- non è consentito installare programmi non inerenti all'attività lavorativa;
- non è consentito copiare dati la cui titolarità sia del A.T.E.R. di Matera su dispositivi esterni personali.

Ai fini della vigilanza nell'utilizzo degli strumenti informatici assegnati, ciascun operatore ha l'obbligo di impedire ad altri l'utilizzo non autorizzato della propria apparecchiatura informatica.
Periodicamente, e comunque con cadenza almeno annuale, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.
Le stazioni di lavoro, da tavolo e portatili, o gli strumenti comunque funzionalmente assimilabili, messi a disposizione del personale, non devono essere lasciati incustoditi.
L'operatore è tenuto a bloccare o a spegnere il personal computer in caso di sospensione o termine dell'attività lavorativa e, comunque sempre, al termine dell'orario di servizio.
Per quanto non espressamente ivi contemplato, si applica il vigente "*Regolamento aziendale per l'utilizzo degli strumenti informatici*" (adottato con deliberazione dell'A.U. 0027/2023 DEL 28/03/2023).

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

La riservatezza delle registrazioni di protocollo è garantita dal sistema informatico di gestione del protocollo attraverso l'uso di profili utente e password.
L'accesso al Sistema di Gestione Informatica dei Documenti, da parte degli utenti interni all'AOO, avviene, difatti, attraverso l'utilizzo di credenziali di autenticazione. 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.
Agli incaricati è prescritto di adottare le necessarie cautele volte ad assicurare la segretezza della *Password*.
La *Password* è modificata dall'incaricato al suo primo utilizzo e, successivamente, con **cadenza trimestrale.**
Qualora il titolare delle credenziali di autenticazione dimenticasse la propria *password* si procederà all'assegnazione di una nuova chiave di accesso.
Le credenziali di accesso sono strettamente personali e ogni attività non regolare effettuata e riconducibile alle stesse è imputata al titolare delle credenziali medesime.
L'accesso diretto alla banca dati, l'inserimento di nuovi utenti, la modifica degli accessi e le impostazioni sui documenti sono consentiti agli amministratori del sistema.

Accesso al trattamento di dati personali sensibili o giudiziari e politiche di sicurezza espressamente previste
L'accesso ai documenti contenti 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 secondo quanto stabilito dall'art. 19 del presente manuale.
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, come precedentemente indicato, non possono lasciare incustodita e accessibile la propria postazione di lavoro durante il trattamento degli stessi.

Trattamento dei dati personali, sensibili o giudiziari anche 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 medesimi si assicureranno che a tali documenti non accedano persone prive di autorizzazione.

Sicurezza delle registrazioni di protocollo
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 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 il Sistema manterrà traccia. Per l'annullamento di una registrazione di protocollo vedasi quanto riportato nell'art.20 del presente manuale.
Al fine di garantire l'immodificabilità delle registrazioni di protocollo, il Sistema permette 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 alla struttura di conservazione accreditata di cui l'Ente si serve, secondo quanto previsto dall'articolo 21 del presente manuale.

Gestione dei documenti e sicurezza del Sistema
I documenti informatici, una volta registrati sul Sistema di Gestione Informatica dei Documenti, risultano immodificabili; 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 (log di sistema) sono protette al fine di non consentire modifiche non autorizzate. I dati registrati nei file di log sono raccolti, memorizzati e conservati dal sistema informatico in conformità alla normativa vigente.

La sicurezza fisica ha lo scopo di tutelare le persone, le strumentazioni e i locali e, in tale ambito è previsto quanto segue:

- il server su cui risiede il sistema di protocollo informatico dell'Amministrazione è riservato all'amministratore del sistema informatico aziendale;
- l'impianto di alimentazione del server è protetto da un gruppo di continuità.

La sicurezza logica è finalizzata all'implementazione dei requisiti di sicurezza nell'architettura informatica del sistema di protocollo, dotato di meccanismi opportuni e di specifiche funzioni di gestione e controllo ed in tale ambito è previsto quanto segue:

- controllo degli accessi, che consiste nel garantire che tutti gli accessi agli oggetti del sistema di protocollo informatico avvengano secondo modalità prestabilite;
- autenticazione, ovvero il meccanismo che consente ad un utente l'accesso ad un elaboratore solo dopo che lo stesso ha dimostrato la propria identità.
- confidenzialità, ovvero il criterio per cui ogni utente autorizzato può accedere ai soli documenti a cui ha diritto d'accesso in base al proprio ruolo nell'organigramma;
- integrità fisica dei dati, garantita da back-up quotidiani effettuati in automatico dal sistema;
- integrità logica, dei dati, assicurata da firewall e dal sistema antivirus centralizzato della rete informatica dell'Amministrazione, che impediscono l'intrusione di utenti/programmi non desiderati e dalla politica dell'accesso ai dati che consente ad ogni utente di svolgere solo le funzioni a cui è abilitato.

Backup e ripristino dell'accesso ai dati

Il sistema informatico, per la conservazione dei dati, garantisce che le informazioni in esso memorizzate siano consultabili ed estraibili.

Viene effettuata, in maniera automatica e giornaliera, copia del database generale del protocollo informatico nelle seguenti cartelle E:\tecnosys\BackupDB E:\tecnosys\eW del server "srv-gestionale".

Queste cartelle inoltre sono salvate, in maniera automatica e giornaliera, su un dispositivo di rete denominato NAS Synology nel quale vengono conservati 30 punti di ripristino (backup con storico).

In aggiunta alle copie del database di cui sopra, viene effettuata una copia completa, automatica e giornaliera e con diversi punti di ripristino nel tempo, del server "srv-gestionale" sui dispositivi di backup dell'infrastruttura centrale on-premises dell'Ente.

Il responsabile della gestione documentale vigila sulla corretta esecuzione delle operazioni di salvataggio della banca dati, effettuando controlli a campione.

Conservazione dei documenti

I documenti informatici registrati sul SGID sono affidati per la conservazione digitale ad un soggetto conservatore accreditato dall'AgID, che svolge tale attività in conformità a quanto sancito dalle regole contenute nelle Linee guida AgID. Il trasferimento in conservazione avviene mediante la produzione di pacchetti di versamento.

Formati elettronici adottati dall'ATER di Matera

Al fine di produrre e gestire documenti informatici che siano conformi alla normativa vigente e compatibili con un processo conservativo a lungo termine, l'A.T.E.R. Matera utilizza i formati elettronici individuati dalla normativa vigente come idonei alla conservazione.

Nell'utilizzo dei formati più comuni, l'Ente segue le indicazioni di seguito riportate:

- I documenti informatici prodotti dall'Ente, per poter essere acquisiti nel Sistema di Gestione Informatica dei Documenti, devono essere prodotti o convertiti in uno dei formati previsti dalle Linee Guida AgID; tale conversione avviene preferibilmente nei formati PDF o PDF/A;

- i documenti informatici prodotti dall'Ente, al fine di essere sottoscritti con firma digitale, vengono migrati nel sistema di gestione informatica previa conversione nel formato PDF o PDF/A, dopodiché viene apposto il numero di protocollo e sottoscritti con firma digitale;
- per l'acquisizione in formato digitale di documenti, nativamente prodotti in formato cartaceo, mediante l'attività di scansione, l'Ente può utilizzare i formati PDF, PDF/A, TIFF e JPG; l'utilizzo di quest'ultimo formato, tuttavia, avviene preferibilmente nella versione JPEG2000 (.jp2) perché può utilizzare una compressione senza perdita di informazioni e dunque senza pregiudicare la qualità dell'immagine;
- per l'acquisizione di documenti sottoscritti con firma digitale o altra sottoscrizione elettronica inviati all'AOO da parte di utenti esterni, l'ATER Matera richiede l'utilizzo dei formati PDF e PDF/A (costituiscono eccezione le fatture elettroniche, le quali sono in formato XLM);
- per la produzione di distinte di mandati, reversali informatici, fatture elettroniche viene utilizzato il formato XML conforme allo standard OPI.
- per l'acquisizione sul sistema di documenti che non necessitano di firma digitale o altra sottoscrizione elettronica l'ATER accetta, a seconda delle finalità per cui i documenti sono utilizzati, tutti i formati previsti dalla vigente normativa in materia, adatti ai fini della conservazione digitale; in tal caso possono essere utilizzati (oltre al PDF e PDF/A di cui si predilige) anche i formati RTF, ODF, OOXML (es. DOCX o XLSX) e TXT;
- ai fini della conservazione dei messaggi di posta elettronica lo standard a cui fare riferimento è RFC 2822/MIME, mentre per quanto riguarda il formato degli allegati al suddetto messaggio si utilizzeranno, a seconda della tipologia del documento trattato e delle esigenze, i formati elettronici precedentemente indicati;
- al fine della pubblicazione di documenti sul proprio sito istituzionale l'Ente utilizza i formati PDF/A;
- per la produzione del registro giornaliero di protocollo da inviare al conservatore accreditato l'Ente utilizza i formati PDF o PDF/A.
- per quanto riguarda la scelta di formati compressi, ai fini di un processo di conservazione a lungo termine sono sempre da preferire, laddove sia necessaria la compressione del file, formati con compressione di tipo lossless.

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 241/90 e s.m.i., dal D. Lgs. 196/03 e s.m.i. e del Regolamento Europeo sulla Protezione dei Dati n. 679 del 2016. Qualora l'utente esterno decida di esercitare il proprio diritto di accesso rivolgendosi direttamente all'ufficio protocollo 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, l'Ente predispone le apposite attività formative per il personale, con particolare riferimento ai seguenti temi:

- utilizzo del Sistema di Gestione Informatica dei Documenti;
- nozioni relative alle funzionalità di base del sistema di protocollo informatico;
- politiche e aspetti organizzativi previsti nel manuale di gestione documentale.

La formazione deve riguardare anche il personale del sistema informatico dell'Amministrazione relativamente agli aggiornamenti e al ripristino delle funzionalità del sistema, al salvataggio e conservazione

dei dati, alla cooperazione con la ditta fornitrice del software del protocollo per la risoluzione delle problematiche e per l'ottimizzazione dell'utilizzo dello stesso.

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 minime di sicurezza avvalendosi di soggetti esterni alla propria struttura, per provvedere all'esecuzione, riceverà dall'installatore una descrizione scritta dell'intervento che attesti la conformità dello stesso ai criteri di protezione dei dati sensibili, personali e giudiziari.