

CAMELOT BIOMEDICAL SYSTEMS SRL

Operations Security Policy

1	10/06/2026	Prima versione	FUMAGALLI	SANTORO
REV	DATA	DESCRIZIONE	AUTORE	APPROVATORE
		Operations Security Policy	Pagina 1 di 13	

Sommario

1.	SCOPO E CAMPO DI APPLICAZIONE	3
2.	ACRONIMI E DEFINIZIONI.....	3
3.	BACKUP	4
4.	PROTEZIONE DEI DATI PERSONALI	5
5.	GESTIONE DEI LOG	6
6.	USO ACCETTABILE DELLE INFORMAZIONI E DEGLI ASSET	7
7.	BRING YOUR OWN DEVICE (BYOD)	8
8.	UTILIZZO DEI SERVIZI CLOUD	8
9.	UTILIZZO DEI SUPPORTI DI MEMORIZZAZIONE RIMOVIBILI	9
10.	SCRIVANIA E SCHERMO PULITI.....	9
11.	GESTIONE DELLE CAPACITÀ	10
12.	GESTIONE DELLE VULNERABILITÀ	11
13.	ARCHIVIAZIONE E AGGIORNAMENTO	11

1. SCOPO E CAMPO DI APPLICAZIONE

La presente politica formalizza l'impegno di CAMELOT Biomedical Systems S.r.l. verso il funzionamento sicuro, affidabile e resiliente di tutti i sistemi, le reti e le infrastrutture di elaborazione delle informazioni utilizzate per la progettazione e lo sviluppo di applicazioni software (SW) e piattaforme cloud. Attraverso questo documento, l'organizzazione definisce i principi e i requisiti che governano le operazioni quotidiane, con l'obiettivo di preservare la riservatezza, l'integrità e la disponibilità delle informazioni proprie e dei clienti, minimizzando i rischi di interruzione del servizio, perdita di dati e incidenti di sicurezza.

La politica costituisce il quadro di riferimento per aree operative quali la gestione dei backup, la registrazione e il monitoraggio degli eventi (log), la gestione delle vulnerabilità tecniche, il controllo dei cambiamenti, l'uso accettabile delle risorse informative, la protezione dei dispositivi e la sicurezza del lavoro da remoto. Essa si inserisce nel Sistema di Gestione della Sicurezza delle Informazioni (SGSI) e si coordina con le politiche e le procedure operative che ne dettagliano l'attuazione.

La presente politica si applica a tutte le sedi operative dell'organizzazione — Genova, Milano e Pescara — e a tutto il personale dipendente, i/le collaboratori/collaboratrici e le terze parti che accedono, gestiscono o utilizzano i sistemi informativi e le risorse IT aziendali. Il perimetro di applicazione comprende l'intera infrastruttura tecnologica, compresi i servizi cloud, i servizi SaaS, i dispositivi endpoint, le reti, le applicazioni, i repository di codice sorgente e i sistemi di gestione centralizzata.

Sono esclusi dal perimetro della presente politica i data center fisici proprietari (attualmente non presenti), in quanto l'organizzazione si avvale esclusivamente di servizi cloud forniti da terze parti qualificate.

2. ACRONIMI E DEFINIZIONI

Backup	Copia di dati, SW o configurazioni di sistema creata e conservata allo scopo di consentire il ripristino in caso di perdita, corruzione o indisponibilità dell'originale
CEO	Chief Executive Officer
Dispositivo endpoint	Dispositivo ICT di tipo hardware connesso in rete [27002 – definizione 3.1.10]
Gestione del cambiamento	Insieme di attività strutturate per valutare, autorizzare, implementare e verificare le modifiche ai sistemi di elaborazione delle informazioni, minimizzando gli impatti negativi sulla sicurezza e sulla continuità operativa
InfM	Infrastructure Manager
IT	Information Technology (tecnologia dell'informazione)

Log	Registrazione cronologica di eventi, attività, eccezioni o guasti generati da sistemi, applicazioni o dispositivi di rete, utilizzata per il monitoraggio, l'analisi e le indagini di sicurezza
MDM	Mobile Device Management
MFA	Multi-Factor Authentication
Multi-tenancy	Architettura in cui più clienti condividono risorse di calcolo, archiviazione o rete all'interno di una medesima infrastruttura cloud, mantenendo l'isolamento logico tra i rispettivi ambienti
NTP	Network Time Protocol
PII	Personally Identifiable Information. 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]
QM	Quality Manager
RSGSI	Responsabile del Sistema di Gestione della Sicurezza delle Informazioni
SA	System Administrator
SaaS	Software as a Service
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]
SSO	Single Sign-On
SW	Software
USB	Universal Serial Bus
Vulnerabilità	Punto di debolezza di un asset (3.1.2) o di un controllo (3.1.8) che può essere sfruttato da una o più minacce (3.1.34) [27002 – definizione 3.1.38]

3. BACKUP

CAMELOT riconosce nel backup delle informazioni un presidio fondamentale per la continuità operativa e la protezione del patrimonio informativo. L'organizzazione si impegna a garantire che copie adeguate di dati, SW

e configurazioni di sistema siano prodotte, conservate e verificate con regolarità, in modo da consentire il ripristino tempestivo in caso di perdita, corruzione o indisponibilità degli originali.

La strategia di backup adottata prevede la differenziazione dei meccanismi in funzione della tipologia di dato trattato e garantisce il backup delle seguenti tipologie di dati: codice sorgente, dati applicativi e configurazioni di sistema.

Per ciascun servizio cloud impiegato, l'organizzazione richiede e verifica le specifiche delle funzionalità di backup offerte dal fornitore, assicurandosi che soddisfino i propri requisiti in termini di ambito, pianificazione, metodi, crittografia, periodi di conservazione e procedure di ripristino. L'organizzazione promuove, ove necessario e possibile, la ridondanza geografica dei dati di backup, avvalendosi delle garanzie contrattuali dei fornitori di servizi cloud che replicano le informazioni su regioni fisicamente distinte. Questa impostazione assicura la protezione contro la perdita di dati anche in caso di eventi che colpiscano un singolo sito di archiviazione.

I backup sono soggetti a test periodici di ripristino, finalizzati a validare l'integrità dei dati conservati e l'effettiva capacità di recupero entro i tempi stabiliti. L'organizzazione si impegna, inoltre, a proteggere le copie di backup da accessi non autorizzati, applicando misure di cifratura per le informazioni classificate come riservate e controlli di accesso coerenti con il livello di classificazione assegnato.

Quando l'organizzazione agisce in qualità di responsabile del trattamento di dati personali nel cloud, adotta una politica specifica che disciplina i requisiti di backup per le PII, compresi gli obblighi contrattuali e normativi relativi alla cancellazione dei dati personali contenuti nelle copie di backup al termine del periodo di conservazione.

4. PROTEZIONE DEI DATI PERSONALI

L'organizzazione è fermamente impegnata nella tutela delle PII trattate nell'ambito delle proprie operazioni, sia quando agisce come titolare sia quando opera in qualità di responsabile del trattamento per conto della propria clientela. Questo impegno si fonda sui principi di liceità, correttezza e trasparenza, limitazione della finalità, minimizzazione dei dati, integrità e riservatezza, nonché di protezione dei dati fin dalla progettazione e per impostazione predefinita in coerenza con quanto definito nella **Privacy Policy** e nella **Personally Identifiable Information Policy**.

CAMELOT adotta misure tecniche e organizzative proporzionate ai rischi identificati per assicurare che le PII siano protette da accessi non autorizzati, perdita, alterazione o divulgazione indebita. Tra tali misure rientrano il controllo degli accessi basato sui ruoli, la cifratura dei dati a riposo e in transito e la separazione degli ambienti di sviluppo e produzione, con divieto di utilizzo di dati personali reali negli ambienti di test. È inoltre prevista la registrazione degli accessi alle PII per finalità di tracciabilità e audit.

Quando l'organizzazione tratta PII per conto della propria clientela di servizi cloud, essa si impegna a:

- elaborare i dati esclusivamente secondo le istruzioni documentate della clientela, senza utilizzarli per finalità proprie;

- fornire alla clientela i mezzi tecnici e organizzativi per adempiere ai diritti degli interessati;
- notificare tempestivamente alla clientela in caso di violazione dei dati;
- comunicare preventivamente l'eventuale ricorso a sub-responsabili, assicurando che questi rispettino obblighi di protezione equivalenti;
- specificare contrattualmente le localizzazioni geografiche in cui i dati possono essere trattati.

I sistemi di log registrano gli accessi e le operazioni su dati personali — incluse le divulgazioni a terzi — con indicazione dell'autore, della tipologia di dato e della data dell'evento. I file temporanei generati durante le operazioni ordinarie contenenti PII sono eliminati in modo sicuro entro un periodo documentato. L'organizzazione mantiene un registro dei trattamenti aggiornato e rende disponibile l'informativa sul trattamento dei dati personali a tutti gli interessati, riesaminandola periodicamente o in occasione di modifiche significative alle modalità di gestione dei dati.

5. GESTIONE DEI LOG

L'organizzazione riconosce nella registrazione e nel monitoraggio degli eventi un pilastro essenziale per la rilevazione di anomalie, la risposta agli incidenti e la dimostrazione di conformità. CAMELOT si impegna a produrre, conservare, proteggere e analizzare registri che documentino le attività degli utenti, le eccezioni, i guasti e gli eventi rilevanti per la sicurezza delle informazioni su tutti i sistemi, le applicazioni e i dispositivi in ambito.

I log registrano, come minimo, le azioni degli utenti, le operazioni dei/delle SA, gli accessi ai dati personali, gli errori e le anomalie operative, consentendo di determinare le cause degli incidenti di sicurezza e di supportare eventuali indagini. Particolare attenzione è rivolta alla registrazione delle operazioni privilegiate: ogni attività svolta con diritti amministrativi è tracciata e soggetta a revisione periodica.

L'organizzazione promuove il monitoraggio in tempo reale delle reti, dei sistemi e delle applicazioni per individuare comportamenti anomali, avvalendosi di strumenti che generano notifiche automatiche al personale preposto alla risposta agli incidenti quando vengono rilevati eventi critici. Le pagine di stato pubbliche dei servizi utilizzati integrano le attività di supervisione operativa, offrendo visibilità in tempo reale sulla disponibilità dei servizi.

Le informazioni di log sono protette da alterazione, accesso non autorizzato e cancellazione prematura. L'organizzazione adotta controlli di accesso che limitano la consultazione dei registri al personale autorizzato e ne garantiscono l'utilizzo esclusivo per le finalità previste. Quando i log contengono dati personali, sono applicate misure aggiuntive di protezione coerenti con i requisiti normativi applicabili, compresa la cancellazione (preferibilmente automatica) entro un periodo documentato.

La sincronizzazione degli orologi è assicurata mediante server NTP di riferimento, in particolare per le postazioni di lavoro la sincronizzazione è configurata centralmente tramite l'MDM aziendale (per esempio Microsoft Intune); entrambe le sincronizzazioni garantiscono la correlabilità temporale degli eventi registrati su piattaforme diverse e supportano l'analisi integrata in caso di incidente. Le misure di sicurezza della rete e

di controllo degli accessi che concorrono alla protezione dell'infrastruttura di logging sono disciplinate dalla **QSP-NSM - Network System Management** e dalla **QSP_IS_MCLA - Management and Control of Logical Access**.

L'organizzazione riesamina periodicamente l'adeguatezza dei log generati, verificando che la copertura, il livello di dettaglio e i tempi di conservazione rispondano alle esigenze operative, alle prescrizioni contrattuali e ai requisiti normativi. Nell'ambito dei servizi cloud, CAMELOT definisce i propri requisiti di registrazione degli eventi e verifica che i fornitori di servizi cloud li soddisfino, richiedendo l'accesso ai soli record relativi alle proprie attività nel rispetto dell'isolamento tra tenant.

6. USO ACCETTABILE DELLE INFORMAZIONI E DEGLI ASSET

CAMELOT adotta regole chiare e vincolanti per l'uso delle informazioni e delle risorse associate, al fine di tutelare il patrimonio informativo aziendale e quello dei clienti. Ogni risorsa — dato, applicazione, servizio, dispositivo o infrastruttura — è affidata al personale autorizzato esclusivamente per lo svolgimento delle attività lavorative assegnate, nel rispetto del principio del need-to-know e del livello di classificazione attribuito.

L'organizzazione identifica e documenta gli utenti autorizzati all'uso delle informazioni, stabilendo per ciascuna risorsa le condizioni di accesso, le modalità di utilizzo consentite e i vincoli derivanti dalla classificazione. L'accesso è regolato attraverso un modello autorizzativo che assegna diritti coerenti con le responsabilità operative di ciascun incaricato, applicando il principio del privilegio minimo.

Il personale è tenuto a:

- utilizzare le risorse informative esclusivamente per finalità aziendali legittime;
- rispettare le regole stabilite dalla **Classification & Labeling of Information Policy**, trattando ogni informazione in modo coerente con il livello di protezione ad essa associato;
- non divulgare informazioni classificate come riservate o limitate a soggetti non autorizzati, salvo esplicita autorizzazione formale;
- proteggere le credenziali di accesso, non condividerle e segnalare tempestivamente qualsiasi sospetto di compromissione;
- restituire tutte le risorse aziendali al termine del rapporto di lavoro o in caso di variazione delle responsabilità.

L'organizzazione formalizza l'assegnazione degli asset al personale, in conformità alla **QSP-InfMan – Infrastructure Management**, registrandola nell'**InfPla - Infrastructure Plan** e mantenendo aggiornata la tracciabilità degli accessi, delle risorse assegnate e delle relative autorizzazioni.

7. BRING YOUR OWN DEVICE (BYOD)

L'organizzazione adotta un approccio restrittivo nei confronti dell'utilizzo di dispositivi personali per l'accesso alle risorse informative aziendali. CAMELOT assegna a ciascun collaboratore i dispositivi necessari allo svolgimento delle proprie attività, gestiti centralmente tramite una piattaforma di Mobile Device Management, che consente l'applicazione uniforme delle politiche di sicurezza, il controllo delle configurazioni e il monitoraggio della conformità.

L'uso di dispositivi personali per accedere a informazioni aziendali è consentito soltanto in casi eccezionali e a condizione che il dispositivo sia conforme ai requisiti minimi di sicurezza stabiliti dall'organizzazione, tra cui (ove applicabili):

- protezione mediante password alfanumerica con requisiti di complessità adeguati;
- attivazione del blocco automatico dello schermo dopo un periodo massimo di cinque minuti di inattività;
- cifratura del disco di archiviazione;
- aggiornamento del sistema operativo e delle definizioni antimalware.

L'organizzazione si riserva il diritto di definire le condizioni tecniche e organizzative alle quali l'accesso da dispositivo personale può essere autorizzato, nonché di revocare tale autorizzazione in qualsiasi momento qualora le condizioni di sicurezza non siano soddisfatte. In generale, la memorizzazione di informazioni classificate come riservate e i dati sensibili, su dispositivi personali non approvati è vietata in ogni circostanza.

8. UTILIZZO DEI SERVIZI CLOUD

CAMELOT riconosce nei servizi cloud un elemento centrale della propria infrastruttura operativa e si impegna a gestirne l'acquisizione, l'utilizzo e l'eventuale dismissione in conformità ai requisiti di sicurezza delle informazioni stabiliti dal SGSI. L'organizzazione utilizza servizi cloud di fornitori qualificati e ne governa l'impiego secondo il modello di responsabilità condivisa, in cui le obbligazioni di sicurezza sono ripartite tra il fornitore e la clientela del servizio.

L'organizzazione adotta i seguenti principi per la gestione dei servizi cloud:

- ogni nuovo servizio cloud è soggetto a una valutazione preventiva del rischio, che considera l'isolamento multi-tenant, le capacità di protezione dei dati, la localizzazione geografica dei data center e la conformità a standard di sicurezza riconosciuti;
- i requisiti di sicurezza — compresi backup, crittografia, gestione degli accessi, monitoraggio e registrazione degli eventi — sono verificati rispetto alle specifiche del servizio offerto dal fornitore;
- l'accesso ai servizi cloud è regolato tramite il sistema di gestione delle identità centralizzato e preferenzialmente con accesso SSO e con autenticazione MFA per tutti i sistemi in funzione del livello di criticità di servizio e ove tecnicamente supportato;

- i contratti con i fornitori cloud definiscono le modalità di restituzione dei dati, la cancellazione sicura alla cessazione del rapporto e la portabilità delle informazioni;
- la conformità dei fornitori di servizi cloud è periodicamente riesaminata in relazione alla documentazione contrattuale e alle configurazioni tecniche effettive.

Quando l'organizzazione fornisce servizi cloud ai propri clienti, documenta il modello di responsabilità condivisa applicabile a ciascun servizio, assicura l'isolamento tra i tenant attraverso la segregazione dell'infrastruttura virtuale e garantisce trasparenza sulle procedure operative, sulle capacità di monitoraggio e sulle misure di protezione adottate. La **Cloud Services Security Policy** dettaglia i requisiti specifici per entrambi i ruoli — clientela e fornitore di servizi cloud — assunti dall'organizzazione.

9. UTILIZZO DEI SUPPORTI DI MEMORIZZAZIONE RIMOVIBILI

CAMELOT ha disposto il divieto di collegare ai dispositivi aziendali hard disk esterni, chiavette USB o qualsiasi altro supporto di memoria che non sia stato preventivamente ed esplicitamente autorizzato dall'/dalla InfM, riconoscendo il rischio che tali dispositivi possano introdurre minacce alla sicurezza o consentire l'esfiltrazione non autorizzata di informazioni. L'impiego di tali supporti è autorizzato esclusivamente in casi eccezionali e previa approvazione formale.

Quando l'uso è autorizzato, l'organizzazione richiede che:

- il supporto rechi un'etichetta fisica che ne identifichi chiaramente il contenuto e il livello di classificazione;
- la memorizzazione di informazioni classificate come riservate su supporti rimovibili non approvati sia vietata in ogni circostanza;
- i dati trasferiti su supporti rimovibili contenenti PII siano protetti mediante cifratura con algoritmi adeguati;
- ogni movimento di supporti contenenti dati personali al di fuori dei locali aziendali sia formalmente autorizzato, documentato e tracciato;
- lo smaltimento dei supporti dismessi avvenga secondo modalità sicure che impediscano il recupero dei dati, anche con tecniche forensi.

L'organizzazione gestisce i supporti di memorizzazione attraverso l'intero ciclo di vita — acquisizione, utilizzo, trasporto e smaltimento — in conformità allo schema di classificazione adottato e ai requisiti della **QSP-InfMan – Infrastructure Management**.

10. SCRIVANIA E SCHERMO PULITI

CAMELOT promuove una cultura della riservatezza negli ambienti di lavoro, adottando regole chiare per la protezione delle informazioni visibili su scrivanie e schermi. Questa disciplina mira a prevenire l'accesso non

autorizzato, la divulgazione accidentale e la perdita di informazioni classificate, tanto nei locali aziendali quanto negli ambienti di lavoro remoto.

L'organizzazione, in accordo con quanto stabilito nella **QSP-NSM - Network System Management**, stabilisce che:

- documenti cartacei e supporti rimovibili contenenti informazioni classificate come riservate o limitate non devono essere lasciati incustoditi sulle scrivanie al termine dell'attività lavorativa o in caso di assenza prolungata dalla postazione;
- i dispositivi di elaborazione sono configurati con blocco automatico dello schermo entro pochi minuti di inattività, protetto da password/PIN alfanumerici con requisiti di complessità adeguati;
- il personale è tenuto a bloccare manualmente il proprio dispositivo ogni volta che si allontana dalla postazione, anche per brevi periodi;
- le informazioni sensibili visualizzate su schermo non devono essere esposte alla vista di persone non autorizzate, con particolare attenzione negli spazi condivisi e durante le attività da remoto.

Queste misure sono applicate in modo uniforme su tutti i dispositivi gestiti dall'organizzazione attraverso la piattaforma centralizzata di gestione dei dispositivi, che impone le configurazioni di sicurezza quali il time-out dello schermo e i requisiti di complessità delle credenziali.

11. GESTIONE DELLE CAPACITÀ

L'organizzazione è impegnata nel monitoraggio continuo delle risorse critiche per le proprie operazioni — capacità di elaborazione, archiviazione, rete e personale chiave — al fine di assicurare che la disponibilità dei servizi non sia compromessa da carenze di risorse. CAMELOT adotta un approccio proattivo alla gestione della capacità, fondato sulla sorveglianza sistematica dell'utilizzo e sulla previsione delle esigenze future.

L'organizzazione persegue i seguenti obiettivi:

- monitorare l'utilizzo delle risorse dei servizi cloud in uso, verificando che la capacità contrattualmente concordata con ciascun fornitore soddisfi le esigenze operative correnti e prevedibili;
- definire soglie massime di capacità per ciascuna risorsa critica e attivare tempestivamente processi di adeguamento al raggiungimento di tali soglie;
- avvalersi delle statistiche di utilizzo messe a disposizione dai fornitori di servizi cloud per valutare i livelli massimi e i trend di consumo delle risorse;
- considerare i vincoli di capacità propri di ciascun servizio o abbonamento cloud, pianificando per tempo eventuali evoluzioni contrattuali quando le esigenze li superano.

L'allocazione elastica e scalabile delle risorse offerta dai servizi cloud utilizzati rappresenta un fattore abilitante; tuttavia, l'organizzazione riconosce che essa non elimina la necessità di un presidio attivo, poiché

vincoli specifici possono sussistere in termini di processori, spazio di archiviazione o larghezza di banda. La gestione della capacità è integrata nei processi di riesame operativo e contribuisce alla prevenzione degli incidenti di sicurezza delle informazioni causati dall'esaurimento delle risorse.

12. GESTIONE DELLE VULNERABILITÀ

CAMELOT si impegna a ottenere informazioni tempestive sulle vulnerabilità tecniche dei propri sistemi informativi, a valutare il livello di esposizione dell'organizzazione e ad adottare misure proporzionate al rischio identificato. La gestione delle vulnerabilità è un processo continuativo che combina strumenti automatizzati, pratiche di sviluppo sicuro e collaborazione con i fornitori di servizi cloud.

L'organizzazione promuove i seguenti principi:

- esecuzione regolare di scansioni delle vulnerabilità su dispositivi, applicazioni e infrastruttura, nonché in occasione di cambiamenti significativi all'ambiente operativo;
- integrazione, nei processi di Continuous Integration, di valutazioni automatizzate per l'identificazione delle vulnerabilità lungo l'intero ciclo di vita dello sviluppo SW;
- identificazione, documentazione e trattamento delle vulnerabilità con impatto significativo, che vengono gestite secondo il processo di risposta agli incidenti qualora il rischio lo richieda;
- richiesta ai fornitori di servizi cloud di informazioni sulla gestione delle vulnerabilità tecniche che possono influire sui servizi forniti e chiara definizione delle responsabilità rispettive;
- limitazione rigorosa dell'installazione di SW ai soli programmi approvati e distribuiti centralmente, con gli utenti configurati come account standard privi di privilegi amministrativi, così da ridurre la superficie d'attacco.

L'organizzazione identifica i servizi da sottoporre a penetration test sulla base di una valutazione del rischio e degli eventuali requisiti contrattuali concordati con clienti e/o fornitori. I risultati dei test alimentano il processo di analisi dei rischi e supportano la definizione e l'attuazione delle necessarie azioni correttive. La protezione dai malware è garantita mediante soluzioni antimalware costantemente aggiornate, installate su tutti i dispositivi gestiti dall'organizzazione e integrate con le funzionalità di sicurezza native dei servizi cloud adottati.

La **QSP_IS_RM - Risk Management** fornisce il quadro metodologico per la valutazione e il trattamento dei rischi associati alle vulnerabilità tecniche, mentre la **QSP-DesCon - Design Control** disciplina i controlli di sicurezza integrati nel ciclo di vita del SW.

13. ARCHIVIAZIONE E AGGIORNAMENTO

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/