



Information Security Policy

ClassClerks

A product of OmniPro Labs, a DBA of Sculpt Marketing Group, LLC

Yes. Sculpt Marketing Group, LLC, operating ClassClerks through OmniPro Labs, maintains a documented information security policy and operational procedures to identify, mitigate, and monitor information security risks relevant to the business.

Document control	Value
Policy owner	ClassClerks Administration
Approval authority	Sculpt Marketing Group, LLC executive management
Version	1.0
Effective date	August 26, 2026
Review cycle	At least annually and after a material security or regulatory change
Classification	Confidential - may be shared with clients, regulators, and approved service providers for assurance purposes

1. Purpose and scope

The purpose of this policy is to preserve the confidentiality, integrity, and availability of ClassClerks information systems and the information entrusted to them. It applies to employees, contractors, administrators, developers, support personnel, and approved third parties who access ClassClerks production systems or data.

The policy covers the ClassClerks web application, administrative console, databases, file storage, application infrastructure, source code, deployment systems, backups, monitoring, support workflows, and integrations including Plaid, Stripe, Google Workspace, Twilio, and other client-authorized services.

1.1 Operationalization of the security program

This policy is operationalized through role- and tenant-based access controls, encryption of designated sensitive data and integration credentials, controlled change and deployment procedures, audit logging, incident response, vendor oversight, and monitored backup and recovery controls. Security risks are identified through application monitoring, testing, code review, vendor notices, operational reviews, and client or workforce reports; they are risk-ranked, assigned mitigating actions, and monitored through resolution or documented acceptance.

2. Security principles

- Least privilege: access is limited to the minimum information and functions required for an approved role.
- Tenant isolation: each client organization is logically separated, and requests operate within the authenticated user's assigned organization and location context.
- Defense in depth: authentication, authorization, encryption, validation, logging, vendor controls, backups, and recovery procedures operate as complementary safeguards.
- Data minimization: ClassClerks collects, uses, and retains only information needed to deliver the service, meet contractual duties, and satisfy legal requirements.
- Secure by default: sensitive features and integrations remain unavailable until explicitly configured and authorized.
- Accountability: material access and changes are attributable to authenticated users and are reviewed when security, privacy, billing, or client operations may be affected.

3. Governance and responsibilities

3.1 Executive management

Executive management approves this policy, assigns resources, accepts material security risk, and ensures that contractual, privacy, and regulatory obligations are addressed.

3.2 System administration and engineering

Authorized administrators and engineers maintain secure configuration, identity and access controls, application changes, monitoring, backup coverage, incident response, and vendor integrations. Production access is restricted to approved personnel and is reviewed when duties change.

3.3 Client administrators and users

Client administrators are responsible for assigning appropriate local roles, reviewing access, protecting credentials, and promptly reporting suspected misuse. All users must comply with acceptable-use requirements and may not share accounts or attempt to bypass access controls.

4. Information classification and handling

Class	Examples	Required handling
Restricted	Bank access tokens, integration secrets, tax identifiers, protected student medical or emergency information, authentication tokens	Encrypt in storage and transit; restrict to specifically authorized roles; never place in public pages, source control, support replies, or ordinary logs.
Confidential	Student, family, teacher, academic, attendance, billing, payroll, support, and contact records	Limit by tenant and role; share only for an approved business purpose; transmit through approved secure channels.
Internal	Operational procedures, non-public product documentation, deployment and support records	Limit to authorized personnel and approved service providers.
Public	Published marketing pages, approved school content, public policies	May be disclosed after appropriate review.

Restricted or Confidential information must not be copied to personal accounts, unmanaged devices, public AI services, or unapproved storage. Support and troubleshooting activities must use the narrowest data set necessary and redact credentials, card information, medical details, and other unrelated personal information.

5. Identity and access management

- Every user receives an individual account. Shared user accounts are prohibited except for documented, service-specific technical accounts that cannot support individual identities.
- ClassClerks enforces role- and permission-based access. Client users are placed in an organization context, and protected routes require authenticated tenant and permission checks.
- Administrative and third-party service access must use multi-factor authentication where the provider supports it. Plaid Dashboard access requires MFA for all authorized administrators.
- Authentication sessions are regenerated after successful login. Secure and HTTP-only cookies are required in production, and password-reset requests are rate limited.
- Access is granted on approval, reviewed periodically and following material role changes, and removed promptly when a relationship ends or access is no longer required.
- Privileged access must not be used for routine work. Development preview or impersonation capabilities, where enabled, must remain attributable to the initiating administrator and must not change a user's saved permissions.

5.1 Password and authentication requirements

Passwords must be unique, kept confidential, and stored only through approved one-way password hashing. Users are encouraged to use a password manager. Suspected credential compromise requires immediate reset and session revocation. Google sign-in and other approved identity providers may be used through state-validated OAuth flows.

6. Data protection and privacy

6.1 Encryption

- Production web traffic must use HTTPS with current, vendor-supported TLS configurations.
- Sensitive integration credentials and designated protected fields are encrypted using application-managed encryption before database storage.
- Production database and object-storage encryption status is monitored as part of recovery and infrastructure assurance.
- Encryption keys and secrets must be stored in protected server configuration or approved secret-management systems, never in source control or client-side code.

6.2 Plaid and financial data

ClassClerks uses Plaid Link to connect authorized business bank accounts for accounting and transaction reconciliation. ClassClerks does not request or store a user's online-banking username or password. Plaid provides a tokenized access credential after successful connection; that credential is encrypted before ClassClerks stores it. Bank connections are limited to the approved Transactions product and the minimum account information needed to present and reconcile financial activity.

- Plaid client credentials are maintained only in protected server configuration.
- Plaid access tokens are not displayed to users, stored in ordinary logs, or transmitted through support tickets.
- A bank connection may be removed through the application, which revokes the corresponding Plaid Item where supported.
- Only authorized accounting, executive, or specifically delegated roles may view connected bank data.
- Financial information is not sold and is not used for advertising or unrelated profiling.

6.3 Payment data

Payment card collection and payment processing are delegated to approved payment providers such as Stripe. ClassClerks does not intentionally store full payment card numbers or card security codes. Webhook signatures are verified before payment events are accepted.

7. Secure development and change management

- Application changes are maintained in version control and are scoped to a documented business or security requirement.
- Changes receive proportionate code review, automated tests, build checks, and focused regression testing before production deployment.
- Production releases use controlled deployment mechanisms. Credentials are not embedded in release packages, commands, or public logs.
- High-risk changes involving authentication, permissions, protected records, payments, grades, attendance, enrollment, or migrations require explicit approval and enhanced verification.
- After deployment, the application health endpoint and affected behavior are verified. A failed verification requires the release to stop, be corrected, or be rolled back.
- Dependencies and runtime components are maintained on supported versions and evaluated for known vulnerabilities in proportion to risk.

8. Infrastructure, logging, and monitoring

8.1 Infrastructure safeguards

Production systems are hosted in approved cloud infrastructure. Network access, administrative interfaces, storage, and databases are restricted to required services and authorized operators. Production and non-production environments must use separate credentials and must not share live customer data unless a documented, protected testing process requires it.

8.2 Logging and auditability

- Successful login, logout, material write operations, and selected administrative activities are recorded with the acting user, organization context, route or action, time, and source information when available.
- Logs must not contain passwords, Plaid secrets, bank-access tokens, full card data, or unnecessary protected personal information.
- Logs and operational alerts are reviewed when investigating errors, suspicious access, data-integrity concerns, or client-reported incidents.
- Log access is restricted and retention is based on security, legal, contractual, and operational requirements.

9. Vulnerability and incident management

9.1 Vulnerability management

Security issues identified through monitoring, testing, vendor notices, code review, or client reports are documented, risk-ranked, and addressed according to severity. Critical vulnerabilities with a credible path to compromise receive immediate containment and expedited remediation.

9.2 Incident response

- Identify and triage: confirm the affected systems, data, clients, and potential business impact.
- Contain: limit access, revoke credentials or tokens, isolate affected functions, and preserve relevant evidence.
- Eradicate and recover: remove the cause, patch or reconfigure systems, validate integrity, and restore service from a trusted state.
- Communicate: notify executive management and affected clients, providers, regulators, or individuals when required by law, contract, or material risk.
- Review: document root cause, timeline, impact, actions, and preventive improvements after recovery.

Suspected loss of Restricted data, compromise of a privileged account, or unauthorized access to financial information must be escalated to ClassClerks administration immediately.

10. Business continuity, backups, and recovery

ClassClerks maintains recovery controls designed to protect production databases and uploaded files from accidental deletion, corruption, or infrastructure failure. The recovery objective is to provide a minimum seven-day protected recovery window, subject to the capabilities and verified configuration of the hosting provider.

- Database point-in-time recovery and automated snapshots are monitored through the administrative recovery workspace when available.
- Uploaded documents and protected files use approved object storage; encryption, versioning, and noncurrent-version retention are monitored where supported.
- A restore request must be authorized, must identify the target recovery point, and must create a fresh pre-restore recovery point before production data is changed.
- Restored data must be validated in isolation when practicable before it replaces or modifies live data.
- Recovery procedures and provider coverage are reviewed periodically and after a material infrastructure change or incident.

11. Third-party risk management

Third-party services are selected based on business need, security capabilities, data-handling practices, contractual terms, and service reliability. Access is limited to the narrowest available scopes. Integration tokens are encrypted, provider access is reviewed, and connections are removed when no longer required.

Provider category	Control objective
Bank connectivity (Plaid)	Use hosted Plaid Link, tokenized credentials, Transactions-only access, MFA-protected administration, and revocation on disconnect.
Payments (Stripe and approved processors)	Keep card data with the processor, verify signed events, and restrict payment administration.
Cloud hosting and storage	Require access control, encryption capabilities, monitoring, backup or versioning support, and documented recovery processes.
Communications and productivity	Use OAuth or encrypted credentials, minimize scopes, and restrict messages and files by client role.
Forms and other integrations	Limit collected data, encrypt tokens and protected payloads, and review continued business need.

12. Data retention and secure disposal

Information is retained only as long as necessary for the service, client instructions, legal requirements, dispute resolution, financial recordkeeping, and security investigations. Deletion or archival must follow approved workflows, preserve required audit history, and avoid exposing other clients' information. Integration access is revoked before obsolete credentials are deleted.

13. Workforce security and acceptable use

- Personnel with production or Restricted-data access must understand this policy and receive role-appropriate security guidance.
- Company systems may be used only for authorized purposes. Attempts to bypass access controls, export unrelated client data, or share credentials are prohibited.
- Managed devices must use current security updates, screen locking, malware protection where applicable, and encrypted storage where supported.
- Security concerns, suspicious messages, lost devices, and accidental disclosures must be reported promptly without fear of retaliation for good-faith reporting.
- Access is reviewed and removed during offboarding or when a person's responsibilities change.

14. Exceptions and enforcement

A policy exception requires a documented business reason, defined scope and duration, compensating safeguards, and written approval from executive management. Violations may result in access suspension, disciplinary action, contract termination, and legal or regulatory notification when appropriate.

15. Review and maintenance

This policy is reviewed at least annually and after a material change to ClassClerks architecture, financial integrations, legal obligations, threat environment, or ownership. Updates are versioned, approved, and communicated to affected personnel.

Appendix A - Plaid security control summary

Control area	ClassClerks policy
Authentication	Plaid Dashboard administrators use individual accounts and MFA.
Credentials	Client ID and secret remain in protected server configuration; bank usernames and passwords are never collected by ClassClerks.
Data access	Production request is limited to Transactions for SMB bookkeeping and reconciliation.
Token protection	Plaid access tokens are encrypted before database storage and excluded from ordinary logs and user interfaces.
User authorization	A bank connection is initiated by an authenticated, authorized ClassClerks user through Plaid Link.
Revocation	Disconnecting a bank account removes local access and requests Plaid Item removal where supported.
Incident handling	Suspected compromise is contained by restricting access and rotating or revoking relevant credentials and tokens.

Approval

Approval field	Record
Approved by	Sculpt Marketing Group, LLC executive management
Policy owner	ClassClerks Administration
Effective date	August 26, 2026
Next review due	August 26, 2027, or earlier after a material change