IT System Security and Access Control

Purpose

This policy defines access control standards to protect company systems, data, and identities.

Access Principles

- Least privilege: grant only required access.
- Segregation of duties for sensitive financial systems.
- Access reviews conducted quarterly.

Authentication Standards

- Multi?factor authentication required for all remote access.
- Password length minimum 12 characters with complexity.
- Session timeout after 15 minutes of inactivity.

Account Lifecycle

Event	Action	SLA
New hire	Provision role?based access	1 business day
Role change	Update access	2 business days
Termination	Disable accounts	Same day

Privileged Access

- Admin accounts are separate from standard user accounts.
- Privileged access is time?bound and logged.
- Use of shared admin credentials is prohibited.

Access Review Metrics

Review Completion % = Completed reviews / total reviews x 100. Removal Rate = Access removals / access items reviewed.

Logging and Monitoring

- Authentication logs retained for 12 months.
- Critical system events trigger alerts within 5 minutes.
- Privileged activity is monitored and reviewed monthly.

Data Classification

Classification	Examples	Handling
Public	Marketing materials	No restrictions
Internal	Policies, procedures	Company use only
Confidential	Employee data, financials	Encrypt at rest
Restricted	Credentials, secrets	MFA + limited access

Incident Response

Security incidents must be reported within 1 hour. Containment and eradication follow the IR playbook.

Access Exceptions

Exceptions require documented justification, risk acceptance, and approval by Security.

Policy Review

This policy is reviewed annually or after material security incidents.

Version History

Version	Date	Description
1.0	2025-01-05	Initial access control policy
1.1	2026-02-01	Added privileged access logging requirements