



## POLITICA SGSI

### CONTROLLO DEL DOCUMENTO

CODICE ORGANIZZAZIONE DIREZIONE	CODICE DOCUMENTO POL-SGSI	LIVELLO DI REVISIONE 1.3
------------------------------------	------------------------------	-----------------------------

#### Stato delle revisioni

Revisione n.	Sezione n.	Pagina n.	Motivo della revisione	Data
1		1	Revisione obiettivi	24/04/2019
1.1		2	Revisione oggetto del campo di certificazione	03/06/2020
1.2	Revisione generale	All	Variazione del CdA aziendale e revisione generale	19/01/2022
1.3	Revisione generale	All	Verifica ed implementazione dei capitoli relativi alle norme di certificazione	10/01/2023

		IDONEITÀ	ADEGUATEZZA
PREPARATO DA: <i>omissis</i>	DATA 10/01/2023	FIRMA <i>omissis</i>	FIRMA <i>omissis</i>
RIESAMINATO DA: <i>omissis</i>	DATA 10/01/2023	FIRMA <i>omissis</i>	FIRMA <i>omissis</i>
APPROVATO DA: <i>omissis</i>	DATA 10/01/2023	FIRMA <i>omissis</i>	FIRMA <i>omissis</i>

#### Controllo delle copie

<b>Copia controllata</b>	<b>Copia non controllata</b>
Copia n.:	
Consegnata a:	
In data:	

*Nota: se la copia non è controllata deve recare, nell'apposito spazio, la dicitura "Copia non controllata / per informazione"*

Codice Organizzazione: Direzione	Data: 10/01/2023
Documento: Politica	Codice: POL- SGSI
Titolo: Politica SGSI	Pag.: 2/3

SAET S.p.A. ha deciso di conformare i propri processi per la sicurezza delle informazioni allo standard UNI CEI EN ISO/IEC 27001:2017 per quanto concerne la protezione delle informazioni inerenti le seguenti attività:

**Progettazione, realizzazione e manutenzione di sistemi di sicurezza e di videosorveglianza, di impianti elettrici, di impianti antincendio, di telecomunicazione, trasmissione dati, automazione industriale, centri di supervisione e servizi connessi.**

Le finalità del SGSI sono:

- Assicurare la riservatezza, l'integrità e la disponibilità delle informazioni alle parti interessate;
- Minimizzare l'impatto in caso di incidenti relativi alla sicurezza delle informazioni;
- Garantire la continuità dei servizi secondo quanto definito dalle normative vigenti e dai requisiti contrattuali;
- Migliorare in modo continuo la sicurezza delle informazioni contemperando l'evolversi continuo degli aspetti tecnologici

SAET si impegna ad un costante miglioramento del SGSI, tenendo conto che:

- L'esigenza nasce dalla necessità di rispondere alle molteplici richieste provenienti dall'esterno e dall'interno dell'organizzazione, inclusa la necessità di rispondere a quanto definito dal GDPR in materia di protezione dei dati personali di clienti, dipendenti e fornitori.
- L'organizzazione ha individuato le figure di risk owner (di seguito RO) e le interfacce per le tematiche di sicurezza delle informazioni verso le terze parti. Il RO riporterà sugli andamenti e sullo stato della sicurezza delle informazioni con cadenza periodica.
- L'organizzazione ha incaricato il reparto ICT aziendale con il supporto dei consulenti esterni degli aspetti tecnologici per la sicurezza delle informazioni ed il supporto alla definizione del SGSI. Il reparto IT svolge anche il ruolo di gestore delle anomalie tecniche e degli incidenti di sicurezza delle informazioni.
- SAET S.p.A. ha definito gli obiettivi per la sicurezza delle informazioni che vengono aggiornati in occasione del Riesame della Direzione o quando ritenuto necessario dalla Direzione di SAET S.p.A. Il RO è responsabile del loro monitoraggio e della rilevazione di eventuali anomalie rispetto a quanto predisposto.
- SAET S.p.A. predispone, con programma dedicato, audit interni per mezzo dei quali assicura il controllo del proprio SGSI ed effettua specifici interventi formativi come indicato nel programma di formazione dedicato.
- SAET S.p.A. si impegna al rispetto delle leggi e direttive in materia di protezione dei dati e di sicurezza delle informazioni nonché delle prescrizioni legislative applicabili ai propri servizi (ad es. L. 48/2008, diritto di proprietà intellettuale, responsabilità amministrativa ecc.).
- L'azienda si prefigge il miglioramento continuo del Sistema di Gestione per la Sicurezza delle Informazioni utilizzando il presente documento (completo degli obiettivi), le verifiche ispettive, la raccolta e l'analisi dei dati, le azioni correttive e preventive, i riesami della Direzione e tutto ciò ritenuto opportuno.

## Responsabilità:



<b>Codice Organizzazione: Direzione</b>	<b>Data: 10/01/2023</b>
<b>Documento: Politica</b>	<b>Codice: POL- SGSI</b>
<b>Titolo: Politica SGSI</b>	<b>Pag.: 3/3</b>

- Il RO è responsabile di assicurare che il SGSI sia implementato e mantenuto in conformità con questa Politica e per garantire che tutte le risorse necessarie siano disponibili
- Il RO è responsabile del coordinamento operativo del SGSI e della segnalazione delle prestazioni del SGSI
- La Direzione deve rivedere il SGSI almeno una volta all'anno o ogni volta che si verifica un cambiamento significativo e preparare verbali di quella riunione. Lo scopo del riesame della direzione è stabilire l'adeguatezza e l'efficacia del SGSI
- Il RO implementerà programmi di formazione sulla sicurezza delle informazioni e di sensibilizzazione per i dipendenti
- La protezione dell'integrità, della disponibilità e della riservatezza nelle attività è responsabilità del proprietario/assegnatario di ciascun bene
- Tutti gli incidenti o i punti deboli di sicurezza devono essere segnalati al RO
- Il RO definirà quali informazioni relative alla sicurezza delle informazioni saranno comunicate a quale parte interessata (sia interna che esterna), da chi e quando
- Il RO è responsabile dell'adozione e dell'attuazione del piano di addestramento e sensibilizzazione, che si applica a tutte le persone che hanno un ruolo nella gestione della sicurezza delle informazioni

La politica del SGSI è comunicata all'interno di SAET S.p.A. per mezzo di apposite sessioni formative e/o comunicazioni da parte del RO.

La politica può essere comunicata all'esterno (clienti, fornitori, autorità ecc.) solo dopo parere positivo da parte del RO e del Titolare del trattamento.

La presente Politica verrà rivista ed aggiornata dalla direzione di SAET ogniqualvolta vi si verificano avvenimenti e cambiamenti sostanziali degli asset aziendali e verrà analizzata ad ogni Riesame della Direzione.

