

CAMELOT BIOMEDICAL SYSTEMS SRL

Cloud Services Security Policy

1	10/06/2026	Prima versione	FUMAGALLI	SANTORO
REV	DATA	DESCRIZIONE	AUTORE	APPROVATORE
		Cloud Services Security Policy	Pagina 1 di 9	

Sommario

1.	SCOPO E CAMPO DI APPLICAZIONE	3
2.	ACRONIMI E DEFINIZIONI.....	3
3.	PRINCIPI DI SICUREZZA PER I SERVIZI CLOUD.....	4
3.1	VALUTAZIONE DEL RISCHIO E SELEZIONE DEI FORNITORI	4
3.2	GESTIONE DELLE IDENTITÀ E DEGLI ACCESSI.....	4
3.3	PROTEZIONE DEI DATI NEL CLOUD	5
3.4	GESTIONE OPERATIVA E MONITORAGGIO	5
3.5	GESTIONE DEGLI INCIDENTI DI SICUREZZA CLOUD.....	5
4.	REQUISITI SPECIFICI PER LA FORNITURA DI SERVIZI CLOUD	6
4.1	DEFINIZIONE DEI SERVIZI CLOUD E GESTIONE DELLE CAPACITÀ	6
4.2	GESTIONE DELLA SICUREZZA E DEI SUB-FORNITORI.....	6
4.3	SICUREZZA DELL'INFRASTRUTTURA VIRTUALE	6
4.4	TRASPARENZA OPERATIVA	6
5.	REQUISITI SPECIFICI PER L'UTILIZZO DI SERVIZI CLOUD	7
5.1	GESTIONE CONTRATTUALE E DELLA CESSAZIONE DEL SERVIZIO	7
5.2	VERIFICA DEI DIRITTI DI PROPRIETÀ INTELLETTUALE E DELLE LICENZE SOFTWARE	7
5.3	VERIFICA DEI CONTROLLI DI SICUREZZA DELLE INFORMAZIONI	7
6.	REQUISITI SPECIFICI PER LA PROTEZIONE DELLE PII.....	7
6.1	PROTEZIONE DELLE PII SIN DALLA FASE DI PROGETTAZIONE E PER IMPOSTAZIONE PREDEFINITA..	7
6.2	LEGITTIMITÀ, FINALITÀ E MINIMIZZAZIONE	8
6.3	TRASPARENZA E DIRITTI DEGLI INTERESSATI	8
6.4	SICUREZZA E RISERVATEZZA	8
7.	ARCHIVIAZIONE E AGGIORNAMENTI	8

1. SCOPO E CAMPO DI APPLICAZIONE

La presente politica definisce i principi e i requisiti per la gestione della sicurezza delle informazioni negli ambienti di cloud computing utilizzati o forniti da CAMELOT Biomedical Systems S.r.l. Lo scopo è garantire che i dati, i sistemi e i servizi gestiti nel cloud siano protetti in conformità con gli standard di settore, i requisiti contrattuali e le normative vigenti, con particolare riferimento agli standard ISO/IEC 27017 e ISO/IEC 27018.

Questa politica si applica a tutto il personale, ai/alle collaboratori/collaboratrici e alle terze parti che progettano, sviluppano, gestiscono o utilizzano servizi cloud per conto dell'azienda.

2. ACRONIMI E DEFINIZIONI

AM	Account Manager
Cliente di servizi cloud	Parte (3.3.1) che agisce nel ruolo di cliente del servizio cloud (3.3.14) [22123 – definizione 3.3.2]
DPO	Data Protection Officer
Fornitore di servizi cloud	Parte (3.3.1) che agisce nel ruolo di fornitore del servizio cloud (3.3.15) [22123 – definizione 3.3.3]
InfM	Infrastructure Manager
Interessato	Persona fisica a cui i dati personali si riferiscono [27002 – definizione 3.1.22]
MFA	Multi-Factor Authentication
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]
PriM	Privacy Manager
PurM	Purchase Manager
QM	Quality Manager
Responsabile del trattamento delle PII	Stakeholder relativo alla privacy che tratta dati personali (3.1.21) per conto e in conformità alle istruzioni di un titolare [27002 – definizione 3.1.23]
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]

Titolare del trattamento delle PII

Stakeholder relativo alla privacy che determina le finalità e i mezzi del trattamento di PII escludendo le persone fisiche che usano i dati per scopi esclusivamente personali [29100 – definizione 3.8]

TM

Technologies' Manager

3. PRINCIPI DI SICUREZZA PER I SERVIZI CLOUD

La presente sezione definisce i principi fondamentali che CAMELOT adotta per garantire la sicurezza delle informazioni, dei sistemi e dei dati gestiti in ambienti di cloud computing, sia in qualità di cliente che di fornitore di servizi cloud.

3.1 VALUTAZIONE DEL RISCHIO E SELEZIONE DEI FORNITORI

Il/La RSGSI, in collaborazione con il/la PurM, dovrà assicurare che tutti i fornitori di servizi cloud siano sottoposti a una valutazione del rischio prima della stipula di qualsiasi contratto. Tale valutazione deve considerare, come minimo:

- La capacità del fornitore di garantire l'isolamento in ambienti multi-tenant.
- Le politiche e le capacità tecniche del fornitore per la protezione dei dati, inclusa la crittografia.
- I rischi associati all'accesso del personale del fornitore ai dati e ai sistemi di CAMELOT.
- L'ubicazione geografica dei data center dove i dati possono essere archiviati o elaborati, per garantire la conformità con i requisiti legali e contrattuali applicabili.
- La conformità del fornitore a standard di sicurezza riconosciuti come ISO/IEC 27001, ISO/IEC 27017 e ISO/IEC 27018.

Le attività di valutazione e selezione sono condotte in accordo con la **QSP-InfMan - Infrastructure Management** e la **QSP-IS_RM - Risk Management**.

3.2 GESTIONE DELLE IDENTITÀ E DEGLI ACCESSI

L'/La InfM dovrà implementare e mantenere controlli di accesso per tutti i servizi cloud, in conformità con la "PRO Procedura di gestione e controllo degli accessi logici". I seguenti principi sono obbligatori:

- **Minimo privilegio:** agli/alle utenti e ai sistemi deve essere concesso solo l'accesso strettamente necessario per svolgere le proprie funzioni.
- **Autenticazione forte:** l'accesso a tutte le console di amministrazione dei servizi cloud e agli account con privilegi elevati dovrà richiedere l'uso di meccanismi di autenticazione a più fattori (MFA).

- **Ciclo di vita degli accessi:** la creazione, la modifica e la revoca degli account utente per i servizi cloud devono seguire un processo formalizzato e tracciato, gestito centralmente.
- **Restrizione dell'accesso:** l'azienda, in qualità di cliente, dovrà assicurarsi che i servizi cloud utilizzati permettano di limitare l'accesso alle informazioni in base alla propria politica di controllo degli accessi. In qualità di fornitore, l'azienda dovrà fornire ai propri clienti controlli di accesso che consentano loro di limitare l'accesso ai servizi e ai dati.

3.3 PROTEZIONE DEI DATI NEL CLOUD

Il/La RSGSI dovrà garantire che tutti i dati aziendali e dei clienti gestiti in ambienti cloud siano protetti in base alla loro classificazione, come definito nella **Classification & Labeling of Information Policy**.

- **Crittografia:** tutti i dati classificati come “riservati” o di livello superiore dovranno essere protetti tramite crittografia sia a riposo (at-rest) che in transito (in-transit), utilizzando algoritmi e protocolli conformi agli standard di settore. La gestione delle chiavi crittografiche deve seguire la **QSP_IS_ECM - Encryption and Cryptographic Key Management**.
- **Localizzazione dei dati:** il/La PriM, in accordo con il/La RSGSI, dovrà definire e approvare le aree geografiche in cui i dati, in particolare le PII, possono essere archiviati ed elaborati, in conformità con i requisiti normativi e contrattuali.

3.4 GESTIONE OPERATIVA E MONITORAGGIO

L'/La InfM dovrà definire e documentare le procedure operative per le attività di amministrazione critiche negli ambienti cloud, quali l'installazione, la modifica o l'eliminazione di risorse virtuali (server, reti, storage), nonché le procedure di backup e ripristino. Tali operazioni devono essere monitorate da un supervisore per prevenire incidenti. Inoltre, l'/la InfM dovrà:

- In qualità di cliente, richiedere ai fornitori di servizi cloud le informazioni sulle funzionalità di monitoraggio disponibili.
- In qualità di fornitore, fornire alla clientela funzionalità adeguate a monitorare l'utilizzo dei loro servizi, garantendo che l'accesso a tali funzionalità sia controllato e limitato alle informazioni di pertinenza del singolo cliente. Le attività di monitoraggio sono disciplinate dalla **QSP_IS_MM - Monitoring and Measurement**.

3.5 GESTIONE DEGLI INCIDENTI DI SICUREZZA CLOUD

Il/La RSGSI dovrà garantire che la procedura “QSP-ISIM - Information Security Incident Management” includa disposizioni specifiche per gli ambienti cloud. Questo processo deve definire:

- Le modalità di rilevamento e risposta agli incidenti che coinvolgono servizi cloud.
- I protocolli di comunicazione e le responsabilità per la notifica degli incidenti ai fornitori di servizi cloud, ai clienti, alle autorità competenti e al/alla DPO, ove applicabile.

- Le linee guida per la raccolta di evidenze a supporto delle indagini e delle attività forensi, in collaborazione con il fornitore di servizi cloud.

4. REQUISITI SPECIFICI PER LA FORNITURA DI SERVIZI CLOUD

4.1 DEFINIZIONE DEI SERVIZI CLOUD E GESTIONE DELLE CAPACITÀ

Nel caso di fornitura di cloud a nostri clienti, CAMELOT sulla base dei diversi modelli di business può agire in due modi: o (responsabilità dell'AM) provvedendo a documentare e comunicare alla clientela il modello di responsabilità condivisa relativo ai servizi cloud offerti, definendo in modo chiaro le responsabilità di CAMELOT e quelle del cliente in materia di sicurezza oppure (responsabilità del PM) definendo le stesse informazioni all'interno degli Input Requirements di progetto.

Qualora siano richiesti approfondimenti di natura tecnica o richieste specifiche relativi a particolari servizi, configurazioni o esigenze del cliente, l'/la AM o l'/la PM si possono avvalere del supporto del/della TM o del/della RSGSI se necessario. Responsabilità del/della PM assicurarsi la corretta comprensione da parte del cliente e che siano chiare le competenze di responsabilità tra le parti.

4.2 GESTIONE DELLA SICUREZZA E DEI SUB-FORNITORI

In caso sussistano sub-fornitori, il/la RSGSI, in collaborazione con il/la PurM, dovrà garantire che i requisiti di sicurezza delle informazioni e di protezione delle PII applicabili ai servizi offerti ai clienti siano trasferiti contrattualmente a tutti i sub-fornitori (es. provider di infrastrutture come AWS) che contribuiscono all'erogazione del servizio.

4.3 SICUREZZA DELL'INFRASTRUTTURA VIRTUALE

L'/La InfM dovrà implementare e mantenere controlli tecnici per garantire la segregazione degli ambienti virtuali.

- **Isolamento dei tenant:** le risorse dei clienti (dati, applicazioni, reti) in ambienti multi-tenant dovranno essere separate logicamente per impedire accessi non autorizzati tra clienti diversi.
- **Hardening delle macchine virtuali:** le immagini delle macchine virtuali utilizzate per erogare i servizi dovranno essere configurate secondo principi di hardening, come descritto nella **QSP-DesCon - Design Control**.
- **Allineamento della sicurezza di rete:** la configurazione delle reti virtuali dovrà essere coerente con le policy definite per la rete fisica, come stabilito nella **QSP-NSM - Network System Management**.

4.4 TRASPARENZA OPERATIVA

Nei contratti per i quali è previsto, il/la SA dovrà rendere disponibile ai clienti, su richiesta, la documentazione relativa alle procedure operative critiche e alle capacità di monitoraggio dei servizi cloud forniti, come specificato negli accordi contrattuali, nelle specifiche di progetto o nei Service Level Agreement (SLA).

5. REQUISITI SPECIFICI PER L'UTILIZZO DI SERVIZI CLOUD

5.1 GESTIONE CONTRATTUALE E DELLA CESSAZIONE DEL SERVIZIO

Il/La PurM, con il supporto del/della RSGSI e del/della PriM, dovrà assicurare che ogni contratto con un fornitore di servizi cloud includa clausole specifiche che disciplinino la cessazione del servizio. Tali clausole devono definire:

- Le modalità e le tempistiche per la restituzione di tutti gli asset del cliente, inclusi i dati.
- L'obbligo per il fornitore di procedere alla cancellazione sicura di tutte le copie dei dati dai propri sistemi dopo la restituzione.
- I formati di dati per la restituzione, per garantirne la portabilità. Le procedure di cancellazione devono essere conformi alla **Information Retention & Disposal Policy**.

5.2 VERIFICA DEI DIRITTI DI PROPRIETÀ INTELLETTUALE E DELLE LICENZE SOFTWARE

Il/La SA dovrà istituire una procedura per verificare la conformità delle licenze software prima di installare qualsiasi software in un ambiente cloud. Particolare attenzione deve essere prestata ai modelli di licenza in ambienti elastici e scalabili, per evitare violazioni dovute all'aumento del numero di sistemi o core di processore utilizzati.

5.3 VERIFICA DEI CONTROLLI DI SICUREZZA DELLE INFORMAZIONI

Il/La RSGSI dovrà eseguire revisioni periodiche della conformità dei fornitori di servizi cloud rispetto alle politiche e agli standard di sicurezza aziendali. Tali attività, svolte in conformità alla **QSP-IntAud - Internal Audits**, possono includere:

- La revisione della documentazione di conformità del fornitore (es. certificazioni, report di audit).
- L'esecuzione di verifiche tecniche sulla configurazione dei servizi cloud utilizzati per assicurare l'aderenza ai requisiti di sicurezza aziendali.

6. REQUISITI SPECIFICI PER LA PROTEZIONE DELLE PII

La presente sezione, in linea con la norma ISO/IEC 27018 e la **Personally Identifiable Information Policy**, definisce i requisiti per il trattamento delle PII in ambienti cloud pubblici in cui CAMELOT agisce come responsabile del trattamento per conto dei propri clienti.

6.1 PROTEZIONE DELLE PII SIN DALLA FASE DI PROGETTAZIONE E PER IMPOSTAZIONE PREDEFINITA

Il/La SA e il/La PriM dovranno garantire che i principi di "*privacy by design*" e "*privacy by default*" siano integrati nella progettazione e configurazione di qualsiasi servizio cloud che tratti PII. Questo include la minimizzazione

dei dati raccolti e l'implementazione di misure di protezione adeguate fin dall'inizio, come descritto nella **QSP-DPM - Data Protection Management**.

6.2 LEGITTIMITÀ, FINALITÀ E MINIMIZZAZIONE

Il/La PriM dovrà assicurare che ogni trattamento di PII in ambiente cloud sia supportato da una base giuridica valida e che i dati siano trattati solo per le finalità esplicite e legittime definite contrattualmente con il cliente (titolare del trattamento). Il trattamento deve essere limitato alle PII strettamente necessarie per tali finalità.

6.3 TRASPARENZA E DIRITTI DEGLI INTERESSATI

Il/La PriM, in collaborazione con il/la DPO, dovrà garantire che siano in atto procedure per supportare il cliente (titolare del trattamento) nell'adempimento dei suoi obblighi verso gli interessati, quali le richieste di accesso, rettifica, cancellazione e portabilità dei dati.

6.4 SICUREZZA E RISERVATEZZA

Il/La RSGSI e il/la PriM dovranno garantire che gli accordi contrattuali con i clienti definiscano chiaramente le responsabilità per la protezione delle PII. Tali accordi devono includere:

- L'impegno a trattare le PII solo su istruzione documentata del cliente.
- L'obbligo di garantire la riservatezza da parte del personale autorizzato al trattamento.
- L'implementazione di misure di sicurezza tecniche e organizzative adeguate al rischio.
- La definizione di procedure per la notifica delle violazioni di dati personali (*data breach*) al cliente senza ingiustificato ritardo.

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: camelotbio@legalmail.it E-mail: info@camelotbio.com Web: https://www.camelotbio.com/