Access Control Policy

|  |  |
| --- | --- |
| **Company** | Guatemaltek |
| **Version** | 1.0 |
| **Effective Date** | 2026-01-01 |
| **Review Schedule** | Annually |
| **Responsible Officer** | Chief Information Security Officer (CISO) |

# Purpose

This Access Control Policy establishes requirements for managing access to Guatemaltek's information systems and data to ensure only authorized individuals can access resources appropriate to their role and responsibilities.

# Scope

Applies to all Guatemaltek employees, contractors, and third parties requiring access to information systems, applications, networks, and data.

# Policy

## User Account Management

1. Unique Accounts: Each user must have a unique account - no shared credentials
2. Provisioning: Access requests require manager approval
3. Least Privilege: Users granted minimum access required for job functions
4. Review: Access rights reviewed quarterly for privileged users, annually for standard users
5. Termination: Access revoked immediately upon termination or role change

## Authentication

1. Passwords: Minimum 12 characters, complexity requirements per Password Policy
2. Multi-Factor Authentication (MFA): Required for:

* Remote access (VPN)
* Email systems
* Administrative accounts
* Cloud services
* Financial systems

1. Session Management:

* Auto-logout after 15 minutes inactivity
* Screen lock after 10 minutes
* No concurrent sessions from different locations

## Privileged Access

1. Separate Accounts: Administrative tasks require separate privileged accounts
2. Approval: Privileged access requires CISO approval
3. Monitoring: All privileged actions logged and reviewed monthly
4. Just-in-Time: Temporary elevation for specific tasks when possible

## Access Control Lists (ACLs)

1. Role-Based: Access based on job role, not individual
2. Documentation: All ACLs documented and maintained
3. Default Deny: Access denied unless explicitly granted
4. Segregation of Duties: Critical functions require multiple people

# Compliance

ISO 27001: A.9.1, A.9.2, A.9.3, A.9.4 (User access management)

NIST CSF: PR.AC-1 through PR.AC-7 (Identity management, authentication)

Approved by: CISO | Date: 2026-01-01 | Next Review: 2027-01-01