

ACCESS CONTROLS POLICY

ClassClerks

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

Policy statement

Sculpt Marketing Group, LLC, operating ClassClerks through OmniPro Labs, maintains documented and operationalized access controls designed to ensure that access to systems and data is authorized, role-appropriate, attributable, periodically reviewed, and removed when no longer required.

Document control	Record
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, organizational, regulatory, or system change
Classification	Confidential - may be shared with clients, regulators, auditors, and approved service providers for assurance purposes

Policy objectives

- Limit access according to least privilege and approved business need.
- Separate client organizations and protect restricted financial, student, family, academic, and operational data.
- Require strong authentication for administrative and third-party service access.
- Make material access attributable, reviewable, and promptly revocable.
- Govern human and non-human access throughout its lifecycle.

1. Purpose and scope

This policy defines how ClassClerks requests, approves, provisions, authenticates, reviews, changes, and removes access to information systems and data. It applies to employees, contractors, administrators, developers, support personnel, client administrators, users, and approved service providers with access to ClassClerks systems or information.

The scope includes the ClassClerks web application, administrative console, production infrastructure, databases, object storage, source code, deployment tools, backups, monitoring, support workflows, and integrations including Plaid, Stripe, Google Workspace, Twilio, and other client-authorized services.

2. Access control principles

- Least privilege: access is limited to the minimum data and functions needed for an approved role.
- Need to know: restricted or confidential information is available only for an authorized business purpose.
- Individual accountability: users receive individual accounts; shared accounts are prohibited except for documented technical accounts that cannot support individual identities.
- Tenant isolation: requests operate within the authenticated user's assigned client, program, location, family, student, or class context.
- Secure by default: sensitive features and integrations remain unavailable until explicitly configured and authorized.
- Separation of duties: privileged, financial, deployment, and approval responsibilities are separated when practicable and receive additional review.
- Timely revocation: access is changed or removed promptly when duties, employment, contract status, or business need changes.

3. Governance and responsibilities

Role	Responsibilities
Executive management	Approves this policy, assigns resources, accepts material access risk, and authorizes exceptional privileged access.
ClassClerks administration and engineering	Implements identity, authentication, authorization, deployment, logging, review, and revocation controls for the platform and production environment.
Client administrators	Approve and maintain role-appropriate access for their organization, review local access, and report changes or suspected misuse promptly.
Managers and system owners	Confirm business need, scope, duration, and role for workforce or service-provider access.
Users	Protect credentials, use only assigned accounts, follow acceptable-use requirements, and report suspected compromise or inappropriate access.

4. Access lifecycle management

4.1 Request and approval

- Access requests must identify the individual or service, requested role or permissions, client or system scope, business purpose, approver, and any defined end date.
- Workforce production access requires approval from authorized ClassClerks management or the relevant system owner. Client access is approved by an authorized client administrator within that client's scope.
- Privileged, accounting, payment, bank-data, deployment, or integration-administration access requires explicit approval and is not granted by default.

4.2 Provisioning

- Accounts are uniquely assigned and mapped to approved roles and tenant context.
- Permissions are granted through role- and capability-based controls rather than broad ad hoc access whenever the platform supports it.
- Sensitive integrations use the narrowest available scopes and remain disabled until configured by an authorized administrator.
- Initial or reset credentials are delivered through approved secure flows and must not be sent through ordinary support messages.

4.3 Changes and transfers

When responsibilities change, managers, system owners, or client administrators review existing access and update it to the minimum required for the new duties. Access from a prior role is removed unless a documented continuing business need is approved.

4.4 Termination and revocation

- Access is disabled or removed promptly when employment, contract, client affiliation, or approved business need ends.
- Where compromise is suspected, sessions are revoked and passwords, API credentials, OAuth grants, and integration tokens are reset, rotated, or removed as appropriate.
- Client administrators are responsible for notifying ClassClerks of local offboarding needs that cannot be completed through self-service administration.

5. Authentication and session controls

- Passwords are stored only through approved one-way hashing and must not be available in plaintext.
- Google sign-in and other approved identity providers use state-validated OAuth flows.
- Administrative and third-party service access uses multi-factor authentication where supported. Plaid Dashboard access requires MFA for all authorized administrators.
- Production sessions use secure and HTTP-only cookies, are regenerated after successful authentication, and are subject to configured expiration and logout controls.
- Password-reset and authentication endpoints use rate limiting and validation intended to reduce automated abuse.
- Users must not share accounts, authentication codes, recovery codes, or passwords.

6. Role-based access and tenant isolation

ClassClerks enforces permissions in both the user interface and protected server routes. Hiding a button is not treated as authorization. Server-side checks evaluate the authenticated identity, assigned roles or capabilities, client organization, program or location context, and relationship to the protected record.

- Client users may access only the organizations, programs, locations, families, students, classes, records, and functions permitted by their assigned roles and relationships.
- Parents and students receive family- or self-scoped access. Teachers and assistants receive class-scoped access. Coordinators, principals, directors, accounting personnel, and administrators receive only the operational scope approved for their responsibilities.
- Restricted data such as bank tokens, tax identifiers, authentication secrets, protected medical information, and full payment-card data is not exposed through ordinary application views or support workflows.

7. Privileged and production access

- Privileged access is limited to approved administrators and engineers with a documented operational need.
- Privileged access must not be used for routine work when a lower-privilege account or role is sufficient.
- Production access uses approved administrative channels and separate production credentials. Production secrets must not be embedded in source code, release packages, public logs, or support tickets.
- Development preview or impersonation features, where enabled, remain attributable to the initiating administrator and must not silently change saved user permissions.
- High-risk actions involving authentication, permissions, protected records, payments, grades, attendance, enrollment, migrations, or production data corrections require explicit authorization and enhanced verification.

8. Service accounts and non-human access

- Technical accounts are used only when individual identities are not supported or when an application-to-application credential is required.
- Service accounts, API keys, OAuth credentials, deployment roles, and integration tokens are assigned the narrowest available permissions and documented owner or system purpose.
- Credentials are stored in protected server configuration or approved secret-management services and are never placed in client-side code or source control.
- Non-human credentials are reviewed, rotated when required by risk or provider capability, and revoked when the integration, system, or business need ends.
- Webhook events from payment and other sensitive providers are accepted only after applicable signature or authenticity validation.

9. Access reviews

Access is reviewed periodically and at least annually, as well as after material role changes, organizational changes, incidents, integration changes, or suspected misuse. Privileged, production, financial, bank-data, and third-party administrative access receives priority during reviews.

Review element	Required check
Identity	The account is assigned to a current, identifiable person or documented service.

Review element	Required check
Authorization	The role, capability, tenant, and data scope remain approved and necessary.
Privilege	No lower-privilege alternative would satisfy the business purpose.
Authentication	Required MFA and provider security controls remain enabled where supported.
Dormancy	Inactive, duplicate, obsolete, or unexplained accounts are disabled or investigated.
Integrations	OAuth grants, tokens, service accounts, and scopes remain necessary and appropriately restricted.
Evidence	Material findings, removals, exceptions, and follow-up actions are documented.

10. Endpoint and remote-access expectations

- Devices used for privileged or restricted-data access must use supported software, current security updates, screen locking, malware protection where applicable, and encrypted storage where supported.
- Users must not access restricted information through unmanaged public devices, shared browser profiles, or unapproved storage and messaging services.
- Lost devices, suspected phishing, credential exposure, or unauthorized access must be reported promptly so sessions and credentials can be revoked.

11. Logging, monitoring, and enforcement

- Successful login, logout, material write operations, and selected administrative actions are logged with the acting identity, time, organization context, route or action, and source information when available.
- Logs must not contain passwords, Plaid secrets, bank-access tokens, full card data, authentication recovery codes, or unnecessary protected information.
- Logs and operational alerts are reviewed when investigating access anomalies, errors, suspicious behavior, data-integrity concerns, or client-reported incidents.
- Unauthorized access attempts, account sharing, privilege misuse, or attempts to bypass controls may result in access suspension, investigation, disciplinary action, contract termination, and legal or regulatory notification when required.

12. Third-party and Plaid access controls

Third-party access is selected and configured according to business need, security capability, data handling, contractual requirements, and the minimum necessary scope. Provider connections are reviewed and removed when no longer required.

Control area	ClassClerks requirement
Administrative access	Individual Plaid Dashboard accounts are limited to authorized administrators and protected with MFA.
User connection	An authenticated, authorized ClassClerks user initiates the connection through hosted Plaid Link.
Credentials	ClassClerks does not collect bank usernames or passwords. Plaid client credentials remain in protected server configuration.

Control area	ClassClerks requirement
Product scope	Access is limited to the approved Transactions product and minimum account information needed for authorized bookkeeping and reconciliation.
Token protection	Plaid access tokens are encrypted before database storage and excluded from ordinary logs, user interfaces, support tickets, and source code.
Application access	Connected bank data is limited to authorized accounting, executive, or specifically delegated roles within the correct client scope.
Revocation	Disconnecting a bank account removes local access and requests Plaid Item removal where supported.

13. Exceptions

An exception requires a documented business reason, defined scope and duration, identified risk, compensating controls, an accountable owner, and written approval from executive management or an authorized client decision-maker within that client's scope. Exceptions are reviewed before expiration and may be revoked at any time.

14. Review and maintenance

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

Appendix A - Access control matrix

Access category	Typical scope	Approval and safeguards
Family and student	Self, linked family, enrolled classes, and authorized records	Relationship-based scope; protected server-side authorization; parent-managed options for students where applicable
Teacher and assistant	Assigned classes, rosters, classwork, attendance, grades, and permitted communications	Class assignment or approved role; no general access to unrelated student records
Coordinator and team	Approved operational area, location, or workflow	Role-specific capabilities; restricted actions remain unavailable unless separately approved
Principal and director	Approved program, location, or organization oversight	Management approval; enhanced review for financial or privileged capabilities
Accounting and bank data	Client or program accounting, authorized transactions, reconciliation, and related records	Explicit accounting or executive authorization; tenant restriction; Plaid admin MFA; tokens never exposed
Platform administration	System configuration and approved cross-client administration	Executive approval; individual account; MFA where supported; logging; privileged access used only when needed
Engineering and deployment	Source, build, deployment, and approved production operations	Authorized personnel only; separate production credentials; controlled deployment and verification
Service and integration	Specific application-to-application functions	Documented owner and purpose; minimum scopes; protected secrets; revocation when obsolete

Appendix B - Access review evidence checklist

- Review date, reviewer, systems, clients, and roles in scope.
- Current user and service-account inventory for the reviewed scope.
- Approval and business purpose for privileged, production, accounting, bank-data, and third-party administrative access.
- MFA status for administrative providers that support it.
- Duplicate, dormant, expired, transferred, or terminated access identified and resolved.
- Service-account owner, credential storage, active scopes, and continued need.
- Exceptions, compensating controls, responsible owner, and expiration date.
- Completed removals, follow-up actions, and management acceptance of any remaining risk.

Approval status: Approved and effective August 26, 2026. Policy owner: ClassClerks Administration. Next review due August 26, 2027, or earlier after a material change.