Incident Response Policy

|  |  |
| --- | --- |
| **Company** | Guatemaltek |
| **Version** | 1.0 |
| **Effective Date** | 2026-01-01 |
| **Review Schedule** | Annually |
| **Responsible Officer** | CISO |

# Purpose

Establishes procedures for detecting, reporting, responding to, and recovering from security incidents.

# Scope

All Guatemaltek employees, contractors, IT systems, and security events.

# Policy

## Incident Definition

Security incident: Any event that compromises confidentiality, integrity, or availability of information or systems.

## Incident Response Team

* CISO: Team lead, overall coordination
* IT Department: Technical response and recovery
* Legal: Legal/regulatory guidance
* HR: Employee-related incidents
* Communications: External communication (if needed)

## Incident Classification

* Data breach affecting customer/employee data
* Ransomware/cryptolocker attack
* Complete system compromise
* Active attacks in progress
* Malware infection
* Unauthorized access attempts
* Service degradation affecting business
* Lost/stolen devices with sensitive data
* Policy violations
* Suspicious activity
* Minor security control failures
* Failed login attempts
* Spam/phishing emails
* Minor configuration issues

## Incident Response Process

* 24/7 reporting: security@guatemaltek.com or call IT Department
* Report immediately - don't investigate alone
* Preserve evidence - don't delete or modify
* Classify severity
* Activate incident response team
* Document initial findings
* Isolate affected systems
* Prevent spread
* Preserve evidence for investigation
* Remove threat/vulnerability
* Patch systems
* Reset compromised credentials
* Restore systems from clean backups
* Verify system integrity
* Monitor for recurrence
* Document lessons learned
* Update procedures
* Implement preventive measures
* Report to management

## Reporting Requirements

* All incidents reported to CISO within 1 hour of detection
* P1/P2 incidents: CISO notifies executive management immediately
* Customers: Within 72 hours for data breaches
* Regulators: Per regulatory requirements
* Law Enforcement: For criminal activity

## Documentation

* Incident log maintained by IT Department
* All actions documented with timestamps
* Evidence preserved for analysis
* Monthly incident summary to management

# Compliance

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