Annex principale di riferimento:	5	
Revisione:	00 Ed. I	
Data della revisione:	16 12 2025	
Autore:	Andea Cannaos	
Revisione:	Francesca Torta	
Approvazione	CdA	Delibera n. xx del 16 12 2025
Grado di riservatezza:	Uso Pubblico	

Indice delle revisioni

Data	*Rev.*	*Descrizione delle revisioni*
16 12 2025	00	Prima emissione

Il CdA di **Nova Aeg** ha deciso di progettare e rendere operante un **Sistema di Gestione della Sicurezza delle Informazioni** conforme ai requisiti della norma internazionale ISO/IEC 27001:2022 e in linea con i requisiti della Direttiva (UE) 2022/2555 del Parlamento Europeo e del Consiglio del 14 dicembre 2022 (NIS2) relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, per meglio strutturare i propri processi ed ottimizzare la sua organizzazione al fine di rendere coerenti gli obiettivi di Sicurezza delle Informazioni con le proprie linee strategiche, divenute essenziali e determinanti nel mercato molto particolare e in continua evoluzione in cui **Nova Aeg** opera.

La Direzione di **Nova Aeg** ha analizzato il contesto in cui opera ed identificato le parti interessate dalla propria attività. Da questa analisi ha evinto le parti interessate rilevanti e identificato i requisiti delle stesse, impliciti ed espliciti, che si impegna a soddisfare.
Da tale raccolta dati deriva l'elaborazione, da parte della Direzione, della pianificazione aziendale e l'identificazione degli obiettivi aziendali.

Per **Nova Aeg** la sicurezza delle informazioni ha come obiettivo primario la soddisfazione del cliente (interno ed esterno), che si traduce nella protezione dei dati e delle informazioni e nella gestione della struttura tecnologica, fisica, logica ed organizzativa. Proteggere i dati, anche personali, di tutti i nostri interessati al trattamento è per noi fondamentale. Lo stesso impegno lo chiediamo quindi a tutti i nostri stakeholders (fornitori, collaboratori, business partner, consorziati, aziende partecipate e collegate). Questo significa ottenere e mantenere un sistema di gestione sicura delle informazioni, nell'ambito del campo di applicazione definito per l'Information Security Management System (ISMS), attraverso il rispetto delle seguenti proprietà:

1. **Riservatezza**: assicurare che l'informazione sia accessibile solamente ai soggetti e/o ai processi debitamente autorizzati;
2. **Integrità**: salvaguardare la consistenza dell'informazione da modifiche non autorizzate;
3. **Disponibilità**: assicurare che gli utenti autorizzati abbiano accesso alle informazioni e agli elementi associati quando ne fanno richiesta.
4. **Privacy**: in ottemperanza dell'art.24 del "Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE" ("GDPR").

Per perseguire questi obiettivi di primo livello in obiettivi pianifichiamo obiettivi di secondo livello correlati alla corretta adozione di controlli operativi ("misure tecnico organizzative") applicabili per il trattamento dei rischi. La presente politica può quindi richiamare politiche più operative che indirizzano specifici aspetti di protezione dei dati personali.

Nell'ambito della gestione dei servizi offerti **Nova Aeg** assicura:
• il miglioramento continuo della sicurezza delle informazioni, reale e percepita, dei propri prodotti/servizi, attraverso il miglioramento tecnologico dell'esistente e con un metodo di lavoro predisposto alla ricerca ed innovazione continua
• la soddisfazione dei requisiti impliciti ed espliciti del cliente
• L'efficace gestione del funzionamento e della sicurezza dei servizi erogati in cloud
• la completa osservanza delle Service Level Agreement stabilite con i clienti
• il rispetto delle normative vigenti e degli standard internazionali di sicurezza
• la gestione della sicurezza delle informazioni nei rapporti con fornitori e outsourcers di servizi cloud e verso i clienti
• la garanzia di affidare a partner affidabili e qualificati il trattamento del proprio patrimonio informativo
• l'impegno a trattare i dati personali degli interessati in conformità ai principi richiamati dall'Articolo 5 del GDPR e di seguito riportati:

- liceità, correttezza e trasparenza dei trattamenti;
- finalità determinate, esplicite, legittime;
- dati adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);
- dati esatti e, se necessario, aggiornati; sono adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);
- dati conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi esclusivamente a fini di archiviazione e previa l'attuazione di misure tecniche e organizzative adeguate a

tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»);

- dati trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).

La politica della Sicurezza delle Informazioni di **Nova Aeg** si ispira ai seguenti principi:
a. Garantire all'organizzazione la piena conoscenza delle informazioni gestite e la valutazione della loro criticità, al fine di agevolare l'implementazione degli adeguati livelli di protezione.
b. Garantire l'accesso sicuro alle informazioni, in modo da prevenire trattamenti non autorizzati o realizzati senza i diritti necessari.
c. Garantire che l'organizzazione e le terze parti collaborino al trattamento delle informazioni adottando procedure volte al rispetto di adeguati livelli di sicurezza.
d. Garantire la sicurezza fisica e logica degli information asset e degli asset operativi.
e. Garantire la conformità con i requisiti di legge ed il rispetto degli impegni di sicurezza stabiliti nei contratti con le terze parti.
f. Garantire la rilevazione di eventi anomali, incidenti e vulnerabilità dei sistemi informativi al fine di rispettare la sicurezza e la disponibilità dei servizi e delle informazioni.
g. Garantire la business continuity aziendale e il disaster recovery, attraverso l'applicazione di procedure di sicurezza stabilite.

La politica della sicurezza delle informazioni è formalizzata nell'ISMS, viene costantemente aggiornata per assicurare il suo miglioramento continuo ed è condivisa con l'organizzazione, le terze parti ed i clienti, attraverso un sistema intranet e specifici canali di comunicazione.

Vercelli, lì 16 12 2025

Il Consiglio di Amministrazione