Blobb

VENDOR SECURITY REFERENCE

Security Overview and Questionnaire

How Blobb Eco Technologies Inc. handles client data, access, and infrastructure across cloud consulting, software development, technical audits, and fractional CTO engagements.

Blobb Eco Technologies Inc.
Comox, British Columbia, Canada

Version 1.0
[Month] 2026

Contents

This document answers the questions most often raised in a client vendor security review. It is intended to stand on its own or to accompany a client's own questionnaire.

01 Purpose and How to Use This Document

This document sets out how Blobb Eco Technologies Inc. ("Blobb") manages security across our engagements: cloud infrastructure consulting, software development, technical audits (including the security pillar), and fractional CTO work. It is written to answer the questions most commonly raised in a client vendor security review, so that a formal back-and-forth questionnaire is rarely needed.

If your organization uses a standard vendor security questionnaire, this page should cover the majority of it. For anything not addressed here, or for a signed copy of this document, contact us directly using the details in Section 14.

02 Company and Team

Legal entity	Blobb Eco Technologies Inc., incorporated in British Columbia, Canada
Location	Comox, British Columbia, Canada. Fully remote practice.
Founders	Muriel Marc and Xavier Raffin
Services	Cloud infrastructure architecture and audits, software development, technical due diligence, security pillar audits, fractional CTO engagements

Team structure

Blobb is operated by its two founders, Muriel Marc and Xavier Raffin, whose skill sets are complementary with some deliberate overlap for coverage. Depending on the size and nature of an engagement, we occasionally bring on additional staff, as we did for a past engagement with Canal+. Any such addition is disclosed to the client in advance and works under Blobb's direction and security practices. We do not sub-contract engagement work to third-party firms.

03 Engagement Model and Data Handling

Each engagement begins with a Statement of Work that defines scope, duration, and the systems and data we will access. We access only what the engagement requires.

- Client data is handled according to its sensitivity, as agreed at the start of the engagement.
- Client data, code, and infrastructure details are used only for the purposes of the engagement, never repurposed for other clients or shared externally.

- **Retention:** engagement materials are kept for 12 months after the engagement ends, unless a different period is agreed with the client, after which they are deleted.
- On request or at engagement close, client data and credentials are returned or securely deleted, with written confirmation available on request.

04 Access Control and Identity Management

- Access to client systems is requested on a least-privilege, time-boxed basis, scoped to the current engagement.
- Multi-factor authentication is enabled on all accounts used to access client environments.
- Credentials are never shared across clients or reused between engagements.
- Access is revoked at the end of the engagement, or sooner if scope changes.
- Where a client provides SSO, VPN, or bastion-host access, we work through that infrastructure rather than standing credentials of our own.

05 Devices, Workstations and Backups

Primary workstations

Work is primarily performed on Mac M4 and M1 laptops with full-disk encryption enabled, complemented by Ubuntu and Windows 11 virtual machines, or bare-metal machines where a task requires it. All devices used for client work are kept current on operating system and security patches.

Client-provided or client-required machines

Where a client's security policy requires it, or where a specific engagement calls for it, we work directly from client-provided machines instead of our own equipment.

Backups

Engagement materials are backed up to secured cloud storage on AWS and Google Drive, under access controls consistent with the rest of our practice. No client data is stored on personal or unmanaged storage outside these channels.

06 Cloud Infrastructure Practices

- Cloud work follows the principle of least privilege for IAM roles and policies.
- Infrastructure changes are made through version-controlled, auditable processes (infrastructure as code) wherever practical.

- Some changes are made manually, either because that reflects the client's own operating process and engagement timeline, or because the operation itself is not readily automated, for example domain verification or external SSL certificate issuance. These are documented as part of the engagement record regardless of method.
- Recommendations follow the pillars of the AWS Well-Architected Framework (operational excellence, security, reliability, performance efficiency, and cost optimization), adapted to the equivalent frameworks of other cloud providers where relevant.
- Cost and security are treated as linked concerns: misconfigured resources are flagged as both a cost and a security risk during audits.

07 Software Development Practices

- Code is written with secure defaults: input validation, parameterized queries, and secrets kept out of source control.
- Dependencies are tracked and reviewed for known vulnerabilities.
- Code review is applied before merge on any engagement involving more than one developer.
- Secrets and credentials are managed through a secrets manager or environment-level injection, never committed to a repository.

08 Encryption and Key Management

- Data in transit is encrypted using TLS.
- Data at rest is encrypted using provider-native encryption (for example, EBS, RDS, and S3 encryption on AWS, or the equivalent on other providers).
- AWS KMS is used to manage encryption keys on engagements hosted on AWS.
- Local device storage is encrypted at the disk level on all machines used for client work.
- Credentials are stored in a password manager rather than in plain text. Where a client requires the use of their own password manager for shared credentials, we work within that tool instead of our own.

09 Tools, Subprocessors and AI Assistants

We disclose any tool or subcontractor with access to client data as part of the Statement of Work. The tools below are the ones that may, depending on the engagement, come into contact with client data, code, or credentials.

General tools

GitHub Pro · Visual Studio Code · Google Workspace · Insomnia · Slack · Obsidian · Google Chrome · Brave · Safari

Credential management

1Password · KeeWeb

Or a client-provided password manager, where required by the client's own policy.

AI assistants

We use AI coding and productivity assistants as part of normal engagement work. Their use follows the same access boundaries as any other tool: scoped to what the engagement requires, and disclosed in the Statement of Work where an engagement's sensitivity warrants a specific discussion of AI tool usage.

Primary	Claude Code, Claude (desktop and web app), Codex (ChatGPT app)
Secondary	Cursor, Gemini, Antigravity

> For engagements with specific restrictions on AI tool usage, data residency, or model training opt-outs, tell us at the start of the engagement and we will scope tool use accordingly. This is a standard part of our SOW discussion.

10 Incident Response

- In the event of a suspected security incident involving client data or systems, we notify the client within 24 hours of discovery.
- We cooperate fully with the client's own incident response process, including providing logs, timelines, and access records relevant to the incident.
- Access believed to be compromised is revoked immediately as a containment step, ahead of full investigation.

11 Audit Methodology

Our audits combine a technical review with a business-strategy review, on the view that a technically sound recommendation that ignores cost, timeline, or organizational reality is not a useful one.

Technical axis

The technical review is structured around the pillars of the AWS Well-Architected Framework: operational excellence, security, reliability, performance efficiency, and cost optimization. Each pillar is scored against the client's current architecture, with findings ranked by risk and effort to remediate.

Business axis

Alongside the technical review, we assess the business dimension of the technology decisions in scope, drawing on common technical due-diligence practice:

- **Total cost of ownership:** not just infrastructure spend, but the ongoing engineering time a given architecture demands.
- **Alignment with strategy:** whether the current technical direction supports the client's actual growth plans, or was inherited from a different set of priorities.
- **Build versus buy:** where custom-built systems are absorbing effort better spent on differentiated work.
- **Organizational and key-person risk:** how dependent the system is on a small number of people, and what that means for continuity.

The result is a prioritized roadmap that a client's team can act on, rather than a compliance checklist alone.

12 Confidentiality and Legal

- All engagements are covered by a mutual NDA and confidentiality terms set out in the Statement of Work.
- Our standard contracts are governed by the laws of British Columbia, Canada. We are open to contracting under the client's jurisdiction where that is required by the client's own policy.
- References and summaries of past engagements are available on request, redacted as needed for confidentiality.

13 Business Continuity

Blobb is built around two founders, Muriel Marc and Xavier Raffin, with complementary skills and deliberate overlap in some areas so that either can step in on the other's work. We are direct about the limits of this: if one founder became unavailable, business continuity would be difficult for a two-person practice, and we do not represent otherwise.

To reduce that risk in practice, we maintain clear engagement documentation as work progresses rather than after the fact, share credentials and access between founders so neither is a single point of failure for client access, and organize engagement resources (repositories, notes, credentials, contacts) so a transition, if needed, is as smooth as possible. We have also brought on additional staff for larger engagements when the

work called for it, as with a past engagement for Canal+, and would do so again where continuity or capacity requires it.

14 Security Contact

For questions beyond this document, to request a signed copy, or to complete a client-specific security questionnaire, contact:

Security point of contact
Xavier Raffin
xavier.raffin@blobb.ca

END OF DOCUMENT