POLITICA AZIENDALE PER LA SICUREZZA DELLE INFORMAZIONI

ai sensi dell'art. 32 del Regolamento (UE) 2016/679 Revisione 02 – Aggiornamento 2026

REGISTRO DELLE REVISIONI	
Rev. 01	Delibera di CdA n. 07 del 13/04/2026
Rev. 02 – 12/08/2026	Integrazione: DPO esterno; contitolarità E-KILLER; aggiornamento misure tecniche; allineamento a Procedura Data Breach (SRR_13) e Procedura Diritti (SRR_14)

ARTICOLO 1 – SCOPO E AMBITO DI APPLICAZIONE

1.1 La presente Politica definisce i principi, gli obiettivi e le regole fondamentali per la sicurezza delle informazioni trattate dalla S.R.R. Enna Provincia ATO 6, al fine di garantire la riservatezza, l'integrità e la disponibilità dei dati personali e delle informazioni aziendali.

1.2 Si applica a: tutto il personale (dipendenti, collaboratori, personale in comando); Responsabili del trattamento (3S Telematica, Vitruvio Tech); Contitolari (Libero Consorzio Comunale); visitatori e soggetti terzi che accedono ai locali o ai sistemi.

1.3 Le misure sono definite ai sensi dell'art. 32 del GDPR, tenendo conto dello stato dell'arte, dei costi di attuazione, della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà degli interessati.

ARTICOLO 2 – PRINCIPI GENERALI

- **Riservatezza:** le informazioni sono accessibili solo ai soggetti autorizzati, nei limiti delle proprie competenze.
- **Integrità:** le informazioni sono protette da modifiche non autorizzate, garantendo completezza e correttezza.
- **Disponibilità:** le informazioni e i sistemi sono accessibili e utilizzabili dai soggetti autorizzati nei tempi previsti.
- **Accountability:** ogni azione sui dati è tracciabile e attribuibile a un soggetto identificato.
- **Minimizzazione:** i dati trattati sono limitati a quanto necessario per le finalità del trattamento.

ARTICOLO 3 – GOVERNANCE DELLA SICUREZZA

RUOLO	SOGGETTO	RESPONSABILITÀ SICUREZZA
Titolare / Presidente	Dott. Antonio Licciardo	Approvazione politiche; decisioni su investimenti sicurezza; disposizione notifiche data breach
DPO	Avv. Gianvito Rizzini	Sorveglianza, consulenza, audit privacy, gestione violazioni, formazione

RTD	Dott. Di Mattia Fabrizio	Coordinamento ICT; implementazione misure tecniche; gestione incidenti informatici
Referente Privacy	Arch. Nicolò Mazza	Punto di contatto operativo DPO; coordinamento interno
RT ICT – 3S Telematica	Ing. Andrea Nardelli	Gestione infrastruttura; backup; firewall; antivirus; monitoraggio
RT E-KILLER – Vitruvio Tech	Sig. Massimiliano Nenni	Sicurezza sistema videosorveglianza; crittografia; digital watermarking

ARTICOLO 4 – MISURE DI SICUREZZA TECNICHE

MISURA	DESCRIZIONE	RESPONSABILE
Autenticazione	Server Windows con dominio aziendale e SSO; credenziali nominative per tutti i sistemi (XTime, Amica 2.0, ProtocolloPA)	3S Telematica
Policy password	Complessità minima 8 caratteri; cambio trimestrale; blocco dopo 5 tentativi falliti	3S Telematica
Firewall	Con web filtering e content filtering; protezione perimetrale della rete	3S Telematica
Antivirus EDR	Su server e postazioni; aggiornamento automatico; monitoraggio centralizzato	3S Telematica
Backup	Giornaliero su NAS locale + cloud; test di ripristino periodico	3S Telematica
UPS	Protezione alimentazione server e apparati critici	3S Telematica
Crittografia E-KILLER	AES 256 su Micro SD; trasmissione 4G/LTE crittografata; digital watermarking	Vitruvio Tech
Accesso E-KILLER	Credenziali nominative; accesso solo dalla Sala Operativa Polizia Provinciale; flag esclusione PM	Vitruvio Tech / LCC
Log accessi	Registrazione accessi ai sistemi E-KILLER conservati 6 mesi	Vitruvio Tech
Monitoraggio rete	Sistema di alert automatici per anomalie	3S Telematica
HTTPS	Protocollo sicuro per il sito web istituzionale	3S Telematica

ARTICOLO 5 – MISURE DI SICUREZZA ORGANIZZATIVE

- **Designazione autorizzati:** tutto il personale è designato ex art. 29 GDPR con istruzioni operative scritte (SRR_03).
- **Formazione:** programma annuale obbligatorio per tutto il personale (SRR_16).
- **Procedura Data Breach:** procedura formalizzata con tempi, ruoli e moduli (SRR_13).
- **Procedura Diritti:** procedura per la gestione delle istanze degli interessati (SRR_14).

- **Nomine Responsabili:** tutti i fornitori che trattano dati personali sono nominati ex art. 28 GDPR (SRR_04, SRR_05, SRR_06).
- **Contitolarità:** accordo ex art. 26 GDPR con il Libero Consorzio Comunale (SRR_07).
- **DPIA:** valutazione d'impatto condotta e aggiornata per il sistema E-KILLER (SRR_12).
- **Registro trattamenti:** redatto e aggiornato ex art. 30 GDPR (SRR_02).
- **Informative:** complete per tutte le categorie di interessati (SRR_08, SRR_09, SRR_10, SRR_11).
- **Documentazione cartacea:** custodia in armadi chiusi a chiave; distruzione mediante distruggi-documenti.
- **Clean desk:** obbligo di non lasciare documenti contenenti dati personali incustoditi sulla scrivania.

ARTICOLO 6 – SICUREZZA FISICA

- accesso ai locali della sede controllato;
- server e apparati di rete in locale dedicato ad accesso limitato;
- UPS a protezione dei sistemi critici;
- Sala Operativa Polizia Provinciale ad accesso riservato al solo personale autorizzato per il sistema E-KILLER.

ARTICOLO 7 – GESTIONE DEGLI INCIDENTI

La gestione degli incidenti di sicurezza (data breach) segue la procedura SRR_13. Ogni incidente è documentato nel Registro delle Violazioni e, se necessario, notificato al Garante e comunicato agli interessati.

ARTICOLO 8 – AUDIT E VERIFICHE

8.1 Il DPO effettua verifiche periodiche (almeno annuali) sulle misure di sicurezza adottate, anche mediante audit presso i Responsabili del trattamento.

8.2 I risultati degli audit sono documentati e comunicati al Presidente, con eventuali raccomandazioni di adeguamento.

8.3 Il RTD e 3S Telematica eseguono test di vulnerabilità periodici sull'infrastruttura informatica.

ARTICOLO 9 – CESSAZIONE DEL RAPPORTO

Al termine del rapporto di lavoro o di servizio, si procede a: revoca delle credenziali di accesso; restituzione dei dispositivi aziendali; cancellazione dei dati personali dai dispositivi restituiti; aggiornamento del Registro Trattamenti e delle nomine.

ARTICOLO 10 – RIESAME E AGGIORNAMENTO

La presente Politica è riesaminata con cadenza annuale o in occasione di: variazioni organizzative significative; incidenti di sicurezza; evoluzioni normative; risultati degli audit.

Le modifiche sono approvate dal CdA, previo parere del DPO.

Il Presidente S.R.R.
Dott. Antonio Licciardo

Firmato digitalmente da:
Licciardo Antonio
Firmato il 12/08/2026 13:12
Seriale Certificato: 5735363
Valido dal 17/02/2026 al 17/02/2029
InfoCamere Qualified Electronic Signature CA

Visto Il DPO
Avv. Gianvito Rizzini
dpo@srrennaprovincia.it