Cybertech Access Control Policy and Procedure

Introduction

Cybertech is committed to safeguarding its physical or digital assets by implementing a robust access control policy. This document shows the policies and procedures that are very important to regulate access to physical locations, information systems, and sensitive data to prevent unauthorized access and ensure compliance with relevant laws, regulations, and industry standards.

1. User Access Provisioning

a. User Registration

- All new employees and contractors must register their accounts through the IT department.
- Registration must be approved by the department manager and IT security team.

b. Access Request

- Employees must submit formal requests for system access.
- Requests must be reviewed and approved by appropriate managers and IT security personnel.

c. Account Creation

- The IT department will create accounts with appropriate access levels based on role-based access control principles.
- Temporary access will have predefined expiration dates.

2. User Access De-Provisioning

a. Termination Process

- Upon termination, HR will notify the IT department immediately.
- Access will be revoked within 24 hours of termination.

b. Account Disablement

- Accounts of inactive users will be disabled after a predefined period.

c. Access Removal

- Access to all company systems and physical locations will be removed upon termination.

3. Periodic Access Reviews

a. Access Review Frequency

- Access reviews will be conducted quarterly.

b. Access Review Process

- IT security will generate access reports.
- Department managers will review and validate access rights.

c. Access Review Reporting

- Findings will be documented and reported to senior management.

4. Password Requirements

a. Password Policy

- Passwords must be at least 12 characters long and include a combination of uppercase, lowercase, numbers, and special characters.

b. Password Storage

- Passwords will be stored using industry-standard encryption methods.

c. Password Reset

- Users must reset their passwords every 90 days.
- Forgotten passwords must be reset through secure identity verification methods.

5. Privileged User Accounts

a. Privileged Account Management

- Privileged accounts will be restricted to designated personnel.

b. Privileged Access

- Access to privileged accounts must be approved by senior management.

c. Privileged Account Monitoring

- Privileged account activity will be logged and reviewed periodically.

d. Physical Access

i. Physical Access Control

- Employees must use badge-based authentication to enter secure areas.

ii. Physical Access Request

- Requests for physical access must be approved by facility security personnel.

iii. Physical Access Monitoring

- Surveillance cameras and access logs will be reviewed periodically.

6. Compliance and Enforcement

- Cybertech will comply with GDPR, HIPAA, ISO 27001, NIST 800-53, and other applicable regulations.

- Violations of this policy may result in disciplinary action, including termination of employment.
- Regular security awareness training will be conducted for all employees.

7. Review and Updates

- This policy shall be reviewed and updated annually or as needed.
- The IT security team will ensure continuous regulatory requirements.

This policy has been in line to incorporate detailed procedures for user access provisioning, de-provisioning, periodic access reviews, password management, privileged user accounts, and physical access control, all aligned with the NIST Cybersecurity Framework.

Effective Date: 29/10/2025
Approved By: Mr Aliu B. Sanusi
Next Review Date: 28/01/2026