

ALLEGATO 14

§

PIANO DELLA SICUREZZA

SOMMARIO

PREMESSA.....	3
1 – ANALISI DEL RISCHIO.....	3
2 – MODALITÀ DI ACCESSO AL SISTEMA.....	4
3 – GESTIONE DEI DOCUMENTI E LORO SICUREZZA.....	5
4 – AUTORIZZAZIONI.....	6
5 - DISPOSIZIONI SPECIALI PER DOCUMENTI RISERVATI O CONTENENTI DATI SENSIBILI.....	7
6 – DELEGHE E SOSTITUZIONI.....	8
7 - MONITORAGGIO PERIODICO DELL'EFFICACIA E DELL'EFFICIENZA DELLE MISURE DI SICUREZZA	8
8 – MISURE DI TUTELA E GARANZIA.....	9
9 - ACCESSI NON AUTORIZZATI E SOTTRAZIONE DI DATI.....	9

PREMESSA

Il seguente Piano è redatto ai sensi del Paragrafo 3.9 delle Linee Guida per la Gestione Documentale e la Conservazione.

Esso definisce le misure tecniche e organizzative necessarie a garantire l'integrità, la disponibilità, la riservatezza e il valore giuridico-probatorio dei documenti informatici della ASL n. 5 di Oristano.

Descrive le misure da adottare ai fini di garantire che il Sistema di Gestione Documentale e le procedure messe in pratica per la gestione dei documenti ivi contenuti siano adeguate a garantire la tutela dei dati personali ai sensi dell'art. 32 del GDPR.

Il presente Piano, si basa sui risultati dell'analisi dei rischi a cui sono esposti i dati (personali, sensibili e non), e/o i documenti trattati, e su questa base 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 così come descritti nella circolare Agid 2/2017;
- la formazione degli addetti;
- le modalità con le quali deve essere effettuato il monitoraggio periodico dell'efficacia e dell'efficienza delle misure di sicurezza.

In linea con il riassetto del Servizio Sanitario Regionale, si stabilisce che:

- La ASL n. 5 di Oristano dipende da ARES Sardegna per la fornitura del software e per gli aspetti correlati all'ICT, in conformità a quanto previsto dalla L.R. n. 24 del 11/09/2020 ("Riforma del sistema sanitario regionale e riorganizzazione sistematica delle norme in materia...") e ss.mm.ii., come integrata e modificata dalla L.R. n. 8 dell'11/03/2025.
- La responsabilità della profilazione degli utenti e della conformità dei flussi documentali interni rimane in capo alla ASL n. 5 di Oristano (Referente della gestione documentale, RTD e DPO).
- La responsabilità della definizione dei requisiti di sicurezza, dell'adeguamento tecnologico dell'infrastruttura, dello sviluppo del software SISaR e dell'applicazione fisica delle misure di sicurezza logica è demandata ad ARES Sardegna in qualità di ente fornitore, Amministratore di Sistema e gestore dell'ICT.

1 – ANALISI DEL RISCHIO

I principali elementi di rischio cui sono soggetti i documenti informatici e i dati trattati attraverso il Sistema di Gestione Documentale dell'Ente sono essenzialmente riconducibili alle seguenti tipologie:

- Accesso non autorizzato, sia esso inteso come accesso al Sistema 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, in particolare rispetto ai principi di pertinenza e minimizzazione/non eccedenza.

Il sistema di gestione documentale è protetto mediante misure tecniche e organizzative coerenti con i rischi del trattamento, dettagliati nel resto del documento. In particolare:

- Autenticazione individuale degli utenti e gestione credenziali secondo policy dell'Ente;
- Profilazione e autorizzazioni per ruoli/gruppi, secondo principio di stretta necessità (Allegato 9 – Profilazione Tipo);
- Gestione delle utenze con privilegi elevati tramite account dedicati, non utilizzati per operatività ordinaria, con tracciamento e revisione periodica;
- Logging degli eventi rilevanti (accessi, consultazioni, operazioni su protocolli/fascicoli/documenti, annullamenti/correzioni, amministrazione profili), con conservazione e protezione dei log e accesso consentito ai soli soggetti autorizzati per finalità di sicurezza/audit;
- Backup periodici e test di ripristino;
- Aggiornamento e patching della piattaforma secondo pianificazione concordata con il fornitore, gli interventi di aggiornamento/manutenzione vengono anticipatamente indicati nelle Home Page dei software;
- Controlli periodici di coerenza tra profili assegnati e mansioni, almeno con cadenza annuale e comunque in caso di variazioni organizzative.

2 – MODALITÀ DI ACCESSO AL SISTEMA

Di norma, gli utenti autorizzati dall'Amministrazione hanno accesso al sistema di gestione documentale dell'Ente.

L'accesso avviene previa autenticazione con credenziali personali rilasciate dagli Amministratori di Sistema di ARES Sardegna previa autorizzazione scritta del Responsabile della Gestione Documentale o suo delegato. Se queste non coincidono con quelle rilasciate per l'accesso alla rete locale/Dominio Aziendale, devono essere attribuite con le modalità per queste stabilite.

Le politiche di sicurezza delle password sono le medesime di quelle adottate per l'accesso alla rete locale e comunque conformi a quanto indicato alla su citata circolare AgID 2/2017.

Il sistema di autenticazione, laddove sia diverso di quello di accesso alla LAN/Dominio Aziendale,

deve avere le medesime caratteristiche di sicurezza di quest'ultimo ed in particolare tenere traccia del log degli accessi eseguiti.

La cessione delle credenziali a terzi è severamente vietata e passibile di provvedimento disciplinare.

In applicazione di tale principio e in conformità alle direttive del Garante per la Protezione dei Dati Personali, è fatto tassativo divieto di comunicare le password delle caselle PEC istituzionali (@pec.asloristano.it) a fornitori di software esterni o terzi per consentire l'interoperabilità. L'integrazione e il recupero dei messaggi PEC all'interno dello Sistema di Gestione Documentale dovranno avvenire esclusivamente tramite protocolli di autenticazione sicura (es. Gateway dedicati, chiavi API o protocolli OAuth2) configurati e presidiati dal Dipartimento ICT di ARES Sardegna, senza visibilità delle credenziali da parte di soggetti esterni.

Le postazioni di lavoro non devono essere lasciate incustodite; in caso di momentanea assenza dell'operatore la postazione di lavoro deve essere spenta oppure l'utente deve scollegarsi dal sistema oppure la postazione deve essere bloccata in modo che per accedervi debba essere reintrodotta la password.

Gli utenti non più dipendenti dell'Amministrazione devono essere immediatamente disabilitati, salvo che per motivate esigenze relative al passaggio di consegne non sia necessario mantenerli attivi per un qualche limitato periodo. Tale eventualità deve essere esplicitamente autorizzata dal Responsabile per la Gestione Documentale o suo delegato ed essere il più breve possibile per consentire di terminare le operazioni di passaggio delle consegne.

Gli utenti assenti dal servizio per più di 30 giorni devono essere disabilitati e riabilitati al momento del loro rientro in servizio.

Se il Sistema è fruito al di fuori della rete locale (es. in modalità telelavoro / smartworking) oppure erogato attraverso un servizio Cloud, la connessione deve rispettare i criteri di sicurezza stabiliti da ACN e alla circolare 2/2017 di AgID, in particolare è necessario l'utilizzo di una VPN o di una connessione HTTPS basata su certificati rilasciati dalle apposite Autorità di Certificazione in corso di validità.

3 – GESTIONE DEI DOCUMENTI E LORO SICUREZZA

La sicurezza e la riservatezza dei documenti informatici è garantita dal Sistema di Gestione documentale dell'Ente.

Pertanto, i documenti formati o ricevuti dall'Ente devono essere memorizzati, gestiti e acceduti

esclusivamente attraverso il Sistema tramite le funzionalità da questo messe a disposizione.

I documenti sono accessibili limitatamente alle autorizzazioni concesse a ciascun utente secondo le modalità stabilite nel successivo paragrafo.

Il sistema assicura la tracciabilità delle operazioni mediante registrazione degli eventi di sicurezza e degli eventi applicativi rilevanti.

I log sono protetti da alterazioni, accessibili solo a profili autorizzati (es. amministratore di sistema per finalità tecniche; Responsabile sicurezza per verifiche), e conservati per un periodo coerente con le esigenze di sicurezza, accountability e accertamento di anomalie/incidenti. La durata di conservazione è definita in modo motivato e riesaminata periodicamente.

Non è consentita memorizzazione dei documenti all'esterno del Sistema. La loro trasmissione deve essere effettuata esclusivamente attraverso le funzionalità messe da questo a disposizione, mai attraverso caselle PEC/e-mail non sotto il suo controllo. Pertanto, l'accesso diretto alle suddette caselle può avvenire esclusivamente ad opera dell'Amministratore di Sistema o da persona incaricata per sole attività di manutenzione e previa richieste o autorizzazione del Responsabile della Gestione Documentale.

La sosta o l'archiviazione di documenti d'ufficio all'interno delle cartelle locali delle Postazioni di Lavoro (PDL) è da sconsigliare in quanto tale pratica può causare la perdita dei metadati di protocollo e dei vincoli archivistici, pertanto tali documenti dovranno transitare nel sistema di gestione documentale nel breve tempo possibile. Inoltre, ai sensi dell'art. 44 del CAD, per garantire l'inalterabilità e il valore legale nel tempo (evitando la scadenza dei certificati di firma) ed escludere sanzioni fiscali, l'Amministrazione demanda ad ARES Sardegna l'attivazione di flussi automatici e incrementali per l'invio al sistema di conservazione a norma del Registro giornaliero di protocollo, tutti i documenti fiscali, contratti, decreti, delibere e relativi fascicoli informatici.

L'inalterabilità dei documenti e delle registrazioni di protocollo e dei repertori sono garantite dal Sistema in base a quanto stabilite dalla normativa vigente in materia di gestione e tenuta del protocollo e dell'archivio digitale.

Il Responsabile della Gestione Documentale deve pertanto attivarsi con il fornitore per verificare, a fronte di ogni modifica alla normativa, che il software venga prontamente aggiornato.

4 – AUTORIZZAZIONI

Ogni utente deve essere dotato di un particolare profilo autorizzativo, autorizzato dal Responsabile della Gestione Documentale o suo delegato, che consente di operare secondo le autorizzazioni e i

limiti per questo stabiliti. L'autorizzazione all'uso delle diverse funzionalità del sistema (registrazione, modifica delle registrazioni, trasmissione dei documenti, ecc.) devono essere assegnate secondo il principio di stretta necessità. Funzioni non necessarie all'espletamento dell'attività di una persona non devono essere autorizzate.

In linea generale l'utente ha accesso ai soli documenti da lui prodotti e a quelli a cui è esplicitamente autorizzato. Le autorizzazioni di norma avvengono attraverso il processo di smistamento/assegnazione, che è tracciato dal sistema.

Le assegnazioni, al fine di garantire i principi di pertinenza e minimizzazione devono avvenire secondo i seguenti principi:

- Le assegnazioni di norma avvengono non a singoli utenti ma ad appositi gruppi definiti nel sistema; in genere, ma non sempre, legati a qualche UO; il singolo utente ottiene la visibilità dei documenti attraverso l'appartenenza a uno o più Gruppi/Scrivanie; in questo modo laddove un utente cambiasse, ad esempio, ufficio o in generale non appartenesse più ad un certo gruppo/scrivania, automaticamente non avrà più accesso ai documenti a questo assegnati;
- Le assegnazioni personali possono essere effettuate solo quando il documento è di stretta pertinenza della persona (ad esempio un provvedimento disciplinare a lui indirizzato);
- Le autorizzazioni e la visibilità dei documenti devono essere tassativamente modellate sulla base dei Ruoli istituzionali effettivamente ricoperti e non sulla base dell'intera Unità Organizzativa (UO), per garantire i principi di pertinenza e minimizzazione del GDPR.
- Il software SISaR deve essere adeguato da ARES Sardegna per permettere la storicizzazione del ruolo (es. RdP/RUP) e la revoca automatica e immediata di tutti i diritti di accesso pregressi non appena l'utente viene trasferito ad altro ufficio o servizio, superando il limite delle abilitazioni nominali permanenti;
- Le assegnazioni devono avvenire secondo il principio di pertinenza e le UO organizzate in gruppi/sotto-gruppi, secondo le specifiche funzioni svolte.

Sono comunque previsti speciali profili amministrativi in grado di accedere a tutti i documenti nel caso fosse necessario accedervi per accertate esigenze manutentive o urgenze; tali utenze non sono da utilizzare nel lavoro quotidiano e sono disponibili solo al Responsabile della Gestione Documentale o a suoi delegati.

5 - DISPOSIZIONI SPECIALI PER DOCUMENTI RISERVATI O CONTENENTI DATI SENSIBILI

Nel caso i documenti siano riservati e contengano dati sensibili il loro accesso è ulteriormente limitato dal sistema attraverso l'applicazione di opportuni livelli di riservatezza.

Per documenti di questo tipo il sistema garantisce:

- la non accessibilità, se non ai soggetti espressamente autorizzati alla loro gestione (es. il

- protocollo, non avrà accesso a questi documenti ma al più alla loro registrazione);
- la tracciatura di ogni operazione di accesso da parte di chi in possesso di credenziali amministrative;
 - l'eventuale inibizione di sub-assegnazioni.

Nella fase di registrazione di protocollo l'oggetto non dovrà contenere nessun riferimento alle informazioni sensibili e/o riservate contenute nel documento.

Il RdP (Responsabile del Procedimento), laddove valuti la necessità di ricorrere ad ulteriori misure (es. la cifratura), deve preventivamente informare il Responsabile della Gestione Documentale, in modo da poter stabilire delle modalità di accesso in caso di assenza e/o cessazione del RdP stesso.

È competenza di ARES Sardegna implementare funzioni native di mascheramento, cifratura logica e segregazione dei dati particolari (sanitari e giudiziari) direttamente a livello di database e file system centrale, garantendo al contempo un sistema di Audit Log indipendente, protetto e non manipolabile, in grado di tracciare ogni singolo accesso o tentativo di consultazione sui documenti classificati come riservati o sensibili.

6 – DELEGHE E SOSTITUZIONI

In caso di temporanea assenza di un soggetto, se il sistema lo consente (es. Procedura ATTI), è possibile delegare un utente ad accedere impersonificando l'utente da sostituire.

Il delegato avrà accesso ai documenti del delegante per tutto il periodo della delega. I permessi verranno revocati non appena la delega scadrà o verrà revocata. Le deleghe sono di norma autorizzate dal Responsabile della Gestione Documentale.

7 - MONITORAGGIO PERIODICO DELL'EFFICACIA E DELL'EFFICIENZA DELLE MISURE DI SICUREZZA

L'Amministratore di Sistema, su incarico del Responsabile della Gestione Documentale controlla periodicamente l'archiviazione dei log di sistema 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 alla gestione documentale.

Il monitoraggio include la verifica periodica, da effettuarsi in coordinamento con i tecnici di ARES Sardegna, della piena conformità dello Sistema di gestione documentale ai metadati obbligatori

previsti dall'Allegato 5 delle Linee Guida AgID (identificativi dell'aggregazione, soggetti istanti multipli, fasi del procedimento e tracciabilità degli stati dell'istanza), segnalando tempestivamente le anomalie strutturali del software SISaR per i successivi interventi correttivi centralizzati.

8 – 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 relative al trattamento dei dati personali.

Gli eventuali soggetti esterni che svolgono attività di assistenza, manutenzione, hosting o conservazione operano in qualità di responsabili del trattamento o soggetti autorizzati secondo gli atti e i contratti adottati dall'Ente. Gli accessi tecnici sono consentiti solo ove necessari, tracciati e governati tramite procedure interne (richiesta, autorizzazione, ticket e registrazione dell'intervento).

L'Amministratore di Sistema tratterà i dati contenuti nei sistemi di sicurezza, in modo da non eccedere le finalità per le quali gli stessi sono stati raccolti e solamente per il tempo strettamente necessario al conseguimento delle stesse; il trattamento dei dati dovrà impiegare modalità non invasive e attivare ogni possibile accorgimento finalizzato alla corretta tutela del dato personale.

9 - ACCESSI NON AUTORIZZATI E SOTTRAZIONE DI DATI

In caso si accertassero violazioni negli accessi e/o sottrazione di dati e documenti, il Responsabile della Gestione Documentale deve tempestivamente informare il DPO che provvederà a intraprendere le misure necessarie.