

# CAMELOT BIOMEDICAL SYSTEMS SRL

## Classification & Labeling of Information Policy

|                                                                                     |            |                                                 |                |             |
|-------------------------------------------------------------------------------------|------------|-------------------------------------------------|----------------|-------------|
|                                                                                     |            |                                                 |                |             |
|                                                                                     |            |                                                 |                |             |
|                                                                                     |            |                                                 |                |             |
|                                                                                     |            |                                                 |                |             |
| 1                                                                                   | 10/06/2026 | Prima versione                                  | FUMAGALLI      | SANTORO     |
| REV                                                                                 | DATA       | DESCRIZIONE                                     | AUTORE         | APPROVATORE |
|  |            | Classification & Labeling of Information Policy | Pagina 1 di 10 |             |

## Sommario

|     |                                                             |   |
|-----|-------------------------------------------------------------|---|
| 1.  | SCOPO E CAMPO DI APPLICAZIONE .....                         | 3 |
| 2.  | ACRONIMI E DEFINIZIONI.....                                 | 3 |
| 3.  | CLASSIFICAZIONE DELLE INFORMAZIONI .....                    | 4 |
| 3.1 | RISERVATO.....                                              | 5 |
| 3.2 | LIMITATO .....                                              | 5 |
| 3.3 | PUBBLICO .....                                              | 5 |
| 4.  | ETICHETTATURA DELLE INFORMAZIONI.....                       | 6 |
| 4.1 | DOCUMENTI ELETTRONICI .....                                 | 6 |
| 4.2 | COMUNICAZIONI E-MAIL.....                                   | 6 |
| 4.3 | SUPPORTI FISICI .....                                       | 6 |
| 4.4 | AMBIENTI CLOUD .....                                        | 6 |
| 5.  | GESTIONE DELLE INFORMAZIONI.....                            | 7 |
| 5.1 | TRATTAMENTO DELLE INFORMAZIONI.....                         | 7 |
| 5.2 | PROTEZIONE DEI DATI DI TEST.....                            | 7 |
| 5.3 | SUPPORTI DI MEMORIZZAZIONE E DISPOSITIVI PORTATILI .....    | 7 |
| 5.4 | SMALTIMENTO SICURO E RIUTILIZZO DELLE APPARECCHIATURE ..... | 8 |
| 5.5 | PROTEZIONE DEI DOCUMENTI E DELLE REGISTRAZIONI.....         | 8 |
| 5.6 | APPARECCHIATURA INCUSTODITA .....                           | 8 |
| 6.  | TRASFERIMENTO DELLE INFORMAZIONI.....                       | 8 |
| 7.  | ARCHIVIAZIONE E AGGIORNAMENTI .....                         | 9 |

## 1. SCOPO E CAMPO DI APPLICAZIONE

La presente politica istituisce il framework aziendale di CAMELOT Biomedical Systems S.r.l. per la classificazione e l'etichettatura delle informazioni e degli asset informativi. L'organizzazione riconosce che la protezione efficace delle informazioni richiede un sistema strutturato che permetta di identificare il valore, la sensibilità e la criticità di ogni dato gestito, così da garantire un livello di protezione adeguato e proporzionato al rischio associato.

Attraverso questa politica, l'organizzazione persegue i seguenti obiettivi:

- Definire un sistema di classificazione basato su livelli di riservatezza coerente con i requisiti legali, contrattuali e di sicurezza applicabili.
- Stabilire criteri uniformi di etichettatura che rendano immediatamente riconoscibile il livello di protezione richiesto per ogni informazione.
- Associare a ciascun livello di classificazione specifici requisiti di protezione per il trattamento, la trasmissione e la conservazione dei dati, sia in ambienti on-premise sia in ambienti di cloud computing.
- Promuovere una cultura della responsabilità condivisa in cui tutto il personale contribuisce attivamente alla protezione delle informazioni aziendali e dei clienti.

La presente politica si applica a tutte le informazioni e ai sistemi informativi gestiti da CAMELOT presso le proprie sedi di Genova, Milano e Pescara, nonché negli ambienti cloud utilizzati per l'erogazione dei servizi. Il perimetro comprende dati in formato digitale e cartaceo, indipendentemente dal supporto di memorizzazione. La politica vincola tutto il personale dipendente, i/le collaboratori/collaboratrici e le terze parti autorizzate ad accedere alle informazioni aziendali o a trattarle per conto dell'organizzazione.

## 2. ACRONIMI E DEFINIZIONI

|                                    |                                                                                                                                                                                                               |
|------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CEO                                | Chief Executive Officer                                                                                                                                                                                       |
| Classificazione delle informazioni | Processo di valutazione delle informazioni in base alla loro sensibilità, criticità e ai requisiti legali applicabili, al fine di assegnarle a una delle categorie di protezione definite dall'organizzazione |
| Disponibilità                      | Proprietà di essere accessibili e utilizzabili su richiesta da una entità autorizzata [27000 – definizione 3.4]                                                                                               |
| DLP                                | Data Loss Prevention                                                                                                                                                                                          |
| DPIA                               | Data Protection Impact Assessment (Valutazione d'Impatto sulla Protezione dei Dati)                                                                                                                           |

|                                         |                                                                                                                                                                                                                                                                                                                |
|-----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Etichettatura delle informazioni</b> | Atto di apporre un'indicazione fisica o digitale a un'informazione o al suo contenitore per renderne visibile il livello di classificazione e facilitarne il corretto trattamento                                                                                                                              |
| <b>HW</b>                               | Hardware                                                                                                                                                                                                                                                                                                       |
| <b>Integrità</b>                        | Proprietà di accuratezza e completezza [27000 – definizione 3.3]                                                                                                                                                                                                                                               |
| <b>NC</b>                               | Non conformità                                                                                                                                                                                                                                                                                                 |
| <b>PII</b>                              | <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 [27002 – definizione 3.1.21]              |
| <b>Proprietario delle informazioni</b>  | Persona o funzione aziendale che detiene la responsabilità primaria per un determinato insieme di informazioni, inclusa la definizione del livello di classificazione e l'autorizzazione all'accesso.                                                                                                          |
| <b>QM</b>                               | Quality Manager                                                                                                                                                                                                                                                                                                |
| <b>Riservatezza</b>                     | Proprietà in virtù della quale le informazioni non sono rese disponibili né divulgate a individui, entità o processi non autorizzati [27000 – definizione 3.2]                                                                                                                                                 |
| <b>Risorsa (asset)</b>                  | Qualsiasi cosa che ha valore per l'organizzazione [27002 – definizione 3.1.2]                                                                                                                                                                                                                                  |
| <b>RSGSI</b>                            | Responsabile del Sistema di Gestione per la Sicurezza delle informazioni. Supervisiona l'implementazione e il rispetto della presente politica, ne cura il riesame periodico e gestisce le richieste di eccezione o le segnalazioni di NC relative alla classificazione e all'etichettatura delle informazioni |
| <b>SGSI</b>                             | <b>Sistema di Gestione della Sicurezza delle Informazioni.</b> 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]           |
| <b>SW</b>                               | Software                                                                                                                                                                                                                                                                                                       |

### 3. CLASSIFICAZIONE DELLE INFORMAZIONI

CAMELOT adotta un sistema di classificazione articolato su tre livelli, fondato sulla sensibilità, sulla criticità per il business e sui requisiti di protezione imposti dalla normativa applicabile:

1. Riservato
2. Limitato
3. Pubblico

Ogni sistema informatico è classificato in base al livello più elevato delle informazioni che memorizza o elabora, così da garantire la coerenza delle misure di protezione lungo l'intera catena di trattamento.

Il medesimo principio si applica alle risorse ospitate in ambienti cloud, dove la classificazione orienta le scelte di crittografia, controllo degli accessi e localizzazione dei dati.

### 3.1 RISERVATO

Rientrano in questo livello le informazioni la cui divulgazione non autorizzata comporterebbe un danno grave per CAMELOT, per la propria clientela o per le persone fisiche interessate. L'accesso è strettamente limitato al personale specificamente autorizzato.

Esempi di informazioni classificate come *“riservato”*:

- PII, dati retributivi e dati idonei a rivelare lo stato di salute
- Codice sorgente delle applicazioni sviluppate dall'organizzazione
- Chiavi crittografiche e credenziali di autenticazione
- Dati dei clienti trattati in ambienti cloud nell'ambito dei servizi erogati
- Documentazione relativa a DPIA

### 3.2 LIMITATO

Comprende le informazioni proprietarie di CAMELOT che, pur non raggiungendo la criticità del livello *“riservato”*, richiedono protezione per preservare gli interessi aziendali. L'accesso è concesso esclusivamente al personale che ne ha una comprovata necessità operativa.

Questa è la classificazione predefinita per tutte le informazioni aziendali non diversamente classificate.

Esempi di informazioni classificate come *“limitato”*:

- Procedure interne e istruzioni operative dei Sistemi di Gestione della Qualità aziendali
- Contratti con clienti e fornitori
- Report interni, verbali di riunione e comunicazioni e-mail a contenuto operativo
- Registri del SGSI e registrazioni di audit

### 3.3 PUBBLICO

Include le informazioni destinate alla diffusione esterna e che possono essere distribuite liberamente senza comportare rischi per CAMELOT.

Esempi di informazioni classificate come *“pubblico”*:

- Materiale di marketing e descrizioni di prodotti e servizi

- Politiche dei Sistemi di Gestione della Qualità aziendali comunicate agli stakeholder esterni e presenti sul sito web
- Informazioni istituzionali già di dominio pubblico

## 4. ETICHETTATURA DELLE INFORMAZIONI

CAMELOT riconosce nell'etichettatura il meccanismo essenziale attraverso cui la classificazione diventa visibile a chiunque tratti l'informazione, garantendo che le misure di protezione previste vengano applicate in modo coerente. Tutte le informazioni classificate come “riservato” o “limitato” devono essere etichettate; le informazioni “pubbliche” non richiedono etichettatura obbligatoria.

**NOTA IMPORTANTE:** Considerando la grande quantità di documenti presenti in azienda e che l'implementazione del SGSI è un processo nuovo in divenire (prima certificazione in accordo alla ISO 27001), è stata accettata l'assunzione che al momento tutta la documentazione CAMELOT presenta un livello “riservato” o “limitato” e nulla è pubblico, ad eccezione di quanto presente sul sito web aziendale. Man mano che i documenti vengono emessi, modificati, creati, si inizierà ad etichettare ogni documento, dandoci un anno di tempo (fino a settembre 2027) per arrivare al completamento dell'etichettatura.

### 4.1 DOCUMENTI ELETTRONICI

CAMELOT prescrive che ogni documento elettronico classificato come “riservato” o “limitato” riporti l'etichetta di classificazione nell'intestazione, nel piè di pagina o come filigrana. L'etichetta deve indicare in modo inequivocabile il livello assegnato (es.: “RISERVATO” o “LIMITATO”).

### 4.2 COMUNICAZIONI E-MAIL

Le e-mail contenenti informazioni classificate come “riservato” devono includere l'indicazione del livello di classificazione nell'oggetto del messaggio. CAMELOT promuove l'adozione del medesimo approccio anche per le informazioni di livello “limitato” qualora il contenuto presenti particolare sensibilità.

### 4.3 SUPPORTI FISICI

I documenti cartacei (qualora strettamente necessari in quanto fortemente sconsigliati dal sistema di gestione della qualità aziendale) classificati come “riservato” o “limitato” devono essere fisicamente contrassegnati con l'etichetta corrispondente. Qualora l'utilizzo di supporti di memorizzazione rimovibili sia eccezionalmente autorizzato, tali supporti devono riportare un'etichetta fisica ben visibile che indichi il livello di classificazione del contenuto.

### 4.4 AMBIENTI CLOUD

Quando le informazioni sono mantenute in ambienti cloud, CAMELOT si impegna ad adottare le funzionalità di classificazione e tagging messe a disposizione dai fornitori di servizi cloud, al fine di garantire che

l'etichettatura sia preservata anche all'interno di infrastrutture gestite da terzi. Il livello di classificazione guida le scelte relative alla crittografia e alla localizzazione geografica dei dati.

## 5. GESTIONE DELLE INFORMAZIONI

### 5.1 TRATTAMENTO DELLE INFORMAZIONI

CAMELOT è impegnata ad assicurare che ogni informazione sia trattata in modo coerente con il proprio livello di classificazione, applicando misure di protezione proporzionate al rischio durante l'intero ciclo di vita del dato.

- ❖ **Informazioni “riservate”.** L'accesso è limitato, tracciato e soggetto ad autenticazione nominativa; i sistemi che ospitano tali informazioni non consentono accessi anonimi. La crittografia protegge i dati sia a riposo (at-rest) sia in transito su reti pubbliche, con gestione delle chiavi conforme alla **QSP\_IS\_ECM - Encryption and Cryptographic Key Management**. I dischi dei laptop e dei dispositivi mobili che contengono informazioni “riservate” sono crittografati e protetti da autenticazione forte; il blocco schermo automatico si attiva dopo un periodo di inattività. L'archiviazione su dispositivi personali o supporti rimovibili non approvati non è consentita; i backup sono crittografati. CAMELOT applica misure di DLP ai sistemi, alle reti e ai dispositivi che elaborano informazioni “riservate”, al fine di rilevare e impedire estrazioni o comunicazioni non autorizzate. La creazione di materiale cartaceo contenente PII è limitata allo stretto necessario e l'eventuale materiale cartaceo contenente informazioni “riservate” viene distrutto in modo sicuro mediante taglio trasversale o triturazione.
- ❖ **Informazioni “limitate”.** L'accesso è concesso esclusivamente sulla base della necessità operativa documentata. I sistemi che ospitano informazioni “limitate” non consentono accessi anonimi e i documenti cartacei sono conservati in armadi protetti da chiave, come predisposto nella sede di Genova, e smaltiti in modo sicuro al termine del periodo di conservazione.
- ❖ **Informazioni “pubbliche”.** Non richiedono controlli di accesso specifici e possono essere distribuite liberamente all'esterno di CAMELOT. L'integrità del contenuto resta tuttavia protetta per impedire alterazioni non autorizzate prima della pubblicazione.

### 5.2 PROTEZIONE DEI DATI DI TEST

CAMELOT promuove l'utilizzo esclusivo di dati sintetici o anonimizzati in tutti gli ambienti di sviluppo e test. L'impiego di dati personali reali in ambienti non di produzione è vietato; eventuali eccezioni richiedono una valutazione del rischio documentata e l'autorizzazione formale delle funzioni competenti, secondo quanto stabilito dalla **QSP-DesCon - Design Control**.

### 5.3 SUPPORTI DI MEMORIZZAZIONE E DISPOSITIVI PORTATILI

I supporti di memorizzazione sono gestiti durante il loro intero ciclo di vita — acquisizione, utilizzo, trasporto e smaltimento — in conformità con il livello di classificazione delle informazioni contenute, come dettagliato

nella **QSP-InfMan - Infrastructure Management**. I supporti portatili e i dispositivi che non consentono la crittografia non devono essere utilizzati per informazioni classificate come *“riservato”*, salvo casi di assoluta necessità documentata. Quando le informazioni lasciano i locali dell'organizzazione su supporti fisici, la protezione mediante crittografia e l'autorizzazione preventiva sono obbligatorie.

#### 5.4 SMALTIMENTO SICURO E RIUTILIZZO DELLE APPARECCHIATURE

Prima dello smaltimento o del riutilizzo, le apparecchiature contenenti supporti di memorizzazione sono sottoposte a procedure di cancellazione sicura (wiping o distruzione crittografica) che rendono i dati non recuperabili. Le apparecchiature che possono aver contenuto PII sono trattate con le medesime precauzioni, indipendentemente dalla certezza della loro presenza. CAMELOT si impegna, altresì, a verificare che i fornitori di servizi cloud adottino procedure equivalenti per lo smaltimento delle risorse.

#### 5.5 PROTEZIONE DEI DOCUMENTI E DELLE REGISTRAZIONI

Le registrazioni dei Sistemi di Gestione della Qualità aziendali e i documenti rilevanti sono protetti da perdita, distruzione, falsificazione, accesso non autorizzato e diffusione indebita. CAMELOT conserva i documenti secondo i periodi definiti nella **Information Retention & Disposal Policy**, garantendo la disponibilità delle informazioni per esigenze operative, legali e di audit. Le copie delle politiche e delle procedure sostituite sono conservate per un periodo minimo di cinque anni dalla data di sostituzione.

#### 5.6 APPARECCHIATURA INCUSTODITA

CAMELOT richiede che i dispositivi contenenti informazioni classificate come *“riservato”* o *“limitato”* siano protetti quando lasciati incustoditi, mediante blocco schermo, disconnessione delle sessioni e custodia fisica adeguata. Tali requisiti si applicano sia alle postazioni nelle sedi aziendali sia ai dispositivi utilizzati in modalità di lavoro remoto.

### 6. TRASFERIMENTO DELLE INFORMAZIONI

CAMELOT disciplina il trasferimento delle informazioni verso l'esterno in funzione del livello di classificazione, al fine di prevenire la divulgazione non autorizzata e garantire la conformità agli obblighi contrattuali e normativi.

Il trasferimento a terzi di informazioni *“riservate”* è consentito unicamente in presenza di un accordo legale o contrattuale che vincoli la parte destinataria a un livello di protezione equivalente e con l'esplicita autorizzazione del Management o del proprietario delle informazioni. Tutti i trasferimenti elettronici avvengono tramite canali crittografati.

Il trasferimento di informazioni *“limitate”* richiede l'approvazione del proprietario delle informazioni e la sottoscrizione di un accordo di riservatezza da parte del destinatario. Anche in questo caso i canali di trasmissione elettronica devono essere protetti da crittografia.

Le informazioni “*pubbliche*” possono essere trasferite liberamente; CAMELOT si limita a verificare che il contenuto sia stato formalmente approvato per la diffusione esterna.

Nell'ambito della fornitura di servizi cloud ai propri clienti, CAMELOT garantisce che i dati dei clienti siano protetti secondo la classificazione concordata contrattualmente e che il trasferimento verso Paesi terzi avvenga esclusivamente nel rispetto delle garanzie previste dalla normativa sulla protezione dei dati personali, come ulteriormente dettagliato nella **Cloud Services Security Policy** e nella **Personally Identifiable Information Policy**.

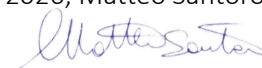
## 7. ARCHIVIAZIONE E AGGIORNAMENTI

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> |