EncryptaGuard LLC: Standard Security Profile

Version: 1.4 (January 2026)
Classification: Business Reference / Compliance Documentation

1. Core Security Philosophy

EncryptaGuard LLC utilizes an **In-Line Hardening** architecture to provide enterprise-grade network protection for small business environments. Our methodology prioritizes **Traffic Integrity** and **Managed Resilience**, ensuring that critical business operations—such as credit card processing and internal data streams—are physically secured and encrypted at the network edge before reaching the public internet.

2. Managed Threat Intelligence

These categories are active fleet-wide and represent our baseline defense against global cyber vulnerabilities.

PROTECTION CATEGORY	TECHNICAL PURPOSE	BUSINESS VALUE
Traffic Hardening	Encrypts outbound traffic and blocks malicious DNS requests.	Privacy & Compliance Shield
Malware/C2 Block	Halts communication with Command & Control botnets.	Ransomware Prevention
Phishing Defense	Blocks known fraudulent login pages and scam domains.	Credential Protection
Tracking Cloak	Eliminates "invisible" third-party background trackers.	Up to 3x Faster Page Loads

3. The "Resilient Network" Filter

To maintain **Performance Integrity**, the EncryptaGuard Standard Profile enforces a policy designed to protect professional production environments from high-risk or non-business-critical data consumption.

A. High-Risk Web Categories

We mitigate risk by restricting access to categories that historically serve as vectors for malware or legal liability:

- **Gambling & Betting:** Prevents exposure to high-risk financial platforms.

- **Adult Content:** Enforces professional environment standards at the hardware level.
- **Illegal/Copyrighted Material:** Protects the business from ISP-level penalties due to customer activity.

B. Privacy & Performance Optimization

- **DNS-over-HTTPS (DoH):** All DNS requests are wrapped in an encrypted tunnel, preventing ISP-level snooping and data harvesting.
- **Tracker Elimination:** We block thousands of background requests from telemetry services, reclaiming up to 40% of wasted bandwidth and significantly reducing Time-to-Content (TTC).

---

4. Fleet-Wide Integrity & Zero-Touch Management

EncryptaGuard LLC maintains a **Standardized Global Policy** across all managed nodes to ensure uniform protection.

- **Automated Threat Updates:** New vulnerabilities are blocked across the entire fleet in real-time without user intervention.
- **Zero-Touch Provisioning:** Nodes arrive pre-hardened; the EncryptaGuard Master-Replica architecture handles all security patches and performance optimizations remotely via secure outbound-only tunnels.
- **No Manual Configuration Gaps:** By standardizing the policy, we eliminate the human errors associated with traditional local network management.

---

5. Privacy Commitment

EncryptaGuard LLC **does not log individual browsing history**. Our nodes process requests locally on-premise to determine if they match a security blocklist. We do not sell data, store PII (Personally Identifiable Information), or maintain records of specific destination traffic for your business.

Managed Resilience by EncryptaGuard LLC *Hardened Infrastructure. Privacy Focused. Remotely Managed.*