

CAMELOT BIOMEDICAL SYSTEMS SRL

Information Security Management System Policy

1	10/06/2026	Prima versione	FUMAGALLI	SANTORO
REV	DATA	DESCRIZIONE	AUTORE	APPROVATORE
		Information Security Management System Policy	Pagina 1 di 6	

Sommario

1.	SCOPO E CAMPO DI APPLICAZIONE	3
2.	ACRONIMI E DEFINIZIONI.....	3
3.	IMPEGNO E OBIETTIVI DEL SGSI.....	4
3.1	PRINCIPI FONDAMENTALI DEL SGSI.....	4
3.2	QUADRO DI RIFERIMENTO PER GLI OBIETTIVI	5
3.3	COMUNICAZIONE E DISPONIBILITÀ	5
4.	ARCHIVIAZIONE E AGGIORNAMENTI	5

1. SCOPO E CAMPO DI APPLICAZIONE

Questo documento definisce la politica per la sicurezza delle informazioni di CAMELOT Biomedical Systems S.r.l. e stabilisce i principi guida e l'impegno della Direzione per la gestione della sicurezza delle informazioni.

La politica si applica a tutti i processi, le risorse informative, il personale e i/le collaboratori/collaboratrici coinvolti/e nell'ambito di applicazione del Sistema di Gestione della Sicurezza delle Informazioni (SGSI), definito come *"Fornitura di servizi e prodotti in ambito IT"*.

I ruoli e le responsabilità relative al SGSI sono definiti nel record **QFR-ComPla - Competences Plan**. Il/La Responsabile del Sistema di Gestione della Sicurezza delle Informazioni (RSGSI) assicura il riesame e l'aggiornamento di tali attribuzioni con frequenza almeno annuale o con maggiore frequenza qualora ritenuto necessario a seguito di modifiche organizzative, operative o normative che possano influire sul SGSI.

2. ACRONIMI E DEFINIZIONI

CEO	Chief Executive Officer
Disponibilità	Proprietà di essere accessibili e utilizzabili su richiesta da una entità autorizzata [27000 – definizione 3.4]
GDPR	Regolamento Generale sulla Protezione dei Dati
HRM	Human Resources Manager
Integrità	Proprietà di accuratezza e completezza [27000 – definizione 3.3]
IT	Information Technology (tecnologia dell'Informazione)
QM	Quality Manager
Riservatezza	Proprietà in virtù della quale le informazioni non sono rese disponibili né divulgate a individui, entità o processi non autorizzati [27000 – definizione 3.2]
RSGSI	Responsabile del Sistema di Gestione della Sicurezza delle Informazioni
SGSI	Sistema di Gestione della Sicurezza delle Informazioni. Sistema di gestione per la preservazione della sicurezza delle informazioni, che può essere costituito da politiche, processi, persone, entità fisiche e tecnologie, nonché dalle risorse ad essi associate [27000 – requisito 4.1.6]
Sicurezza delle informazioni	Preservazione della riservatezza (3.2), dell'integrità (3.3) e della disponibilità (3.4) delle informazioni [27000 – definizione 3.1]

3. IMPEGNO E OBIETTIVI DEL SGSI

La Direzione di CAMELOT, consapevole del valore strategico delle informazioni per il proprio business, incentrato sulla fornitura di servizi e prodotti IT ad alto contenuto tecnologico destinati alla Pubblica Amministrazione e a privati, stabilisce la presente politica per la sicurezza delle informazioni.

Questa politica definisce i principi e gli impegni per la protezione degli asset informativi aziendali e di quelli affidati dalla clientela, istituendo un SGSI conforme ai requisiti della norma ISO/IEC 27001.

Il/La CEO approva e sostiene attivamente la presente politica, assicurando che gli obiettivi di sicurezza siano integrati nei processi di business e allineati alle direzioni strategiche dell'organizzazione.

3.1 PRINCIPI FONDAMENTALI DEL SGSI

L'SGSI di CAMELOT si fonda sui seguenti principi:

- **Riservatezza, Integrità e Disponibilità:** l'organizzazione si impegna a proteggere le informazioni da accessi, modifiche o divulgazioni non autorizzate (**Riservatezza**), a salvaguardarne l'accuratezza e la completezza (**Integrità**) e a garantirne l'accesso e l'utilizzo quando richiesto (**Disponibilità**).
- **Approccio Basato sul Rischio:** le decisioni relative alla sicurezza e l'implementazione dei controlli devono basarsi su un processo strutturato di valutazione e trattamento del rischio, come definito nella **QSP_IS_RM - Risk Management**. Questo assicura che le misure di protezione siano proporzionate alle minacce identificate e allineate alla propensione al rischio definita dalla Direzione.
- **Responsabilità Condivisa:** la sicurezza delle informazioni costituisce una responsabilità condivisa da tutto il personale e da tutti i collaboratori e le collaboratrici dell'organizzazione. La consapevolezza di tale responsabilità è promossa attraverso attività continuative di sensibilizzazione, formazione e accrescimento della consapevolezza sui temi della sicurezza delle informazioni. Il rispetto dei *"Principi Etici"*, contenuti nel Regolamento Aziendale e parte integrante dello stesso, rappresenta un elemento fondamentale per garantire comportamenti coerenti con gli obiettivi di tutela della riservatezza, dell'integrità e della disponibilità delle informazioni. Le responsabilità specifiche sono formalizzate nel record **QFR-ComPla - Competences Plan**.
- **Conformità ai Requisiti:** l'organizzazione si impegna a soddisfare tutti i requisiti legali, normativi e contrattuali applicabili in materia di sicurezza delle informazioni. Ciò include, a titolo esemplificativo, il GDPR e gli obblighi specifici derivanti dai contratti con la clientela, in particolare con la Pubblica Amministrazione e le aziende del settore medicale.
- **Miglioramento Continuo:** la Direzione si impegna al miglioramento continuo dell'idoneità, adeguatezza ed efficacia del SGSI. Tale impegno si realizza attraverso il monitoraggio delle prestazioni, l'esecuzione di audit periodici e il riesame sistematico del sistema, come disciplinato dalla **QSP-ManRev - Management Review**.

3.2 QUADRO DI RIFERIMENTO PER GLI OBIETTIVI

La Direzione definisce e riesamina periodicamente gli obiettivi per la sicurezza delle informazioni, assicurando che siano:

- Coerenti con la presente politica e con le direzioni strategiche definite nel documento **Analisi del contesto**.
- Misurabili, per consentire una valutazione oggettiva delle prestazioni del SGSI.
- Allineati ai risultati della valutazione dei rischi e ai requisiti applicabili.
- Supportati da risorse adeguate e assegnati a funzioni specifiche per il loro raggiungimento.

Il processo per la definizione, il monitoraggio e il raggiungimento degli obiettivi è descritto nella **QSP_IS_MM - Monitoring and Measurement**.

3.3 COMUNICAZIONE E DISPONIBILITÀ

La presente politica è mantenuta come informazione documentata e comunicata a tutto il personale e ai collaboratori e alle collaboratrici per garantirne la comprensione e l'applicazione.

Il/La CEO, con il supporto del/della RSGSI e del/della QM, ne assicura la diffusione.

La politica è, inoltre, resa disponibile alle parti interessate rilevanti, quali clientela, fornitori e autorità, ove appropriato, per dimostrare l'impegno di CAMELOT nella protezione delle informazioni.

4. ARCHIVIAZIONE E AGGIORNAMENTI

La presente Politica è conservata nel sistema documentale del SGSI ed è resa disponibile a tutto il personale interessato attraverso i canali di comunicazione interni dell'organizzazione.

Il riesame della presente Policy è effettuato con cadenza almeno annuale o in occasione di modifiche significative all'infrastruttura tecnologica, ai processi operativi, al contesto normativo o a seguito di incidenti rilevanti.

Le versioni superate sono archiviate in conformità alla **QSP-DocCon - Documents Control**. Ogni aggiornamento è approvato dal/dalla QM prima della relativa distribuzione.

10/06/2026, Matteo Santoro (CEO)

	CAMELOT BIOMEDICAL SYSTEMS S.R.L.
	Sede Legale: Via Al Ponte Reale n. 2/20, 16124, Genova (GE)
	Codice Fiscale / Partita IVA: 01859390997 Capitale Sociale: 500.000,00 € i.v.
	Iscritta al Registro delle Imprese di Genova - REA: GE - 441013
	PEC: camelotbio@legalmail.it E-mail: info@camelotbio.com Web: https://www.camelotbio.com/