

## 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'art. 4, comma 1, lettera c), del DPCM 3/12/2013 "Regole tecniche per il protocollo informatico", garantisce che:

- 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'art. 7 del suddetto DPCM, individua i requisiti minimi di sicurezza dei sistemi di protocollo informatico a cui il presente piano si conforma.

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, 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;
- 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 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 **Comune di Donori** 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 Donori** non è esposto all'accesso attraverso la rete internet, ma opera all'interno di un server installato nella rete LAN dell'Ente denominato "SERVERCENTRALE" "COMUNEDONORI.LOCAL", 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, tra cui almeno un numero e un carattere maiuscolo e almeno due numeri e non contiene riferimenti

agevolmente riconducibili al titolare. La *Password* è modificata dall'incaricato al suo primo utilizzo e, successivamente, con cadenza mensile.

L'User-Id non può essere assegnato ad altri incaricati neppure in tempi diversi.

Le credenziali di autenticazione non utilizzate da parecchio tempo (non definito) 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 Responsabile 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.

L'Ente non ha nominato un Responsabile informatico.

#### **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, fascicolo, sottofascicolo o inserto, secondo quanto stabilito dall'art. 28 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, non viene 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.

Le credenziali di autenticazione di ciascun operatore dovrebbero essere consegnate in busta chiusa e sigillata al Responsabile dell'Area di riferimento (allo stato attuale non avviene); la consegna delle suddette password 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 non vengono, con tali password il Responsabile di settore verrebbe autorizzato ad utilizzare le credenziali contenute nella suddetta busta per procedere al trattamento, comunicandolo al titolare. Il soggetto titolare delle credenziali provvederebbe, 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**

Ai fini del trattamento dei dati personali, sensibili o giudiziari, sono impartite agli incaricati istruzioni scritte da parte del Responsabile per il trattamento dei dati personali, 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, dovrebbero avvenire con cadenza almeno annuale.

I suddetti documenti, sono controllati e custoditi dagli incaricati del trattamento 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 DPCM 3/12/2013 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 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.

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.

La sottoscrizione del documento con firma digitale avverrà prima dell'effettuazione della registrazione di protocollo.

### **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 al registro di protocollo è consentito sulla base dell'organizzazione dell'Ente: di norma, 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.

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'art. 28 del presente manuale, 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 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 l'Ente 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.

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'installazione 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 avviene nelle modalità che andiamo ad esplicitare.

Viene garantita la corretta esecuzione giornaliera delle copie dati che vengono effettuate automaticamente in Back-Up schedulati:

- Full Backup su Nas esterno (cadenza giornaliera) tramite Software di Backup MS

I supporti di memorizzazione su cui sono memorizzati i dati sensibili o giudiziari sono custoditi, sotto chiave, a cura del Responsabile della gestione documentale dell'Ente (o del Responsabile del trattamento dei dati personali) al fine di evitare accessi non autorizzati e trattamenti non consentiti.

**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/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 registrati sul SGID sono conformi ai requisiti e contengono i metadati previsti ai fini della conservazione permanente. 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.

### **Sicurezza fisica e infrastrutturale del Sistema**

L'Ente, a quanto disposto dall'art. 50-bis del D. Lgs 82/05, allo stato attuale non si è ancora dotato 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.

### **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 del D. Lgs. 196/03.

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, l'Ente predispone le 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.

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

L'Amministratore di Sistema (Ignazio Aru – Webtronica S.r.l.) controlla giornalmente i log di sistema e li mantiene per 6 mesi, al fine di verificare eventuali violazioni 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.

**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. 196/03.

In base al disposto dell'articolo 34, comma 1, del D. Lgs. 196/03 il trattamento dei dati personali effettuato mediante l'utilizzo di strumenti elettronici è subordinato al rispetto delle misure minime previste nell'allegato B) al Codice in materia di protezione dei dati personali *"Disciplinare tecnico in materia di misure minime di sicurezza"*.

Il trattamento dei dati dovrà impiegare modalità non invasive e attivare ogni possibile accorgimento finalizzato a salvaguardare la sfera privata altrui, come disposto dal D. Lgs. 196/03 e dal disciplinare tecnico di cui all'allegato b) del decreto legislativo stesso.