TECHTEGRITY LLC

Security Practices Statement

Techtegrity LLC — OpenClaw Concierge

This document outlines the security practices employed by Techtegrity LLC ("Service Provider") during the setup and maintenance of OpenClaw AI assistant instances. The undersigned client ("Client") acknowledges review and understanding of these practices.

1. Data Handling

All client credentials, API keys, and sensitive data are transmitted via encrypted channels (TLS 1.2+). Credentials are never stored in plaintext. Where temporary storage is required during setup, industry-standard encryption is used and data is purged upon completion.

2. Access Control

Access to client systems is limited to the Service Provider principal (Chris Borgia) and is performed exclusively from secured devices with full-disk encryption, up-to-date operating systems, and active firewall protection.

No subcontractors or third parties are granted access to client systems or credentials without explicit written consent.

3. Local-First Architecture

OpenClaw is designed to run locally on the client's own hardware. Client data, conversations, and credentials remain on the client's machine and are not transmitted to the Service Provider's servers or any third-party cloud infrastructure, except where explicitly configured by the client (e.g., third-party API integrations).

4. Third-Party Integrations

Where the client requests integration with third-party services (e.g., Gmail, GitHub, Slack), the Service Provider configures these using official APIs and OAuth flows where available. The Client acknowledges that data shared with third-party services is subject to those services' own privacy policies and terms.

5. Incident Response

In the event of a suspected security incident affecting client data, the Service Provider will: (a) notify the Client within 24 hours of discovery; (b) investigate and remediate the incident promptly; (c) provide a written summary of the incident, its impact, and corrective actions taken.

6. Client Responsibilities

The Client is responsible for: (a) maintaining the physical and network security of the machine running OpenClaw; (b) keeping the operating system and software up to date; (c) safeguarding any credentials and API keys after handoff; (d) notifying the Service Provider if they suspect unauthorized access to their OpenClaw instance.

Client Acknowledgment

Name: _____

Title: _____

Company: _____

Signature: _____

Date: _____