Finance Guru Access Control Policy

Effective Date: December 22, 2025
Last Reviewed: December 22, 2025
Next Review Date: June 22, 2026
Policy Owner: Finance Guru Development Team
Classification: Internal

1. Purpose

This policy establishes the access control framework for Finance Guru to ensure that access to production assets, sensitive data, and system resources is appropriately restricted based on business need and the principle of least privilege.

2. Scope

This policy applies to:

- All production systems and environments
- Development and staging environments
- User financial data accessed through Plaid integration
- API keys, tokens, and credentials
- Administrative interfaces and dashboards
- Source code repositories
- Cloud infrastructure and services

3. Access Control Principles

3.1 Principle of Least Privilege

All access is granted based on the minimum permissions necessary to perform job functions:

- Users receive only the access required for their specific role
- Access is not granted "just in case" or for convenience
- Elevated privileges are time-limited and logged
- Default access level is "no access"

3.2 Separation of Duties

Critical functions are divided among different individuals:

Function	Separation Requirement
Code deployment	Separate from code authoring
Access provisioning	Separate from access approval
Database administration	Separate from application development
Security monitoring	Separate from system administration

3.3 Defense in Depth

Multiple layers of access control are implemented:

• Network-level controls (firewalls, VPNs)

• Application-level authentication

• Data-level encryption and access restrictions

• Physical access controls where applicable

4. Identity Management

4.1 Account Types

Account Type	Purpose	Controls
User Accounts	Individual access	Unique per person, MFA required
Service Accounts	Application-to-application	No interactive login, rotated credentials
Administrative Accounts	System administration	Separate from daily-use accounts, enhanced logging
Emergency Accounts	Break-glass access	Sealed credentials, audit trail required

4.2 Account Lifecycle

Provisioning:

1. Access request submitted with business justification
2. Manager approval required
3. Security review for privileged access
4. Account created with minimum necessary permissions
5. User acknowledges acceptable use policy

Modification:

1. Role change triggers access review
2. New permissions require approval
3. Unnecessary permissions removed promptly

Deprovisioning:

1. Access revoked within 24 hours of termination

2. All sessions terminated immediately
3. Credentials rotated for shared resources
4. Access removal logged and verified

5. Authentication Requirements

5.1 Password Policy

Requirement	Standard
Minimum length	12 characters
Complexity	Upper, lower, number, special character
Expiration	90 days for privileged accounts
History	Cannot reuse last 12 passwords
Lockout	5 failed attempts = 30-minute lockout

5.2 Multi-Factor Authentication (MFA)

MFA is required for:

• All production system access
• Administrative interfaces
• Cloud service consoles (AWS, GCP, etc.)
• Source code repositories
• VPN connections
• Access to financial data

Approved MFA methods:

• Hardware security keys (preferred)
• Authenticator applications (TOTP)
• Push notifications from approved apps

5.3 Session Management

• Session timeout: 30 minutes of inactivity
• Re-authentication required for sensitive operations
• Concurrent session limits enforced
• Session tokens are cryptographically secure and non-predictable

6. Authorization Framework

6.1 Role-Based Access Control (RBAC)

Access is granted through predefined roles:

Role	Access Level	Permissions
Developer	Development environments	Code read/write, staging deploy
Operations	Production systems	Deploy, monitor, incident response
Administrator	Infrastructure	Full system access, user management
Auditor	Read-only	Logs, reports, compliance data
Support	Limited production	User assistance, read-only data access

6.2 Data Classification and Access

Data Classification	Access Requirements
Public	No restrictions
Internal	Authenticated users
Confidential	Role-based, need-to-know
Restricted (Financial Data)	Explicit authorization, MFA, audit logging

6.3 API Access Control

• All API endpoints require authentication
• API keys are environment-specific (dev/staging/prod)
• Rate limiting prevents abuse
• API access logged with request details
• Plaid tokens encrypted and never exposed to clients

7. Production Environment Controls

7.1 Access Restrictions

Production environment access is limited to:

• Authorized operations personnel
• On-call engineers during incidents
• Automated deployment systems

Prohibited in Production:

• Direct database modifications without change control
• Ad-hoc queries on financial data
• Debugging with production credentials
• Sharing of production access credentials

7.2 Change Management

All production changes require:

1. Documented change request
2. Peer review and approval
3. Testing in staging environment
4. Rollback plan documented
5. Post-deployment verification

7.3 Emergency Access

Break-glass procedures for emergencies:

1. Emergency access requested with incident reference
2. Access granted for limited duration (max 4 hours)
3. All actions logged and monitored
4. Post-incident review required within 24 hours
5. Access automatically revoked at expiration

8. Third-Party Access

8.1 Vendor Access Requirements

Third-party access to systems requires:

- Signed confidentiality agreement
- Security assessment completed
- Access limited to specific systems and timeframes
- Activity monitoring and logging
- Regular access review

8.2 Plaid Integration Security

- Plaid API credentials stored in secure secrets manager
- Access to Plaid dashboard limited to authorized personnel
- Webhook endpoints authenticated with signature verification
- No storage of end-user banking credentials

9. Physical Access Controls

9.1 Data Center Security

Cloud infrastructure providers (AWS/GCP) maintain:

• 24/7 physical security

• Biometric access controls

• Video surveillance

• Visitor logging and escort requirements

9.2 Endpoint Security

Devices accessing production systems must have:

• Full disk encryption enabled

• Endpoint protection software

• Automatic screen lock (5 minutes)

• Remote wipe capability

• Up-to-date security patches

10. Access Review and Monitoring

10.1 Periodic Access Reviews

Review Type	Frequency	Scope
User access certification	Quarterly	All user accounts
Privileged access review	Monthly	Admin and service accounts
Third-party access audit	Semi-annually	All vendor access
Dormant account review	Monthly	Inactive > 30 days

10.2 Monitoring and Logging

All access events are logged:

• Authentication successes and failures

• Authorization decisions

• Privileged operations

• Data access events

• Configuration changes

Logs are:

• Retained for 12 months minimum

• Protected from tampering

• Reviewed for anomalies

• Available for incident investigation

10.3 Alerting

Real-time alerts for:

Event	Response
Multiple failed logins	Account lockout, investigation
Access from new location	Verification required
Privileged operation	Logged and reviewed
After-hours access	Manager notification
Bulk data access	Immediate investigation

11. Compliance

This policy aligns with:

• **SOC 2 Type II** - Trust Services Criteria (CC6.1-CC6.8)

• **NIST 800-53** - Access Control family (AC-1 through AC-25)

• **OWASP** - Authentication and Access Control guidelines

• **PCI DSS** - Requirements 7 and 8

12. Policy Violations

Violations of this policy may result in:

• Immediate access revocation

• Disciplinary action

• Incident investigation

• Regulatory notification if required

All violations are documented and reviewed for process improvements.

13. Exception Process

Exceptions to this policy require:

1. Written justification with business need
2. Risk assessment and compensating controls
3. Security team approval
4. Time-limited approval (maximum 90 days)
5. Documentation in exception registry

14. Contact

Security Inquiries: support@unifiedental.com
Access Requests: support@unifiedental.com
Incident Reporting: support@unifiedental.com (Subject: SECURITY)

15. Version History

Version	Date	Changes	Author
1.0	2025-12-22	Initial policy creation	Finance Guru Team

Appendix A: Access Control Checklist

New Employee Onboarding

- [ ] Access request form completed
- [ ] Manager approval obtained
- [ ] Background check completed (if applicable)
- [ ] Acceptable use policy acknowledged
- [ ] MFA enrolled and verified
- [ ] Minimum necessary access provisioned
- [ ] Security awareness training completed

Employee Offboarding

- [ ] Access revocation initiated immediately
- [ ] All active sessions terminated
- [ ] Company devices returned
- [ ] Shared credentials rotated
- [ ] Access removal verified in all systems
- [ ] Offboarding logged for audit trail

Quarterly Access Review

- [ ] All user accounts reviewed
- [ ] Dormant accounts disabled
- [ ] Excessive permissions removed
- [ ] Role assignments verified
- [ ] Service account inventory updated

• [ ] Third-party access validated

This policy demonstrates Finance Guru's commitment to protecting sensitive financial data through comprehensive access controls.