Strategia di Sicurezza delle Informazioni

Codice	DOC-ICT-0103
Versione	1.0
Classificazione	Pubblico [PU] - ICT

Redazione e Approvazione

La firma in calce attesta l'approvazione del presente documento e ne autorizza l'emissione e l'entrata in vigore.

	Nome	Funzione	Data
Redazione	Nicola Tigri	CISO	23/03/2026
Revisione	Enrico Garbin	Ufficio Legale	26/03/2026
	Alessandro Speri	CIO	26/03/2026
Approvazione Finale	Erardo Ratzenbeck	CEO	27/04/2026
		In vigore dal	**28/04/2026**

Registro delle Versioni

La seguente tabella contiene il registro delle modifiche significative apportate al documento.

Versione	Data	Autore	Descrizione della Modifica
1.0	27/04/2026	Nicola Tigri (CISO)	Primo rilascio

1. Introduzione

Athena è impegnata a proteggere la riservatezza, l'integrità e la disponibilità delle informazioni aziendali, garantendo la continuità operativa, la conformità normativa e la riduzione dei rischi cyber. La presente Strategia definisce i principi, gli obiettivi e il perimetro delle politiche di sicurezza che costituiscono il Sistema di Gestione della Sicurezza delle Informazioni (SGSI), in coerenza con **ISO/IEC 27001:2022**, della **VDA ISA (TISAX)** e con i requisiti normativi applicabili, inclusa la **NIS2** (d.Lgs. 138/2024) per cui la società è classificata "**Soggetto Importante**".

2. Obiettivi della Strategia di Information Security

- Proteggere la riservatezza, integrità e disponibilità delle informazioni.
- Garantire la conformità alle leggi e ai regolamenti pertinenti (ad es. GDPR, NIS2).
- Minimizzare i rischi associati a minacce interne ed esterne.
- Promuovere una cultura della sicurezza all'interno dell'organizzazione.

3. Valutazione dei Rischi

La Società procede periodicamente:

- **all'identificazione dei Rischi**,
  Conducendo un'analisi per identificare le minacce potenziali (malware, phishing, insider threats, ecc.);
- **alla valutazione**
  dell'impatto e la probabilità di ciascun rischio e classificando le vulnerabilità.
- **alla realizzazione del Piano di Mitigazione**,
  sviluppando strategie per mitigare i rischi identificati.

4. Politiche di Sicurezza

Athena ha enucleato l'impianto SGSI, in differenti politiche su tematiche specifiche, quali a titolo esemplificativo: Sistema di Gestione della Sicurezza delle Informazioni & Governance, Asset Management ed Uso accettabile delle Informazioni, Third Party Risk Management, Policy di Gestione Change Request e nuove progettualità, Patch & Vulnerability Management, Gestione della crittografia, Gestione degli Incidenti di Sicurezza.

5. Formazione e Sensibilizzazione

La Società, riconoscendo il ruolo fondamentale dell'utente nella Strategia di Information Security, definisce:

- **Programmi di Formazione**:
  Erogando corsi di formazione regolari per tutti i dipendenti sulla sicurezza informatica e sulle migliori pratiche.
- **Simulazioni di Phishing**:
  Conducendo esercitazioni di simulazione per sensibilizzare i dipendenti sulle minacce di phishing.

6. Sicurezza Tecnologica

Altresì, a difesa della confidenzialità, integrità e disponibilità delle informazioni, la Società dispone di:

- **Firewall e Antivirus/EDR**
  A difesa della perimetrale adotta da un lato sistemi di rilevamento delle intrusioni e monitoraggio del traffico di rete per finalità di sicurezza, nel rispetto delle normative applicabili, dall'altro di difesa degli end-point.
- **Sistemi di Crittografia**.
  Utilizzando la crittografia per proteggere i dati sensibili sia a riposo che in transito.
- **Backup dei Dati e/o Disaster Recovery**:
  Implementando un piano di backup regolare e di continuità operativa al fine di garantire, come detto sopra, la disponibilità dei dati.

7. Monitoraggio e Audit

La Società, riconoscendo l'importanza del fenomeno del cybercrime e l'importanza dei dati gestiti, procede al

- **Monitoraggio Continuo**,
  Implementando sistemi di monitoraggio per rilevare attività sospette in tempo reale.
- **Audit di Sicurezza**,
  Conducendo audit di sicurezza periodici per valutare l'efficacia delle misure di sicurezza e identificare aree di miglioramento. Ciò anche contemperando attività di Penetration Testing e Network Vulnerability Assessment.

8. Gestione degli Incidenti di Sicurezza

La Società, nell'ottica della trasparenza e del rispetto delle norme, ha sviluppato/previsto:

- **Piano di Risposta agli Incidenti**,
  prevedendo un piano di risposta agli incidenti che delinei le procedure da seguire in caso di violazione della sicurezza (punto 4 – Contingency plan e Incident Handling)
- **Comunicazione**,
  processi per garantirne sia quella interna che esterna (EBP ed Autorità come ACN e CSIRT) in caso di incidenti di sicurezza.

9. Conformità e Regolamentazione

- **Monitoraggio Normativo**
  Mantenendo un aggiornamento continuo sulle normative di sicurezza informatica applicabili e garantire la conformità.
- **Documentazione**
  Tenendo registri accurati delle politiche di sicurezza, delle procedure e delle formazioni svolte.

10. Revisione e Aggiornamento della Strategia

La strategia di Information Security sarà rivista e aggiornata annualmente o in seguito a cambiamenti significativi nell'Organizzazione, nel panorama delle minacce o in quello normativo Nazionale o Europeo.

11. Conclusione

La Società si impegna a garantire la sicurezza delle informazioni come parte integrante della propria operatività. L'implementazione di questa strategia di Information Security contribuirà a proteggere i dati sensibili e a mantenere la fiducia dei clienti e dei partner.

Alonte(VI), 27/04/2026

Il CEO Erardo Ratzenbeck