EncryptaGuard: Standard Security Profile & Blocklist Reference

Version: 1.2 (December 2025) **Classification:** Public / Client Reference

1. Core Security Logic

EncryptaGuard utilizes a "Clean Pipe" methodology. Unlike residential filters, our nodes prioritize **Business Continuity** and **Network Sovereignty**. We block traffic at the DNS level before it enters your hardware, preventing malware from ever making a "call home."

2. Global Threat Protection (Always Active)

These categories are non-negotiable and updated in real-time across the EncryptaGuard fleet to prevent known exploits.

Category	Source / List	Why We Block It
AdGuard DNS	AdGuard DNS Filter	Blocks primary ad-serving domains and known tracking scripts.
Anti-Adblock	Adblock Warning Removal	Ensures web pages load correctly without aggressive anti-adblock popups.
Malware/C2	Malicious URL Blocklist	Prevents ransomware and Command & Control servers from communicating.
Phishing	Scam/Phishing Protection	Protects staff from credential theft and "look-alike" login pages.

3. The "Business Lane" Filter (Productivity)

To ensure your bandwidth is used for work, the following high-latency distraction and high-risk categories are restricted on the **Standard Profile**.

A. High-Distraction Services & Social Media

The following specific services are restricted to reclaim staff productivity:

- **Social:** TikTok, Facebook, Instagram, Snapchat, Reddit, X (Twitter).
- **Entertainment:** Twitch, Disney+, Hulu, Netflix, YouTube.
- **Gaming:** Roblox, Steam, Origin, Epic Games.
- **Communications:** Discord, Telegram (Non-business messaging).

B. High-Risk Category Blocks

Beyond specific apps, we block entire categories of high-risk web traffic:

- **Gambling:** Prevents access to betting sites and online casinos.
- **Dating:** Blocks Tinder, Bumble, and other non-work social networking.
- **Pornography:** Enforces professional environment standards at the hardware level.

C. Privacy-Invasive Trackers

- **Services:** Google Analytics, DoubleClick, Facebook Pixel.
- **Rationale:** These "invisible" requests account for 20-40% of page load time. Blocking them makes your browsing feel 2-3x faster.

---

4. Fleet-Wide Integrity

To maintain a high security posture and ensure consistent performance across all managed locations, EncryptaGuard enforces a **Standardized Policy**.

- **Uniform Protection:** Every node receives identical, hardened security updates simultaneously.
- **Policy Adjustments:** If a legitimate business tool is identified as a false positive, it is reviewed by our architects and whitelisted fleet-wide to ensure global reliability.
- **No Individual Exceptions:** This model prevents security gaps caused by manual configuration errors at individual sites.

---

5. Privacy Commitment

EncryptaGuard **does not log your specific browsing history**. Our nodes only see that a request was made and whether it matched a blocklist. We do not sell data, and we do not store personal identifiable information (PII) regarding "who went where."

Managed Security by EncryptaGuard *Hardened Infrastructure for Small Business.*