

Data Security Policy

RevenuePoint Inc. · *Last reviewed: August 2026*

Our Commitment

RevenuePoint treats client data as a trust, not a resource. We apply consistent security practices designed to protect your data from unauthorized access, disclosure, loss, or misuse. This policy summarizes the standards we hold ourselves to across every engagement.

Scope

This policy applies to all client data RevenuePoint accesses, processes, transmits, or stores in the course of delivering consulting, implementation, managed services, or platform services — regardless of the underlying system or environment. That includes work we do inside client systems and data held in the RevenuePoint Platform, our hosted data and analytics service.

Guiding Principles

- **Least privilege.** We request only the access we need to perform contracted work, and no more.
- **Data minimization.** We avoid extracting, copying, or storing client data unless it's necessary for the engagement.
- **Defense in depth.** Multiple overlapping controls so that no single failure exposes client data.
- **Transparency.** We document what we access, when, and why, and we'll share that record on request.

Access & Authentication

- Work is performed using **named user accounts** provisioned by the client. We do not share credentials between consultants or across engagements.
- **Multi-factor authentication (MFA)** is required on every account with access to client systems.
- We prefer **single sign-on (SSO)** where the client supports it, so access can be centrally managed and revoked.
- **Just-in-time access** is requested when feasible — elevated permissions are granted for specific work and removed afterward.
- Access is reviewed periodically and at minimum at each engagement milestone.

Credential & Secret Management

- All credentials, API keys, and secrets are stored in an enterprise password manager with MFA-protected access.
- Credentials are never transmitted by email, chat, SMS, or stored in plain text in documents, tickets, or code.
- API keys and service credentials are scoped to the least privilege required and rotated on a defined schedule or upon any suspected exposure.
- We never commit secrets to version control. Git repositories are scanned for accidental credential exposure.

Endpoint Security

Every device used to access client systems is:

- Protected by full-disk encryption
- Running a supported, patched operating system with automatic security updates enabled
- Protected by endpoint security software (antivirus / endpoint detection)
- Configured with automatic screen lock after a short period of inactivity
- Capable of remote wipe in the event of loss or theft

Data Handling

- All data in transit is protected by TLS 1.2 or higher. We do not access client systems over unencrypted connections.
- Data at rest is encrypted using industry-standard algorithms on any device or service used to store client data.
- Client data is not stored on personal devices and is segregated from data belonging to other clients.
- When extracts or exports are necessary (e.g., for migration or analysis), they are stored only in approved encrypted locations and deleted promptly when no longer needed.
- Testing and development work uses sandbox environments or scrubbed/synthetic data wherever feasible, rather than production data.

Network Security

- Work involving sensitive client data is performed on trusted, secured networks.
- Untrusted public networks (e.g., open Wi-Fi) are not used for client work without an active VPN connection.
- Home and office networks used for client work are protected by modern WPA2/WPA3 encryption and current router firmware.

The RevenuePoint Platform

The RevenuePoint Platform brings a client's data from their source systems into a managed data warehouse, and delivers it back through dashboards, reports, and AI-assisted tools. Everything above applies to the platform; it adds the following.

- **Hosting.** The platform runs on a major cloud provider's infrastructure in the United States. Databases are not reachable from the internet, web traffic is accepted only over HTTPS through a protected edge with a web application firewall, and administrative access uses audited sessions rather than open remote login.
- **Encryption.** Data is encrypted in transit with TLS 1.2 or higher, and the database refuses unencrypted connections. Databases, disks, and backups are encrypted at rest with managed keys that rotate automatically.
- **Client separation.** Each client's data sits in its own warehouse schema, read through credentials that can see only that client. Within the application, database row-level security keeps every user to their own organization's records.
- **Sign-in and roles.** Every user signs in with their own named account. Roles decide who can view, approve, or administer, and access can be revoked at any time. Multi-factor authentication (authenticator app, security key, or passkey) is available to every user and can be required for a client's whole organization on request.
- **Source connections.** Connections to client systems use the narrowest access each system allows: read-only wherever possible, with write access only where a client has asked us to sync data back (for example, recording payments in their CRM). Connection credentials are held in an encrypted secrets store, never in code, and clients can revoke them from their own systems at any time.
- **Backups.** The database supports point-in-time recovery, and encrypted daily backups are copied to a separate, locked account.
- **Logging.** Administrative and data-changing actions in the platform are recorded in an audit log. Activity in our cloud accounts is written to tamper-evident storage that is locked against deletion, and automated threat detection watches for unusual behavior.

AI features

The platform's AI features — the Otto assistant, and a connector that lets a client's own AI tools query their data — see only what the signed-in user can already see, through the same client separation as dashboards and reports. Data reaches an AI model only when a user asks a question; nothing is sent in the background. The connector is read-only, available only to users who have been given access to it, and that access can be revoked at any time.

Confidentiality

- All engagements are governed by mutual non-disclosure agreements (NDAs) unless the client waives this requirement.

- Client data is not discussed, displayed, or referenced outside the scope of the engagement, including in marketing, case studies, or public communication, without prior written consent.
- We maintain logical separation between clients in all internal systems, documentation, and tooling.

Subcontractors & Third Parties

- Any subcontractor or third-party tool with access to client data is vetted for security posture before engagement.
- Subcontractors are bound to security obligations equivalent to those in this policy via written agreement.
- Clients are informed of any subcontractor relationships that involve access to their data.
- The RevenuePoint Platform relies on a small number of established cloud infrastructure and AI providers. A current list is available on request.

Incident Response

In the event of a confirmed or suspected security incident affecting client data, RevenuePoint will:

1. **Contain** the incident immediately and preserve relevant evidence.
2. **Notify** the affected client within a reasonable timeframe, or sooner if contractually required.
3. **Investigate** to determine root cause, scope, and impact.
4. **Remediate** the underlying issue and document the actions taken.
5. **Review** to identify and apply lessons learned.

Clients receive a written summary of the incident, our response, and any recommended actions on their side.

Data Retention & Disposal

- We retain client data only as long as necessary to perform contracted work or meet legal obligations.
- At engagement conclusion, client data in our possession is returned or securely destroyed upon request, including any backups, working copies, and derived artifacts.
- When a platform subscription ends, we can provide an export of the client's data, then delete their platform data, user accounts, and source connections. Backups and logs expire on their normal schedule.
- Verifiable destruction methods are used for both digital and any physical media.

Audit & Monitoring

- We log access and administrative actions in systems that support logging, and we make those logs available to the client on request.

- Anomalous activity (unexpected logins, permission changes, mass exports) is investigated promptly.
- We support clients who want to perform their own access reviews or audits of our work in their systems.

Engagement Lifecycle

Phase	Security Practice
Onboarding	Documented access request, least-privilege provisioning, MFA enrollment, NDA in place; least-privilege source connections for platform clients
Active engagement	Ongoing access review, secure handling of all artifacts, change tracking
Offboarding	Prompt access revocation, platform accounts and source connections removed, return or destruction of data, written confirmation

Continuous Improvement

- This policy is reviewed and updated at least annually, and whenever material changes to our tools, practices, or the threat landscape warrant it.
- We track emerging best practices and adopt them when they materially improve client data protection.
- We welcome client-specific security requirements and will document any deviations or additions to this baseline in writing.

Responsible Disclosure

Security issues can be reported to security@revenuepoint.com. Full details, scope, and our PGP key are published at revenuepoint.com/security.

Questions

Clients and prospects with security questions, custom requirements, or audit requests are welcome to contact us directly. We're happy to discuss how this policy applies to your specific environment and to accommodate stricter requirements where your industry, contractual, or internal standards demand them.