VaultGuard - The Digital Inspector

Tool #2 of the Builder's Permit System

This document outlines the foundational security scan and checklist protocol for each Builder's Permit session.

VaultGuard is a tier-integrated inspection system designed to safeguard user environments and data integrity prior to tool engagement.

CORE CHECKLIST:

- [ ] User identity verified (name, tier, license)
- [ ] Local machine status: secure, no known compromise
- [ ] Active VPN connection confirmed (recommended: NordVPN, ProtonVPN)
- [ ] AI session confirmed with Builder's Permit credentials
- [ ] Repository permissions set to PRIVATE unless stated otherwise
- [ ] License and IP lock confirmation step passed
- [ ] GitHub repo: license, README, and release tags intact
- [ ] No conflicting local software or executables
- [ ] VaultGuard checksum or hash ID verified
- [ ] (Optional) Pre-engagement system backup created

AUTOMATED TRIGGERS (if integrated):

- GitHub Action runs VaultGuard on repo open
- Auto-check for unauthorized forks or commits
- Scan for foreign IP access to secure files
- Send alert to RMG Owner if violated

FINAL NOTE:

VaultGuard is a pre-toolbelt gatekeeper for the Builder's Permit system and must be run prior to initiating Tool #3 or higher.

Unauthorized bypass or disengagement will terminate access.