# Access Control Policy – Starter Template

This starter policy outlines access control practices for small businesses to help reduce security risk and ensure only authorized individuals have access to sensitive systems and data.

## 1. Purpose

The purpose of this policy is to establish guidelines for granting, reviewing, and revoking access to systems, applications, and data within the organization.

## 2. Scope

This policy applies to all employees, contractors, and third-party users who access the organization’s systems and data.

## 3. Access Control Principles

- Access will be granted based on job role and responsibilities (least privilege).  
- All users must have unique accounts where technically feasible.  
- Shared accounts should be avoided or tightly controlled with audit trails.  
- Administrative privileges must be limited and monitored.  
- Access rights will be reviewed at least quarterly.

## 4. User Account Management

- New user accounts must be requested and approved by a supervisor.  
- Departing employees’ access must be revoked on their last day of employment.  
- Password policies must follow NIST guidelines or vendor best practices.  
- MFA is required for all administrative and remote access.

## 5. Monitoring and Review

- Regular access audits will be conducted to ensure compliance.  
- Any suspicious access must be reported to the IT administrator immediately.  
- Systems should log access events for at least 90 days.

## 6. Exceptions

Any exceptions to this policy must be approved in writing by management and documented accordingly.

## 7. Acknowledgment

All users must review and acknowledge this policy before receiving access to systems.