Table of Contents

# Information Security Policy

**Company:** Guatemaltek **Version:** 1.0 **Effective Date:** 2026-01-01 **Review Schedule:** Annually **Responsible Officer:** Chief Information Security Officer (CISO) **Department:** IT Department **Contact:** security@guatemaltek.com

## Purpose

This Information Security Policy establishes the foundation for Guatemaltek’s information security program. It defines the organization’s commitment to protecting information assets and establishes the framework for all security-related policies, standards, and procedures in compliance with ISO 27001 and NIST Cybersecurity Framework.

## Scope

This policy applies to all Guatemaltek employees, contractors, consultants, temporary workers, and third parties with access to Guatemaltek information or systems. It covers all information assets, systems, networks, and devices, whether owned by Guatemaltek or third parties used for business purposes.

## Policy

### Information Security Objectives

Guatemaltek is committed to ensuring:

1. **Confidentiality**: Information accessible only to authorized individuals
2. **Integrity**: Information accurate, complete, and protected from unauthorized modification
3. **Availability**: Information and systems accessible when needed by authorized users

### Security Governance

**CISO Responsibilities:** - Overall information security program management - Security policy development and enforcement - Security risk management - Compliance oversight and reporting

**IT Department Responsibilities:** - Implementation of technical security controls - Security infrastructure maintenance - Security event monitoring - Incident response support

**All Employees:** - Comply with security policies - Report security incidents promptly - Complete required security training - Protect information assets

### Risk Management

* Conduct annual risk assessments
* Identify and evaluate security threats and vulnerabilities
* Implement risk treatment plans
* Monitor and review security risks continuously

### Access Control

* Unique user accounts for all individuals
* Role-based access control (RBAC)
* Multi-factor authentication for remote and privileged access
* Regular access reviews (quarterly for privileged, annually for standard)
* Immediate access revocation upon termination

### Asset Management

* Maintain inventory of all information assets
* Classify assets based on sensitivity and criticality
* Apply appropriate security controls based on classification
* Secure disposal of assets at end-of-life

### Security Operations

* Continuous security monitoring and logging
* Vulnerability management and patching
* Security event correlation and analysis
* Regular security assessments and audits

### Incident Response

* 24/7 incident reporting mechanism
* Documented incident response procedures
* Incident response team and roles defined
* Post-incident review and improvement

### Business Continuity

* Business impact analysis conducted
* Recovery time and point objectives defined
* Regular backup procedures
* Disaster recovery testing annually

### Third-Party Security

* Security assessment of vendors before engagement
* Contractual security requirements for all vendors
* Regular vendor security reviews
* Data sharing agreements and NDAs

### Security Awareness

* Annual security awareness training for all personnel
* New hire security orientation
* Phishing simulation exercises
* Role-specific security training

## Compliance

**ISO 27001 (Clause 5.2):** - This policy fulfills the requirement for a documented information security policy - Establishes management commitment to information security - Provides framework for setting security objectives

**NIST Cybersecurity Framework:** - **Identify:** Asset management, risk assessment - **Protect:** Access control, awareness, data security - **Detect:** Continuous monitoring, detection processes - **Respond:** Incident response planning - **Recover:** Recovery planning, improvements

**Violations:** Non-compliance may result in disciplinary action up to and including termination of employment or contract.

## Management Support

Guatemaltek’s executive leadership fully supports this Information Security Policy and commits to providing adequate resources, budget, and authority to the CISO and IT Department to implement and maintain the information security program.

The CISO is granted authority to implement security controls, enforce policies, conduct audits, and access all systems for security purposes.

## Review Schedule

This policy will be reviewed **annually** by the CISO and approved by executive management. Next review: **2027-01-01**.

Policy will be reviewed immediately following significant security incidents, organizational changes, or regulatory requirement changes.

**Approved by:** Chief Information Security Officer (CISO) **Approval Date:** 2026-01-01 **Next Review Date:** 2027-01-01

**Document Classification:** Internal Use **Policy Owner:** Guatemaltek IT Department

*Generated using Cybersecurity Policy Generator* *Template Source: SANS Security Policy Templates* *Compliance: ISO 27001, NIST CSF*