Security Protocols Policy

Virtual Antidote Solutions LLC
Security Protocols Policy
Effective Date: May 28, 2025

Purpose

The purpose of this Security Protocols Policy is to outline the technical, physical, and administrative measures taken by Virtual Antidote Solutions LLC to ensure the confidentiality, integrity, and availability of client and internal data.

Scope

This policy applies to all systems, tools, devices, and workflows used by Virtual Antidote Solutions LLC in the course of client work, internal operations, and subcontracted tasks. It also governs any client-facing websites, embedded forms, and intake processes where data is collected, stored, or exchanged.

Client Responsibility

While Virtual Antidote Solutions LLC takes all reasonable precautions to safeguard client data, clients are responsible for maintaining secure access to shared platforms, passwords, or files on their end. Clients who choose to use unencrypted communication methods or third-party tools outside of those recommended by Virtual Antidote Solutions LLC do so at their own risk.

Technical Safeguards

- Data Encryption
  - All data is encrypted in transit using TLS 1.2+ (HTTPS)
  - Files are stored on platforms that use AES-256 encryption at rest (e.g., **Microsoft OneDrive for Business**)

- Secure Communication
  - Standard client communication is conducted via **Microsoft 365 email services**, which use **TLS encryption in transit** and secure Microsoft data centers for storage at rest

  - For clients who prefer additional protection, **end-to-end encrypted messaging via Signal** is available

  - Upon request, Virtual Antidote Solutions can also explore **advanced email encryption options** (such as S/MIME or PGP), depending on client needs and compatibility

- Device Protection

- All work devices are password-protected and encrypted at the disk level using platform-native tools:
    - **BitLocker** for Windows devices

Automatic screen locks are enabled after short periods of inactivity to reduce the risk of unauthorized access

Antivirus and anti-malware protection (currently using **IDrive Inc.**) is actively maintained and kept up to date to defend against threats and vulnerabilities

- Two-Factor Authentication (2FA)
    - 2FA is enabled on all platforms containing client data, including **Microsoft 365**, **IDrive**, and any third-party project tools

- Software Maintenance
    - Operating systems, browsers, and critical software are updated regularly to patch security vulnerabilities

---

Administrative Controls

- Access Restriction
    - Only Rosemary Damato and pre-approved subcontractors (bound by NDA) have access to client files or credentials
    - Role-based access is applied wherever tools support it
- Audit and Access Logs
    - Access to cloud storage, project tools, and sensitive platforms is logged through built-in audit trails (e.g., **Microsoft OneDrive** activity logs, **Bitdefender** alert history).
    - Logs are reviewed on a **quarterly basis** during scheduled security audits to detect unusual patterns, unauthorized access attempts, or permission changes.
    - Any suspicious activity is investigated immediately, documented, and resolved according to incident response protocols.
- Confidentiality Agreements
    - Subcontractors and collaborators are required to sign NDAs before being granted access to client information
- Secure Password Practices
    - Passwords are stored in a secure password manager

    - Unique, complex passwords are used for all platforms
    - Passwords for client platforms may be stored temporarily during active engagements using a secure, encrypted password manager. This access is limited to the founder and governed by strict confidentiality. Clients may request that no passwords be stored or may ask for deletion at any time. Passwords are deleted upon project completion unless retention is otherwise agreed to in writing.

Physical Security

- Work is performed on business-owned or dedicated secure devices
- Devices are never left unattended in public spaces
- Files are never printed or stored physically unless explicitly authorized by the client
- Encrypted external storage drives are kept in a locked, secure location

---

Backup & Recovery

- All active work files are backed up continuously using **IDrive Inc**
- **Microsoft OneDrive** is used for real-time collaboration and secondary redundancy
- In the event of a system failure or breach, restoration can be initiated within 24 hours

---

Data Deletion & Wiping

- Upon request or at the end of a retention period, files are deleted using an industry-standard secure deletion tool (e.g., Eraser or BleachBit)
- Deleted files are overwritten to prevent recovery and logged for audit purposes

---

Incident Response Plan

- Clients will be notified of any confirmed data breach involving their data within 72 hours.
- The notification will include:
    - A summary of the breach
    - What data was affected
    - Steps taken to mitigate the issue
    - Any recommended actions for the client

Legal & Regulatory Alignment
Virtual Antidote Solutions LLC strives to meet key requirements outlined by major data protection regulations, including:

- The **General Data Protection Regulation (GDPR)** for clients based in or working with the EU
- The **California Consumer Privacy Act (CCPA)** for California residents and businesses

This Security Protocols Policy reflects best practices for U.S.-based solo consultancies and aligns with applicable federal and state privacy expectations.

Custom contractual terms (e.g., data processing agreements or regional clauses) can be added upon client request to strengthen compliance and trust.

Custom data processing agreements (DPAs) or regional compliance clauses may be provided upon request to support institutional, international, or grant-funded projects.

Contact

Questions about this policy may be directed to:

Rosemary Damato, Founder
Virtual Antidote Solutions LLC
Email: info@VirtualAntidote.com
Phone: 201-862-7899

Response time: Within 2 business days

Version 1.0 — Last reviewed: July 5, 2025
This policy is reviewed annually and updated as needed to reflect current practices.

Policy Review Schedule

This Security Protocols Policy is reviewed annually or in response to:

- Significant changes in client base, platforms, or service offerings
- Updates to relevant privacy laws (e.g., GDPR, CCPA)
- New risks or security incidents that require policy adjustment

The most recent version of this policy will always reflect current best practices and the tools in use at Virtual Antidote Solutions LLC.
Next scheduled review: July 2026