Access Control Policy

[Your Company Name]

Policy Owner	CTO	**Approved By**	CEO
Effective Date	*[Date]*	**Last Review Date**	*[Date]*
Next Review Date	*[Date]*	**Version**	1.0

1.0 PURPOSE

This policy establishes the requirements for managing user access to *[Company Name]*'s information systems and data. The purpose is to ensure that access is granted appropriately, reviewed regularly, and removed promptly when no longer needed.

2.0 SCOPE

This policy applies to:

- All employees, contractors, and interns of *[Company Name]*
- All systems that store, process, or transmit company or customer data, including *[AWS, GitHub, Google Workspace, etc.]*
- Third-party vendors with access to company systems

3.0 POLICY REQUIREMENTS

3.1 Access Request and Provisioning

All requests for access to company systems must be submitted in writing to the CTO. Access will be granted based on the **principle of least privilege** — users receive only the access necessary for their role.

Request Process:

1. User or manager submits request to CTO via *[email/Slack/ticketing system]*
2. CTO approves and provisions access within *[24/48]* hours
3. User acknowledges receipt of access

3.2 Access Reviews

Access will be reviewed quarterly — by the 15th of January, April, July, and October.

Review Process:

1. CTO generates a list of all active users for each system
2. CTO reviews each user's access with relevant managers
3. Any unnecessary or inappropriate access is removed within 5 business days
4. The review is documented in a spreadsheet saved to *[Company Drive]*, including date, reviewer, and actions taken

3.3 Termination and Transfer

When an employee or contractor leaves the company, their access will be removed within **24 hours** of HR notification.

Offboarding Process:

1. HR notifies CTO of departure date
2. CTO disables all accounts within 24 hours
3. Access is reviewed to ensure no lingering permissions

For internal transfers, access will be adjusted to match the new role's requirements within 48 hours.

3.4 Authentication Requirements

All users must authenticate using the company's approved authentication methods, which include:

- Multi-factor authentication (MFA) for all remote access
- Strong passwords meeting *[tool]* complexity requirements
- No sharing of individual accounts or credentials

3.5 Third-Party Access

Contractors, vendors, and partners requiring access must:

- Sign a confidentiality agreement
- Use company-managed accounts where possible
- Have access reviewed quarterly
- Be removed within 24 hours when engagement ends

4.0 ROLES AND RESPONSIBILITIES

Role	Responsibility
CEO	Ultimate accountability for security program
CTO	Policy owner; approves and provisions access; conducts reviews
All Users	Comply with policy; report suspected unauthorized access
HR	Notify CTO of employee departures and transfers

5.0 COMPLIANCE AND ENFORCEMENT

Failure to comply with this policy may result in disciplinary action, up to and including termination of employment or contract.

6.0 REVIEW AND MAINTENANCE

This policy will be reviewed annually by the CTO and updated as needed.

7.0 DEFINITIONS

Term	Definition
Least Privilege	Granting only the access necessary to perform a job function
Multi-Factor Authentication (MFA)	Authentication using two or more verification methods
Access Review	A periodic assessment of user permissions, documented and retained

Approved By (CEO)	Policy Owner (CTO)	Effective Date
_____	_____	_____
Signature / Name	*Signature / Name*	*Date*