Switch Labs LC — Information Security Policy

Policy	Information Security Policy
Organization	Switch Labs LC
System in scope	Metro2 — credit data furnishing platform (metro2.switchlabs.dev)
Version	5.2
Initialization date	September 20, 2022
Update date	March 10, 2026
Classification	Public — published for customers, partners, and third-party security reviewers
Review cadence	At least annually and upon material change

Table of Contents

1. Purpose

This Information Security Policy establishes the requirements Switch Labs LC ("Switch Labs") applies to protect the confidentiality, integrity, and availability of the data processed by the Metro2 platform, including consumer credit information handled on behalf of data furnishers. It defines the mandatory controls governing Switch Labs' systems, personnel, and vendors, and serves as the authoritative statement of Switch Labs' information security program. This policy is published for customers, partners, and third-party security reviewers as evidence of that program in support of their security and risk assessments.

2. Scope

This policy applies to:

- Systems: the Metro2 production application, its data platform, the file-generation and validation pipeline, the bureau file-transmission systems, and all administrative systems used to operate them.
- Data: all consumer and customer data processed by Metro2, including consumer identifiers (including Social Security Numbers), tradeline/account data, generated Metro 2 files, validation results, bureau responses, dispute records, and consent/authorization records.
- Personnel: all Switch Labs employees, contractors, and any other individuals granted access to systems or data in scope.

- Vendors: all sub-processors and service providers that store, process, or transmit in-scope data on Switch Labs' behalf.

Switch Labs acts as the technical service provider (processor) for its customers; the customer remains the furnisher of record and retains responsibility for the accuracy and lawful basis of the source data it submits.

3. Roles and Responsibilities

- Founder/CEO (Policy Owner and Executive Security Authority). Owns and approves this policy and the information security program; holds final accountability and decision-making authority for security operations, access approvals, vendor oversight, incident response, and compliance; reviews and approves exceptions; and ensures the policy is reviewed on cadence.
- All personnel with access to in-scope systems or data. Must comply with this policy and its supporting procedures, complete required security training, protect credentials and Restricted data, use only approved systems and devices, and report suspected security incidents promptly.
- Vendors and sub-processors. Must meet the security obligations set out in Section 5.14 and their agreements with Switch Labs.

4. Hosting and Infrastructure

Metro2 is a Next.js application hosted on Vercel, using a Supabase-managed PostgreSQL database and object storage running on Amazon Web Services in the US East (`us-east-1`) region. All production data is processed and stored in the United States; there is no offshore processing or storage.

Security of the service is shared across three parties:

Layer	Responsible party
Physical infrastructure, data-center security, hypervisor, managed-service internals	Cloud providers (Vercel, Supabase, AWS — each SOC 2 Type II)
Application, configuration, access, data handling, transmission, monitoring, incident response	Switch Labs
Source-data accuracy, authorization to furnish, management of the customer's own users	Furnisher customer

Switch Labs inherits and relies on the physical, environmental, and infrastructure controls of its cloud providers, validated through review of the providers' SOC 2 Type II reports, and is directly responsible for all controls it configures and operates on top of that infrastructure.

5. Policy

5.1 Information Security Governance

Switch Labs maintains a documented information security program, owned and approved by the Founder/CEO, with control families aligned to ISO/IEC 27002 and the SOC 2 Trust Services Criteria. The program is expressed through written, version-controlled policies and procedures, including this policy, the Incident Response and Data Breach Policy, the Business Continuity and Disaster Recovery Plan, the Change Management process, the Vendor/Third-Party Risk process, and the FCRA Policies and Procedures. Policies are reviewed at least annually and upon material change. Switch Labs performs periodic risk identification across furnishing operations, data handling, technology, and vendors, and tracks identified risks to remediation.

5.2 Data Classification and Handling

Switch Labs classifies data as Restricted (e.g., Social Security Numbers, full tradeline data, generated Metro 2 files, bureau credentials, cryptographic keys), Confidential (e.g., customer business data, dispute and consent records), Internal, or Public, and applies controls commensurate with each classification. Restricted and Confidential data is processed only for the authorized purposes of furnishing, validation, dispute management, compliance, and recordkeeping. Data minimization is required: sensitive identifiers are collected and retained only as necessary, and Restricted values are masked by default in application views, exports, support tooling, logs, and error reporting. Full-value access to a Restricted identifier requires explicit authorization and generates an audit event.

5.3 Access Control and Authentication

- Access to production systems and Restricted data is granted only on the basis of least privilege and documented business need, and only after approval by the Founder/CEO.
- Multi-factor authentication is required on all administrative consoles that hold or process in-scope data, including Vercel, Supabase, GitHub, and Google Workspace, and on bureau transfer accounts where supported.
- Programmatic access uses per-company API keys that are hashed at rest and scoped to their owning company, enforced on every request.
- Company-level role-based access control (administrator and user roles) governs access to application functions.
- Privileged access is reviewed on a defined cadence and upon material staffing, vendor, or system change, with dated evidence retained. Access is promptly reduced or revoked when no longer required.
- Shared administrative accounts are not used where individual accounts are available.

5.4 Encryption and Key Management

- All data in transit is encrypted using TLS 1.2 or higher. All data at rest, including backups, is encrypted using AES-256 provided by the data platform.
- Social Security Numbers receive additional application-layer protection beyond platform encryption: sensitive identifiers are tokenized and referenced by token, and stored SSN values are protected with application-layer envelope encryption.
- Encryption keys are managed through a managed key-management service (KMS), held separately from the data they protect, and rotated on a documented schedule.
- Production secrets, service-role credentials, API keys, and bureau credentials are never committed to source control and are managed as restricted operational secrets; stored bureau transfer credentials are encrypted at the application layer.

5.5 Multi-Tenant Data Isolation

Tenant isolation is enforced in depth. PostgreSQL Row-Level Security (RLS) enforces, at the database layer, that each company can access only its own records; this is the authoritative isolation control. Application-layer company scoping on every API key reinforces it. Isolation is validated through automated tests run in the change pipeline. No company may read, modify, or furnish another company's records.

5.6 Secure Development and Change Management

- All changes are managed in version control with peer review and are traceable through commit history and deployment records.
- Automated checks run on change, including dependency vulnerability scanning and secret scanning; type and test checks must pass before release.
- Production Metro 2 files are generated only through the sanctioned production pipeline, never ad-hoc scripts, so that validation, monetary normalization, UTC date handling, audit metadata, and storage are always applied.
- Changes affecting furnishing logic, validation, access control, security, or bureau transmission are tested before release, and production-deployment authority is restricted.
- Restricted production data is not used in non-production environments.

5.7 Vulnerability Management and Penetration Testing

- Software dependencies and code are scanned for vulnerabilities and secrets; findings are prioritized by severity and remediated.
- Internet-facing surfaces are subject to periodic external vulnerability scanning.
- The internet-facing Metro2 application undergoes penetration testing, with findings tracked to remediation and re-tested as appropriate; summary results are available to partners under NDA on request.

- Infrastructure host patching is performed by the underlying SOC 2 Type II providers; application and dependency patches are applied on a risk-prioritized basis.
- Security-sensitive findings are escalated to the Founder/CEO and tracked to closure.

5.8 Secure Bureau Data Transmission

- Metro 2 files are transmitted to consumer reporting agencies over SFTP and each bureau's managed file-transfer facility, with encrypted transport.
- Outbound files are additionally PGP-encrypted at the file level, applied uniformly across bureaus.
- Connections use key-based authentication (RSA-4096) with dedicated, per-bureau, per-furnisher service identities; automated transfers do not use shared or interactive password accounts, and private transfer keys are stored encrypted.
- Bureau host keys are verified (host-key pinning) to prevent interception, and the transfer client is restricted to modern cipher, key-exchange, and MAC algorithms.
- Transmission originates from a dedicated transfer component with a static egress IP, so bureaus requiring IP allow-listing can restrict connections to Switch Labs.
- SSH and PGP keys are rotated on a documented schedule, and every transmission is recorded with its file reference, remote filename, byte count, status, and any errors.

5.9 Logging, Monitoring, and Audit

Switch Labs maintains a field-level audit trail of changes to credit-reporting records (who, when, what) and of access to Restricted data. The generation pipeline records validation results, generated-file metadata, and storage paths; source snapshots, generated files, bureau responses, dispute records, and consent records are retained as substantiation. Application and platform logs are aggregated for troubleshooting, security review, and anomaly detection, with alerting on security-relevant events. Security-relevant audit records are retained in a tamper-evident manner. Material anomalies and data-integrity issues are escalated to the Founder/CEO.

5.10 Endpoint Security

Devices used to access production systems or Restricted data must run full-disk encryption, current operating-system and security updates, anti-malware protection, and authorized software only. Production credentials are handled through a password manager or equivalent, individual accounts are used in place of shared accounts, and administrative access is performed only from devices approved for Switch Labs operational use.

5.11 Network Security

The application is fronted by the provider's global edge network, providing TLS termination and DDoS mitigation. The data platform enforces network-level access controls, and administrative access to it is restricted. The bureau-transfer environment — which holds transfer credentials and key material and performs outbound bureau connections — is logically segmented from the general application surface, with least-privilege paths between trusted and untrusted zones.

5.12 Business Continuity and Disaster Recovery

Switch Labs maintains a written Business Continuity and Disaster Recovery plan that identifies critical services, defines recovery objectives (RTO/RPO), and documents data-protection, recovery sequencing, and rollback/disable controls. Database backups are maintained and encrypted by the data platform and support point-in-time recovery. Recovery procedures are exercised and evidence retained.

5.13 Incident Response and Breach Notification

Switch Labs maintains a written Incident Response and Data Breach Policy defining incident categories, a severity model, the response lifecycle, evidence preservation, notification assessment, and recordkeeping. Incidents affecting consumer data, bureau data, credentials, generated files, or system integrity are escalated to the Founder/CEO. Where an incident affects a bureau's data, Switch Labs notifies the affected bureau within the timeframe required by that bureau's agreement (as short as 24 hours) and notifies affected customers and authorities as required by law and contract. Incidents are investigated to root cause, remediated to closure, and recorded. The incident-response process is exercised through periodic tabletop exercises.

5.14 Vendor and Third-Party Risk Management

Switch Labs uses a small, deliberately limited set of vetted, US-based sub-processors, each maintaining SOC 2 Type II (Appendix A). Before a vendor processes in-scope data, and at least annually thereafter, Switch Labs reviews the vendor's security controls (including its SOC 2 Type II report), grants least-privilege integration access, imposes contractual confidentiality/security obligations where available, and maintains the ability to escalate any vendor incident that could affect consumer data or furnishing accuracy.

5.15 Personnel Security and Training

Personnel with access to Restricted or Confidential data are screened commensurate with role prior to access and are bound by confidentiality obligations. All personnel with access to consumer or bureau data complete security-awareness training at least annually — covering data handling, phishing, credential hygiene, and incident reporting — with proof of completion retained. Access is provisioned on least privilege and removed promptly on role change or departure.

5.16 Physical and Environmental Security

Switch Labs stores and processes in-scope data exclusively within the facilities of its cloud providers, whose physical and environmental controls (facility access, surveillance, power redundancy, fire suppression, hardware lifecycle) are independently audited under each provider's SOC 2 Type II examination. Switch Labs operates no data centers of its own and does not store Restricted data on local media.

5.17 Data Retention and Secure Disposal

Consumer data is retained only as long as required for furnishing, dispute handling, and legal recordkeeping, per configurable per-company retention settings. Data past its retention window is securely destroyed. FCRA seven-year obsolescence is enforced in the generation pipeline.

5.18 Privacy

Switch Labs processes consumer data solely to provide the furnishing service to its customers, under the Data Processing Addendum published at `/legal/dpa`, which sets out the sub-processor list, US data-residency commitment, security measures, breach-notification terms, and audit rights. A data-deletion capability and configurable retention support consumer data-rights requests and customer retention policies.

5.19 Credit-Reporting-Specific Controls

Beyond general controls, Switch Labs enforces controls specific to consumer credit reporting: every record passes Metro 2 and bureau-specific validation before furnishing (portfolio type, account type, permitted status/ECOA codes), with non-conforming records blocked; the generation pipeline preserves accuracy and integrity; FCRA disputes are tracked from receipt through resolution with automated deadline monitoring; bureau responses and rejects are reconciled against submissions; consent/authorization gating may be enforced as a furnishing precondition; and Switch Labs operates strictly as an inbound furnisher-processor — it does not resell or provide access to consumer credit reports.

6. Compliance and Regulatory Alignment

- Built on SOC 2 Type II infrastructure. Metro2 runs entirely on SOC 2 Type II–certified providers — Vercel, Supabase, and AWS — whose independently audited reports are available under NDA. Under the shared-responsibility model, Switch Labs inherits their physical, infrastructure, availability, and encryption-at-rest controls, while Switch Labs' own application and operational controls are built to the SOC 2 Trust Services Criteria and evidenced through a completed security questionnaire (CAIQ / SIG Lite) and this policy.
- Bureau third-party security requirements. As a furnisher-processor, Switch Labs aligns its program to Experian's third-party Security Requirements (mapped to ISO/IEC 27002) and to the equivalent data-security terms in the TransUnion and Equifax furnisher agreements.
- FCRA / Regulation V furnisher obligations under §623, including accuracy/integrity controls and dispute management with 30-day deadline tracking.
- Metro 2® Format conformance with automated validation prior to furnishing.
- GLBA safeguarding of consumer financial information through encryption, access control, and segregation.

- State privacy / data-protection law: a Written Information Security Program consistent with Massachusetts 201 CMR 17.00; data-deletion capability supporting CCPA and comparable laws; and support for DFS-regulated customers' third-party requirements under NY DFS Part 500 §500.11.

7. Enforcement

Compliance with this policy is mandatory for all personnel and vendors within scope. Violations may result in revocation of access, disciplinary action up to and including termination, and termination of vendor relationships. Suspected violations must be reported to the Founder/CEO.

8. Exceptions

Any exception to this policy requires documented risk assessment and written approval by the Founder/CEO. Approved exceptions are recorded, time-bound where practicable, and reviewed until closed or renewed.

9. Policy Review and Maintenance

This policy is reviewed and, as needed, updated at least annually, and additionally upon any material change to the Metro2 platform, to applicable law or regulation, to bureau requirements, or following a material security incident. Review results are documented through version control and this document's revision history.

10. Adoption

This Information Security Policy was initially adopted by Switch Labs LC on September 20, 2022, and was most recently updated on March 10, 2026.

Appendix A — Sub-Processor Register

Sub-processor	Function	SOC 2 Type II	Data location
Vercel	Application hosting and compute	Yes	United States
Supabase	Managed database, object storage, platform auth	Yes	United States (AWS `us-east-1`)
Amazon Web Services	Underlying infrastructure and key management	Yes	United States
Stripe	Billing and payment processing	Yes	United States
GitHub	Source control and change history	Yes	United States
Google Workspace	Business communications	Yes	United States

All sub-processors are US-based. Sub-processor SOC 2 Type II reports are available from each provider's trust center (some under NDA) and can be furnished on request.

Appendix B — Control-to-Framework Mapping

Policy control	SOC 2 TSC	Experian TPSMS029 (ISO 27002)	FCRA / GLBA
Governance (5.1)	CC1	InfoSec policy / governance	—
Access control (5.3)	CC6.1–6.3	IAM, MFA	GLBA safeguards
Encryption & keys (5.4)	CC6.1, C1	Cryptography	GLBA safeguards
Tenant isolation (5.5)	CC6.1	Data security	—
Secure development / change (5.6)	CC8.1	Change management	—
Vulnerability mgmt / pentest (5.7)	CC7.1	Vulnerability management	—
Secure transmission (5.8)	CC6.7	Data security in transit	GLBA safeguards
Logging & monitoring (5.9)	CC7.2	Logging / monitoring	—
Incident response (5.13)	CC7.3–7.4	Incident management	FCRA breach duties
Vendor management (5.14)	CC9.2	Third-party risk	—
Personnel & training (5.15)	CC1.4	Personnel / training	—
Furnishing accuracy & disputes (5.19)	—	—	FCRA §623 / Reg V

Appendix C — Definitions

- Restricted data — the most sensitive data class (SSNs, full tradeline data, generated Metro 2 files, credentials, key material).
- Furnisher of record — the Switch Labs customer that owns the source data and its bureau relationships; Switch Labs acts as its processor.
- CRA / bureau — consumer reporting agency (Equifax, Experian, TransUnion).
- Metro 2® Format — the CDIA standard file format for furnishing tradeline data.
- Sub-processor — a third party that processes in-scope data on Switch Labs' behalf.
- KMS — key-management service used to manage encryption keys separately from data.

Appendix D — Revision History

Version	Date	Summary
1.0	September 20, 2022	Initial adoption of the Information Security Policy.
5.2	March 10, 2026	Current policy revision.

This Information Security Policy is maintained by Switch Labs LC under version control. For the authoritative current version, contact security@switchlabs.dev.