

# CAMELOT BIOMEDICAL SYSTEMS SRL

## Information Security Policy

|                                                                                     |            |                             |               |             |
|-------------------------------------------------------------------------------------|------------|-----------------------------|---------------|-------------|
|                                                                                     |            |                             |               |             |
|                                                                                     |            |                             |               |             |
|                                                                                     |            |                             |               |             |
|                                                                                     |            |                             |               |             |
| 1                                                                                   | 10/06/2026 | Prima versione              | FUMAGALLI     | SANTORO     |
| REV                                                                                 | DATA       | DESCRIZIONE                 | AUTORE        | APPROVATORE |
|  |            | Information Security Policy | Pagina 1 di 8 |             |

## Sommario

|     |                                                             |   |
|-----|-------------------------------------------------------------|---|
| 1.  | SCOPO E CAMPO DI APPLICAZIONE .....                         | 3 |
| 2.  | ACRONIMI E DEFINIZIONI.....                                 | 3 |
| 3.  | OBIETTIVI DI SICUREZZA DELLE INFORMAZIONI.....              | 4 |
| 4.  | PRINCIPI FONDAMENTALI DI SICUREZZA DELLE INFORMAZIONI ..... | 5 |
| 4.1 | APPROCCIO BASATO SUL RISCHIO .....                          | 5 |
| 4.2 | USO ACCETTABILE DELLE RISORSE.....                          | 5 |
| 4.3 | SICUREZZA NEL CLOUD COMPUTING .....                         | 5 |
| 4.4 | PROTEZIONE DELLE PII.....                                   | 6 |
| 4.5 | SICUREZZA NEL CICLO DI VITA DEI SISTEMI E DEI SERVIZI ..... | 6 |
| 4.6 | PROTEZIONE DEGLI ASSET .....                                | 6 |
| 4.7 | REVISIONE E MIGLIORAMENTO CONTINUO .....                    | 6 |
| 5.  | ARCHIVIAZIONE E AGGIORNAMENTI .....                         | 7 |

## 1. SCOPO E CAMPO DI APPLICAZIONE

La presente politica definisce i principi e gli obiettivi strategici per la gestione della sicurezza delle informazioni all'interno di CAMELOT Biomedical Systems S.r.l. Il suo scopo è proteggere gli asset informativi dell'azienda, della clientela e dei partner commerciali, garantendo la continuità operativa, la conformità normativa e la tutela della reputazione aziendale.

La presente politica si applica a tutto il personale, ai/alle collaboratori/collaboratrici, ai processi e alle tecnologie che gestiscono informazioni di proprietà dell'azienda o affidate da terzi, in tutte le sedi operative e in modalità di lavoro da remoto.

## 2. ACRONIMI E DEFINIZIONI

|                          |                                                                                                                                                                                                                                                                                                          |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CEO                      | Chief Executive Officer                                                                                                                                                                                                                                                                                  |
| Cliente di servizi cloud | Parte (3.3.1) che agisce nel ruolo di cliente del servizio cloud (3.3.14) <b>[22123 – definizione 3.3.2]</b>                                                                                                                                                                                             |
| Disponibilità            | Proprietà di essere accessibili e utilizzabili su richiesta da una entità autorizzata <b>[27000 – definizione 3.4]</b>                                                                                                                                                                                   |
| DPO                      | Data Protection Officer                                                                                                                                                                                                                                                                                  |
| GDPR                     | Regolamento Generale sulla Protezione dei Dati                                                                                                                                                                                                                                                           |
| HW                       | Hardware                                                                                                                                                                                                                                                                                                 |
| IaaS                     | Infrastructure as a Service                                                                                                                                                                                                                                                                              |
| PII                      | <b>Personally Identifiable Information.</b> Qualsiasi informazione che (a) possa essere utilizzata per identificare la persona fisica alla quale tali informazioni si riferiscono, o (b) sia o possa essere direttamente o indirettamente collegata a un interessato <b>[27002 – definizione 3.1.21]</b> |
| Integrità                | Proprietà di accuratezza e completezza <b>[27000 – definizione 3.3]</b>                                                                                                                                                                                                                                  |
| IT                       | Information Technology (tecnologia dell'informazione)                                                                                                                                                                                                                                                    |
| PaaS                     | Platform as a Service                                                                                                                                                                                                                                                                                    |
| PriM                     | Privacy Manager                                                                                                                                                                                                                                                                                          |
| QM                       | Quality Manager                                                                                                                                                                                                                                                                                          |
| Riservatezza             | Proprietà in virtù della quale le informazioni non sono rese disponibili né divulgate a individui, entità o processi non autorizzati <b>[27000 – definizione 3.2]</b>                                                                                                                                    |

|       |                                                                                                                                                                                                                                                                                                         |
|-------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RSGSI | Responsabile del Sistema di Gestione della Sicurezza delle Informazioni                                                                                                                                                                                                                                 |
| SaaS  | Software as a Service                                                                                                                                                                                                                                                                                   |
| SGSI  | <b>Sistema di Gestione della Sicurezza delle Informazioni.</b><br>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] |
| SW    | Software                                                                                                                                                                                                                                                                                                |

### 3. OBIETTIVI DI SICUREZZA DELLE INFORMAZIONI

CAMELOT si impegna a proteggere i propri asset informativi, e quelli della propria clientela e dei propri partner commerciali, per garantire la continuità operativa, la conformità normativa e la tutela della reputazione aziendale.

La Direzione formalizza tale impegno attraverso la definizione, l'implementazione e il mantenimento di un SGSI conforme allo standard ISO/IEC 27001.

Gli obiettivi strategici di sicurezza delle informazioni sono:

- **Riservatezza:** proteggere le informazioni da accessi non autorizzati, con particolare attenzione ai dati personali, ai dati sanitari, alla proprietà intellettuale e ai segreti commerciali trattati nell'ambito dei progetti per il settore medicale e la pubblica amministrazione.
- **Integrità:** assicurare l'accuratezza e la completezza delle informazioni e dei metodi di elaborazione, garantendo che i dati e il SW sviluppato, incluse le soluzioni basate su intelligenza artificiale e blockchain, non subiscano modifiche non autorizzate.
- **Disponibilità:** garantire che le informazioni e le risorse associate siano accessibili agli utenti autorizzati quando necessario, per sostenere i processi di business critici e l'erogazione dei servizi alla clientela.

Per raggiungere tali obiettivi, l'organizzazione si impegna a:

- Soddisfare tutti i requisiti legali, statutari, regolamentari e contrattuali applicabili, inclusi quelli derivanti dal GDPR e dalle norme ISO 9001 e ISO 13485.
- Promuovere una cultura della sicurezza a tutti i livelli aziendali, dove ogni membro del personale è consapevole delle proprie responsabilità.
- Attuare un processo di miglioramento continuo del SGSI, attraverso il monitoraggio delle prestazioni, la gestione degli incidenti e il riesame periodico da parte della Direzione.

Il/La CEO ha la responsabilità ultima del SGSI e, insieme alla Direzione, assicura che le risorse necessarie per il raggiungimento di questi obiettivi siano disponibili.

## 4. PRINCIPI FONDAMENTALI DI SICUREZZA DELLE INFORMAZIONI

### 4.1 APPROCCIO BASATO SUL RISCHIO

Tutte le decisioni in materia di sicurezza delle informazioni devono essere guidate da un processo strutturato di valutazione e trattamento del rischio.

Il/La RSGSI ha la responsabilità di supervisionare l'identificazione, l'analisi e la valutazione dei rischi per gli asset informativi, assicurando che le misure di controllo implementate siano proporzionate alle minacce identificate.

La sicurezza delle informazioni è una responsabilità condivisa che coinvolge tutto il personale. Le responsabilità specifiche sono formalmente definite e assegnate per garantire una governance chiara ed efficace:

- La Direzione fornisce leadership e supporto al SGSI approvandone la politica e garantendone l'efficacia, mentre il/La RSGSI ne assicura la progettazione, l'implementazione, la gestione e il monitoraggio.
- Il/La PriM, in collaborazione con il/La DPO, è responsabile di garantire che il trattamento dei dati personali sia conforme alla normativa applicabile e ai requisiti contrattuali.
- Tutto il personale e i/le collaboratori/collaboratrici sono tenuti a rispettare la presente politica e tutti i documenti ad essa collegati.

### 4.2 USO ACCETTABILE DELLE RISORSE

L'accesso e l'uso di tutte le risorse informative e tecnologiche di CAMELOT, inclusi HW, SW, reti e dati, devono avvenire in modo responsabile, etico e sicuro. Le regole per l'uso accettabile devono essere comprese e accettate da tutto il personale.

### 4.3 SICUREZZA NEL CLOUD COMPUTING

L'organizzazione adotta un approccio strutturato per la gestione della sicurezza negli ambienti cloud, sia come cliente che come fornitore di servizi.

- **Come cliente di servizi cloud:** l'utilizzo di servizi esterni (es. IaaS, PaaS, SaaS) deve essere valutato e gestito per garantire che i fornitori offrano livelli di sicurezza adeguati. Il modello di responsabilità condivisa deve essere chiaramente compreso e i dati devono essere protetti in base alla loro classificazione.
- **Come fornitore di servizi cloud:** nello sviluppo e nell'erogazione di piattaforme e applicazioni cloud per la clientela, l'organizzazione deve implementare la sicurezza by design, garantendo l'isolamento degli ambienti multi-tenant, la protezione dei dati dei clienti e la gestione sicura degli accessi amministrativi.

#### 4.4 PROTEZIONE DELLE PII

CAMELOT si impegna a proteggere le PII in conformità con il GDPR e altre normative applicabili, come la ISO/IEC 27018. Il trattamento delle PII, specialmente in ambienti di cloud pubblico, deve avvenire nel rispetto dei principi di minimizzazione dei dati, limitazione della finalità e trasparenza. Gli accordi contrattuali con la clientela devono definire chiaramente i ruoli e le responsabilità per la protezione delle PII.

#### 4.5 SICUREZZA NEL CICLO DI VITA DEI SISTEMI E DEI SERVIZI

- **Sviluppo sicuro:** la sicurezza deve essere integrata in ogni fase del ciclo di vita dello sviluppo del SW, dalla progettazione al rilascio.
- **Gestione degli incidenti:** tutto il personale ha l'obbligo di segnalare tempestivamente qualsiasi evento o debolezza di sicurezza osservata o sospetta attraverso i canali appositi.
- **Continuità operativa:** l'organizzazione deve mantenere piani di continuità operativa e di ripristino d'emergenza per garantire la disponibilità dei processi critici a fronte di interruzioni.

#### 4.6 PROTEZIONE DEGLI ASSET

- **Classificazione delle informazioni:** tutte le informazioni devono essere classificate in base alla loro sensibilità e criticità per applicare un livello di protezione adeguato durante il loro intero ciclo di vita.
- **Sicurezza delle postazioni di lavoro:** devono essere applicate regole di "scrivania pulita e schermo pulito" per ridurre il rischio di accesso non autorizzato, perdita o danneggiamento delle informazioni. Ciò include il blocco automatico delle sessioni di lavoro dopo un breve periodo di inattività e la custodia di documenti cartacei sensibili.
- **Lavoro da remoto e asset fuori sede:** gli asset aziendali utilizzati al di fuori delle sedi fisiche, inclusi i dispositivi impiegati in modalità di lavoro agile, devono essere protetti con misure di sicurezza equivalenti a quelle applicate internamente. Il personale è tenuto a utilizzare connessioni di rete sicure e a proteggere fisicamente i dispositivi affidati.

#### 4.7 REVISIONE E MIGLIORAMENTO CONTINUO

La presente politica e l'intero SGSI devono essere riesaminati a intervalli pianificati e, comunque, almeno una volta all'anno, o a seguito di cambiamenti significativi nel contesto aziendale, tecnologico o normativo. Il/La RSGSI è responsabile di coordinare il processo di revisione, i cui esiti sono presentati alla Direzione durante il riesame periodico. La presente politica è approvata dal/dalla CEO e comunicata a tutto il personale e alle parti interessate rilevanti.

## 5. 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: <a href="mailto:camelotbio@legalmail.it">camelotbio@legalmail.it</a>   E-mail: <a href="mailto:info@camelotbio.com">info@camelotbio.com</a>  <br>Web: <a href="https://www.camelotbio.com/">https://www.camelotbio.com/</a> |