Politica per la Sicurezza delle Informazioni

ASI DataMyte Italia S.r.l.

Documento	Politica per la Sicurezza delle Informazioni
Codice	ASI-POL-SIC-01
Revisione	00
Data di emissione	1 luglio 2026
Approvazione	Adolfo Lorenzi, Amministratore Delegato
Classificazione	Documento pubblico
Stato	Approvato — in vigore

Indice

1. Premessa e finalità

Le informazioni — proprie, dei clienti e dei partner — costituiscono un patrimonio essenziale per ASI DataMyte Italia S.r.l. La Società sviluppa e integra soluzioni software e hardware per il controllo qualità e tratta, nell'ambito della propria attività, dati di qualità e di produzione che i clienti le affidano in settori a elevata criticità quali l'automotive e il ferroviario. La protezione di tali informazioni e dei sistemi che le gestiscono è pertanto condizione indispensabile per la continuità del servizio, per la fiducia dei clienti e per la competitività dell'impresa.

La presente Politica esprime l'impegno della Direzione verso la sicurezza delle informazioni e costituisce il riferimento di vertice per lo sviluppo di un Sistema di Gestione per la Sicurezza delle Informazioni (di seguito "SGSI") ispirato alla norma UNI CEI EN ISO/IEC 27001. La Società individua nella certificazione ISO/IEC 27001 e nell'attestazione TISAX — riferimento per la sicurezza delle informazioni nel settore automotive — gli obiettivi del proprio percorso di maturazione.

2. Ambito di applicazione e destinatari

La Politica si applica a tutte le informazioni trattate dalla Società, in qualsiasi forma (digitale, cartacea, verbale) e su qualunque supporto, nonché ai sistemi, alle reti, ai dispositivi e ai locali utilizzati per il loro trattamento.

Sono tenuti al rispetto della Politica soci, amministratori, dipendenti e collaboratori a qualsiasi titolo e, per quanto di rispettiva competenza, i fornitori e le terze parti che accedono alle informazioni o ai sistemi della Società.

3. Principi fondamentali

La sicurezza delle informazioni è perseguita salvaguardandone le tre proprietà fondamentali e i criteri di gestione che seguono:

- **Riservatezza —** le informazioni sono accessibili soltanto ai soggetti autorizzati.
- **Integrità —** l'esattezza e la completezza delle informazioni e dei relativi metodi di trattamento sono protette da alterazioni non autorizzate.
- **Disponibilità —** gli utenti autorizzati possono accedere alle informazioni e alle risorse quando ne hanno necessità.
- **Conformità —** il trattamento rispetta gli obblighi di legge, contrattuali e normativi applicabili.
- **Proporzionalità —** le misure di sicurezza sono commisurate ai rischi e al valore delle informazioni protette.
- **Responsabilità —** la sicurezza è responsabilità di tutti i destinatari, ciascuno secondo il proprio ruolo.

4. Obiettivi di sicurezza

Coerentemente con i principi enunciati, la Direzione persegue i seguenti obiettivi: proteggere le informazioni proprie e dei clienti da accessi non autorizzati, perdita, alterazione o divulgazione indebita; garantire la continuità dei sistemi e dei servizi essenziali; assicurare il rispetto degli obblighi normativi e contrattuali in materia di sicurezza e di protezione dei dati; accrescere la

consapevolezza e la competenza del personale; migliorare con continuità il livello complessivo di sicurezza. Tali obiettivi sono tradotti in traguardi misurabili, monitorati e sottoposti a riesame periodico.

5. Organizzazione e responsabilità

La Direzione definisce gli indirizzi in materia di sicurezza delle informazioni, approva la presente Politica e assegna le risorse necessarie alla sua attuazione. La Società individua un referente per la sicurezza delle informazioni, incaricato di coordinare le attività, gestire il processo di analisi del rischio e monitorare l'efficacia delle misure adottate.

Ogni destinatario è responsabile della corretta applicazione delle regole di sicurezza nell'ambito delle proprie attività ed è tenuto a segnalare tempestivamente eventi, anomalie o debolezze che possano comprometterne l'efficacia.

6. Approccio basato sul rischio

La gestione della sicurezza si fonda su un approccio basato sul rischio. La Società identifica e valuta periodicamente i rischi a cui sono esposte le informazioni e i sistemi e definisce, attua e mantiene misure di trattamento proporzionate. Il processo di analisi e trattamento del rischio è riesaminato a fronte di cambiamenti significativi del contesto, delle tecnologie o dello scenario delle minacce.

7. Aree di controllo

La Società sviluppa e mantiene misure di sicurezza nelle seguenti aree, che saranno dettagliate da procedure e istruzioni operative nell'ambito del SGSI:

7.1 Gestione degli asset informativi

Le informazioni e le risorse che le trattano sono identificate, inventariate e classificate in funzione del loro valore e della loro criticità, con regole di utilizzo accettabile.

7.2 Controllo degli accessi

Gli accessi sono concessi secondo i principi del "necessario sapere" e del privilegio minimo, mediante identità individuali e una gestione sicura delle credenziali, con adozione dell'autenticazione a più fattori ove applicabile e revoca tempestiva al venir meno dell'esigenza.

7.3 Sicurezza delle risorse umane

Sono previsti impegni di riservatezza, attività di formazione e una gestione controllata delle fasi di ingresso e di cessazione del rapporto, con restituzione dei beni assegnati e revoca degli accessi.

7.4 Sicurezza fisica e ambientale

Le sedi, i locali tecnici e i dispositivi sono protetti da accessi fisici non autorizzati e da rischi ambientali, con misure proporzionate alla criticità delle risorse ospitate.

7.5 Sicurezza operativa

Sono adottate misure di protezione dai software dannosi, di aggiornamento e gestione delle vulnerabilità, di esecuzione e verifica dei backup e di registrazione e monitoraggio degli eventi rilevanti per la sicurezza.

7.6 Sicurezza delle comunicazioni

Le reti sono protette e segmentate ove opportuno; le comunicazioni e i dati sensibili sono protetti, anche mediante cifratura, in transito e a riposo quando appropriato.

7.7 Sviluppo sicuro

I requisiti di sicurezza sono integrati nel ciclo di sviluppo del software, incluse le piattaforme proprietarie della Società, con separazione degli ambienti e gestione sicura del codice e delle configurazioni.

7.8 Protezione dei dati personali

I dati personali sono trattati nel rispetto del Regolamento (UE) 2016/679 (GDPR) e della normativa applicabile, in coerenza con le misure tecniche e organizzative di sicurezza adottate dalla Società.

7.9 Rapporti con i fornitori e le terze parti

I fornitori e le terze parti che trattano informazioni o erogano servizi rilevanti sono valutati sotto il profilo della sicurezza e vincolati da adeguate clausole contrattuali.

7.10 Gestione degli incidenti

Gli incidenti di sicurezza sono rilevati, segnalati, registrati e gestiti tempestivamente, con analisi delle cause e definizione di azioni correttive e di miglioramento.

7.11 Continuità operativa

Sono previste misure per assicurare il ripristino dei sistemi e dei servizi essenziali entro tempi accettabili a seguito di eventi che ne compromettano la disponibilità.

8. Conformità

La Società opera nel rispetto delle disposizioni di legge, regolamentari e contrattuali applicabili in materia di sicurezza delle informazioni e di protezione dei dati. ASI tiene altresì conto del proprio ruolo all'interno della catena di fornitura di organizzazioni destinatarie di obblighi specifici, anche in materia di cibersicurezza. Il rispetto di tali requisiti è verificato periodicamente.

9. Formazione e consapevolezza

ASI promuove la consapevolezza del personale in materia di sicurezza delle informazioni attraverso attività periodiche di informazione e formazione, affinché ciascuno sappia riconoscere le minacce, comprenda le proprie responsabilità e adotti comportamenti adeguati.

10. Violazioni e segnalazioni

Eventi, debolezze o violazioni della sicurezza delle informazioni devono essere segnalati tempestivamente attraverso i canali definiti dalla Società. È garantita la trattazione riservata delle segnalazioni effettuate in buona fede. La violazione delle regole di sicurezza comporta l'adozione di provvedimenti proporzionati alla gravità della condotta, secondo quanto previsto dal CCNL applicabile e dai rapporti contrattuali in essere.

11. Riesame e miglioramento continuo

La presente Politica e il Sistema di Gestione per la Sicurezza delle Informazioni sono sottoposti a riesame periodico della Direzione, e ogni volta che intervengano cambiamenti significativi, al fine di garantirne la continua idoneità, adeguatezza ed efficacia e di promuoverne il miglioramento continuo.

12. Disposizioni finali

La presente Politica entra in vigore dalla data della sua approvazione da parte della Direzione, è comunicata a tutti i destinatari ed è resa disponibile alle parti interessate. Essa è integrata da procedure e istruzioni operative di dettaglio sviluppate nell'ambito del Sistema di Gestione per la Sicurezza delle Informazioni.

Orbassano, 1 luglio 2026

La Direzione

Adolfo Lorenzi, Amministratore Delegato

ASI DataMyte Italia S.r.l.