# Methodology IT Security Practices

**Effective May 22, 2026. This document supersedes and replaces all prior versions.**

This document describes the security practices of Methodology IT ("Provider") in delivering its services. It is referenced from the Data Processing Agreement and the Service Attachments and serves as Provider's current Security Practices document. Provider may update this document from time to time, provided that no update materially decreases the level of protection Provider maintains.

This document is the customer-facing summary of Provider's internal security program. Detailed internal controls, runbooks, and configurations are Provider's Confidential Information and are not published.

## 1. Security program overview

Provider maintains a comprehensive written information security program with administrative, technical, and physical safeguards. The program is designed to satisfy applicable obligations under the New York SHIELD Act, the FTC Safeguards Rule (GLBA), the HIPAA Security Rule (where applicable), state cybersecurity statutes, and the security obligations set forth in the Data Processing Agreement.

The program is reviewed at least annually and is updated in response to changes in technology, threats, regulatory requirements, and Provider's business operations.

## 2. Security governance

- **Assigned responsibility.** Provider has designated a security lead with overall responsibility for the security program.
- **Policies and procedures.** Provider maintains written policies covering acceptable use, access control, data classification, incident response, business continuity, vendor management, and other operational areas.
- **Annual review.** Policies are reviewed and updated at least annually.
- **Training.** Provider personnel receive security awareness training at onboarding and on a recurring basis.

## 3. Personnel security

- **Background checks** are performed on personnel with access to Client Data, where permitted by applicable law.
- **Confidentiality obligations.** All personnel are bound by written confidentiality agreements covering Client Data and Provider Confidential Information.
- **Role-based access.** Personnel are granted access to Client environments and Provider systems based on role and on the principle of least privilege.
- **Termination procedures.** Access is removed promptly upon termination of employment or change in role.

## 4. Access control

- **Multi-factor authentication** is enforced for all Provider personnel accessing Provider systems and Client environments.
- **Privileged access** to Client environments is administered through dedicated privileged accounts separate from personnel's day-to-day accounts.
- **Just-in-time access** is used where supported by the platform.
- **Access reviews** are performed on a defined cadence.
- **Conditional access** policies enforce device-health, geographic, and risk-based controls on Provider personnel access.

## 5. Endpoint security

- **Provider laptops and workstations** are managed via Provider's RMM and EDR platforms.
- **Disk encryption** is enabled by default on Provider devices.
- **Endpoint detection and response** is deployed on Provider devices and monitored by Provider's 24×7 SOC partner.
- **Operating systems and applications** are kept on supported versions and patched according to Provider's published Patching Policy.

## 6. Network and infrastructure security

- **Segmentation.** Provider's internal network is segmented to limit lateral movement.
- **Firewall and intrusion detection** are deployed at network boundaries.
- **VPN** is required for personnel access to Provider's internal management infrastructure.

- **Logging and monitoring** of network traffic, authentication, and privileged actions is in place with retention aligned to applicable requirements.

## 7. Data protection

- **Encryption in transit.** TLS 1.2 or higher is used for all data transmission across public networks. Internal traffic uses TLS where supported.
- **Encryption at rest.** Where the underlying platform supports it, Client Data managed by Provider is encrypted at rest using industry-standard encryption (AES-256 or equivalent).
- **Data segregation.** Client Data is logically segregated by Client across Provider's tooling and Third-Party Services Providers.
- **Data classification.** Provider classifies data handled by personnel; Client Data and regulated data receive the most stringent handling.
- **Data minimization.** Provider collects and retains Client Data only as needed to deliver the Services.
- **Secure disposal.** Storage media containing Client Data is securely wiped or destroyed at end of life. Vendor-managed storage destruction follows the underlying vendor's certified disposal procedures.

## 8. Vulnerability management

- **Vulnerability scanning** of Provider infrastructure is performed on a recurring basis.
- **Patch management** follows Provider's published Patching Policy.
- **Penetration testing** is performed periodically by qualified third parties.
- **Bug reports** from external researchers may be submitted to security@methodologyit.tech and are reviewed in good faith.

## 9. Incident response

- **Incident response plan.** Provider maintains a written incident response plan covering detection, classification, containment, eradication, recovery, and post-incident review.
- **24×7 detection.** Provider's third-party Managed Detection and Response provider monitors managed environments around the clock.
- **Escalation.** Confirmed incidents are escalated according to severity, with notification to affected Clients in accordance with the breach-notification timing in the Data Processing Agreement (within 72 hours of confirmation).

- **Cooperation.** Provider cooperates in good faith with Clients, regulators, and law enforcement as required during incident response.

## 10. Business continuity and disaster recovery

- **Provider operations** include redundant systems and documented failover procedures for critical Provider infrastructure.
- **Backup of Provider's internal systems** is performed on a defined cadence with periodic restore testing.
- **Personnel readiness.** Provider maintains the ability for personnel to deliver Services remotely in the event of facility-level disruption.
- **Annual review.** The business continuity and disaster recovery plan is reviewed at least annually.

## 11. Vendor and sub-processor management

- **Sub-processors** are identified in the Schedule of Third-Party Services and bound by contractual obligations substantially similar to those in the Data Processing Agreement.
- **Vendor risk assessment.** Provider performs initial risk assessment of material vendors prior to engagement and reviews material vendors on a periodic basis.
- **Vendor security review.** Provider reviews available security artifacts from material vendors (SOC 2 reports, ISO 27001 certifications, security questionnaire responses) on a periodic basis.

## 12. Physical security

- **Provider offices** maintain access controls limiting entry to authorized personnel.
- **Equipment storage.** Provider equipment in transit or in storage is handled in accordance with internal procedures designed to prevent unauthorized access.
- **Visitor management.** Visitors to Provider offices are escorted and logged.

## 13. Change management

- **Change control** procedures govern changes to Provider production infrastructure and Client environments under Provider's management.
- **Documentation.** Changes are documented, reviewed, and approved according to risk.
- **Testing.** Significant changes are tested before deployment to production environments where feasible.

## 14. Continuous improvement

Provider monitors developments in cybersecurity, threat intelligence, regulatory requirements, and industry best practices, and adjusts the security program accordingly.

---

## Reports and attestations

Provider may make available, on request and under appropriate confidentiality protections, the following:

- This Security Practices document (publicly available)
- Provider's annual cybersecurity certifications and assessments (where applicable)
- Vendor-provided artifacts for material sub-processors where Provider is authorized to share them
- Responses to reasonable security questionnaires from Clients with active engagements

Provider may charge for substantial time spent responding to security questionnaires beyond standard scope per the Master Services Agreement.

---

Provider may update this Security Practices document from time to time. Material changes will be published on Provider's website with reasonable notice.