

LINEA GUIDA OPERATIVA PER LA REDAZIONE DELLE POLITICHE DI SICUREZZA (GV.PO-01)

Azienda Socio-Sanitaria Locale n.2 della Gallura

Sede Legale: via Bazzoni-Sircana, 2/2A – 07026 Olbia (SS)

Tel. 0789/552305 - www.aslgallura.it

Posta certificata: protocollo@pec.aslgallura.it

Codice Fiscale e Partita IVA: 02891650901

Redatto:

Dott. Ing. Martino Ruiu

LINEA GUIDA OPERATIVA PER LA REDAZIONE DELLE POLITICHE DI SICUREZZA (GV.PO-01)

Approvato con Delibera del Direttore Generale n. ____ del ____ .08.2026

Dipartimento Area Amministrativa

Edizione:
01/2026

Revisione: 00

Sommario

1	INQUADRAMENTO NORMATIVO E FINALITÀ	3
2	GOVERNANCE E ORGANIGRAMMA DELLA SICUREZZA	3
2.1	DESIGNAZIONI E RESPONSABILITÀ	3
2.2	UFFICIO DELLA CYBER SICUREZZA.....	3
3	INTEGRAZIONE OPERATIVA CON ARES SARDEGNA	4
4	REQUISITI MINIMI DI SICUREZZA (MISURE TECNICHE E ORGANIZZATIVE.....	4
5	GESTIONE DEGLI INCIDENTI E NOTIFICHE	5
6	STRUMENTI DI ATTUAZIONE E RISORSE.....	5
7	CLAUSOLE DI REVISIONE E AGGIORNAMENTO SANZIONATORIO	5
8	APPROVAZIONE E AGGIORNAMENTO DEL MANUALE, REGOLE TRANSITORIE E FINALI	ERRORE. IL SEGNALIBRO NON È DEFINITO.
8.1	MODALITÀ DI APPROVAZIONE E AGGIORNAMENTO DEL MANUALE	ERRORE. IL SEGNALIBRO NON È DEFINITO.
8.2	PUBBLICITÀ DEL PRESENTE MANUALE	ERRORE. IL SEGNALIBRO NON È DEFINITO.
9	ALLEGATI.....	6

1 INQUADRAMENTO NORMATIVO E FINALITÀ

La presente Linea Guida definisce i requisiti cogenti e l'assetto operativo delle Politiche di sicurezza informatica (GV.PO-01) della ASL Gallura. Il documento stabilisce le misure tecniche e organizzative minime necessarie a garantire la resilienza, l'integrità e la riservatezza dei sistemi informativi aziendali, in conformità con le strategie nazionali di protezione delle infrastrutture critiche sanitarie. L'adozione e l'attuazione della policy GV.PO-01 sono vincolate al rispetto rigoroso del seguente quadro normativo:

- **Direttiva (UE) 2022/2555 (NIS2)** e relativo recepimento tramite **D.Lgs. 4 settembre 2024, n. 138**.
- **Legge 28 giugno 2024, n. 90** (Disposizioni in materia di cybersicurezza).
- **Determinazione ACN prot. n. 127434/2026** relativa alle "Specifiche di base ACN 2025" e versione 2.1 della relativa "Guida alla lettura".
- **D.L. 14 giugno 2021, n. 82** (Architettura Nazionale di Cybersicurezza).

2 GOVERNANCE E ORGANIGRAMMA DELLA SICUREZZA

2.1 DESIGNAZIONI E RESPONSABILITÀ

Ai sensi della Determinazione del Direttore Generale di ACN prot. N. 127437 del 13 aprile 2026, si formalizzano le seguenti figure e responsabilità:

- **Approvazione:** La Politica GV.PO-01 è approvata dalla Direzione Strategica nelle figure del Direttore Generale, **Dott. Antonio Irione**, e del Direttore Amministrativo, **Dott. Michele Baffigo**.
- **Punto di Contatto (PdC):** **Ing. Martino Ruiu** (Direttore SC Tecnologia e Transizione Digitale), già designato con prot. PG/2025/6544 e ratificato formalmente in data 19/05/2026. Egli è il referente primario per l'interlocuzione con l'Agenzia per la Cybersicurezza Nazionale (ACN).
- **Sostituto Punto di Contatto (SPdC):** **Ing. Francesca Mura** (IFP Telemedicina), incaricata di assicurare la continuità degli adempimenti e la gestione dei dati sulla piattaforma NIS in caso di assenza del PdC.
- **Segreteria Tecnica (SG):** **Dott. Ciro Soro**, responsabile del supporto amministrativo e del monitoraggio delle scadenze regolatorie.

2.2 UFFICIO DELLA CYBER SICUREZZA

Si dispone che il Direttore della SC Tecnologia e Transizione Digitale provveda a istituire l'atto di costituzione formale dell'Ufficio della Cyber Sicurezza, d'intesa con ARES Sardegna. Tale ufficio deve operare come presidio permanente per la gestione delle richieste di ACN e l'attuazione delle

procedure di resilienza aziendale.

3 INTEGRAZIONE OPERATIVA CON ARES SARDEGNA

In virtù della L.R. 24/2020, che affida ad ARES Sardegna la gestione esclusiva dell'infrastruttura tecnologica, la ASL Gallura impone una cooperazione tecnica costante con i referenti del CSIRT regionale.

- **Referenti CSIRT ARES:** Il coordinamento operativo è demandato ai CSIRT nominati da ARES: **Ing. Gaviano**, all'**Ing. Frau** e al **Sig. Fenudi**.
- **Tavolo Tecnico Congiunto:** Deve essere istituito un Tavolo Tecnico permanente tra ASL Gallura e ARES Sardegna. In ottemperanza alla **Nota prot. PG/2026/20130 del 19/05/2026**, il Tavolo deve riunirsi con **frequenza bisettimanale** nella fase di prima implementazione 2026, garantendo l'aggiornamento tempestivo dei registri NSIS e la validazione dei dati anagrafici (Domini, IP, Fornitori).

4 REQUISITI MINIMI DI SICUREZZA (MISURE TECNICHE E ORGANIZZATIVE)

La ASL Gallura propone l'adozione delle seguenti misure di sicurezza, mappate secondo il framework ACN, per mitigare i rischi cyber sulle infrastrutture critiche:

Codice Controllo	Descrizione Misura	Specifiche di Attuazione
ID.RA-05	Valutazione del rischio	Esecuzione periodica di analisi del rischio metodologica sugli asset critici sanitari.
PR.AA-03	Autenticazione Forte (MFA)	Obbligo di Multi-Factor Authentication per ogni accesso remoto e per tutte le utenze privilegiate/amministrative.
PR.DS-11	Backup offline	Implementazione di soluzioni di backup immutabili e fisicamente disconnessi dalla rete (air-gapped).
DE.CM-09	Protezione endpoint	Adozione di soluzioni avanzate di EDR/XDR e monitoraggio continuo (24/7) per il rilevamento di intrusioni sulle postazioni di lavoro.
GV.SC-01	Sicurezza dei fornitori	Inserimento obbligatorio di clausole contrattuali di cybersicurezza allineate ai requisiti del D.Lgs. 138/2024 per tutti i fornitori critici.

5 GESTIONE DEGLI INCIDENTI E NOTIFICHE

Ai sensi degli Articoli 24 e 25 del D.lgs. 138/2024, la gestione degli incidenti informatici segue un protocollo di escalation tassativo:

1. **Rilevamento:** Identificazione tecnica dell'anomalia da parte dei referenti ARES Sardegna.
2. **Validazione:** Analisi dell'impatto e classificazione dell'evento come "incidente significativo".
3. **Notifica Nazionale:** Il PdC (Ing. Martino Ruiu) o il SPdC (Ing. Francesca Mura) provvedono all'invio della notifica al **CSIRT Italia tramite il portale ACN entro 24 ore** dal momento in cui l'ente ne diviene consapevole.

6 STRUMENTI DI ATTUAZIONE E RISORSE

Il potenziamento dei sistemi di difesa e l'adeguamento tecnologico sono veicolati prioritariamente attraverso i Piani Operativi Lotto 2 Consip. Ogni intervento tecnico deve essere validato dal Tavolo Tecnico Congiunto per garantire la piena compatibilità con l'Architettura regionale centralizzata e gli standard di resilienza definiti a livello nazionale.

7 CLAUSOLE DI REVISIONE E AGGIORNAMENTO SANZIONATORIO

La politica GV.PO-01 è soggetta a revisione annuale o in occasione di mutamenti sostanziali del perimetro informatico.

Si ribadisce la scadenza perentoria del 31 maggio di ogni anno per l'aggiornamento dell'anagrafica e delle informazioni sulla Piattaforma NIS di ACN. Il mancato rispetto di tale termine o l'omesso aggiornamento delle informazioni costituiscono una violazione normativa diretta ai sensi del D.Lgs. 138/2024, soggetta alle sanzioni amministrative pecuniarie previste dal medesimo decreto.

8 DISPOSIZIONI FINALI, APPROVAZIONE E PUBBLICITÀ

8.1 MODALITÀ DI APPROVAZIONE E AGGIORNAMENTO

L'amministrazione adotta la presente "Linea Guida Operativa per la Redazione delle Politiche di Sicurezza (GV.PO-01)" su proposta del Responsabile per la Transizione Digitale (RTD).

In conformità alle specifiche di base dell'Agenzia per la Cybersicurezza Nazionale (ACN), il documento GV.PO-01 rientra tra gli 11 elaborati che devono essere obbligatoriamente approvati dagli organi di amministrazione e direttivi.

Pertanto, l'adozione formale avviene con Deliberazione del Direttore Generale (DG), acquisiti i pareri del Direttore Amministrativo e del Direttore Sanitario, quali figure di vertice responsabili della governance della sicurezza informatica.

LINEA GUIDA OPERATIVA PER LA REDAZIONE DELLE POLITICHE DI SICUREZZA (GV.PO-01)

Considerata la natura transitoria del presente atto, adottato con carattere di urgenza nelle more del completamento delle attività tecnico-documentali coordinate da ARES Sardegna (attraverso i Piani Operativi Consip Lotto 2), la guida sarà oggetto di revisione obbligatoria nei seguenti casi:

- Evoluzione normativa: recepimento di nuove disposizioni nazionali o europee (es. piena attuazione del D.Lgs. 138/2024 - NIS2 o della L. 90/2024);
- Armonizzazione regionale: adozione delle politiche di sicurezza definitive elaborate da ARES Sardegna per garantire l'uniformità di indirizzo e la coerenza operativa su tutto il perimetro sanitario regionale;
- Miglioramento continuo: introduzione di nuove pratiche organizzative o tecnologiche volte a incrementare la resilienza cibernetica dei servizi sanitari;
- Esiti di monitoraggio: qualora le attività di risk assessment o l'analisi di incidenti informatici evidenzino l'inadeguatezza delle procedure correnti.

8.2 PUBBLICITÀ E DIFFUSIONE

Al fine di garantire la massima trasparenza e l'accountability dell'Ente, il presente documento è:

- Pubblicato sul sito istituzionale dell'amministrazione all'interno della sezione "Amministrazione Trasparente", ai sensi del D.Lgs. 33/2013;
- Reso disponibile nella INTRANET aziendale, affinché sia facilmente consultabile da tutti gli operatori che utilizzano i sistemi informativi e di rete rilevanti;
- Trasmeso formalmente ai Direttori delle UOR (Unità Organizzative Responsabili) e ai fornitori ICT critici, per il recepimento dei principi di sicurezza negli ambiti di rispettiva competenza.

9 ALLEGATI

Allegato n. 1: ASL Gallura Cybersecurity Governance