Physical Security Policy

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

# Purpose

Protects Guatemaltek's physical assets, facilities, equipment, and personnel from unauthorized access, damage, and interference.

# Scope

All Guatemaltek facilities, equipment, and physical access to information assets.

# Policy

## Facility Access Control

* Key card/badge required for entry
* Visitors must sign in, receive visitor badge, and be escorted
* Access logs maintained and reviewed monthly
* Keys/badges returned upon termination
* Additional authorization required
* Separate access controls
* Access logged and monitored
* No visitors without explicit approval
* Document after-hours access requirements
* Security system armed when office unoccupied
* Log all after-hours entries

## Physical Security Controls

* Locked doors on all entrances
* Security alarm system
* Adequate external lighting
* Windows secured and locked
* Server room: Locked, climate controlled, fire suppression
* Network equipment: Locked cabinets/rooms
* Sensitive areas: Restricted access
* Security cameras at entrances/exits (retained 30 days)
* Servers and network equipment in locked rooms
* Laptops: Cable locks when unattended in office
* Portable devices: Encrypted, tracked via asset management
* Equipment inventory maintained

## Clean Desk/Clear Screen

* Lock or log off workstations
* Secure confidential documents
* No sensitive information visible
* Shred unnecessary confidential papers
* Lock screen when leaving desk
* Don't leave confidential docs unattended
* Lock laptops when out of sight

## Visitor Management

1. All visitors sign in at reception
2. Visitor badge issued (returned on exit)
3. Employee escort required
4. No unescorted access to work areas
5. Visitor log maintained (name, company, purpose, time in/out)

* Pre-authorized for maintenance/service
* Escorted or logged access
* Background checks for regular vendors

## Equipment Disposal

* Data sanitization required before disposal (per NIST SP 800-88)
* Certificate of destruction for drives
* Asset management updated
* Confidential/Restricted: Cross-cut shredding or professional destruction
* Secure shred bins throughout office
* Quarterly professional shredding service
* USB drives, backup tapes: Physical destruction
* Document serial numbers
* Update inventory

## Mobile Device Security

* Encryption mandatory
* Screen lock (<10 min)
* Remote wipe capability
* Lost/stolen reported immediately
* Must meet security requirements if accessing company data
* Company reserves right to wipe company data

## Environmental Controls

* Climate control: 68-72°F, 40-50% humidity
* Fire suppression: Clean agent system
* Water detection sensors
* UPS (uninterruptible power supply)
* Generator backup for extended outages
* Regular maintenance schedules
* Smoke detectors and fire extinguishers
* Emergency evacuation plan posted
* First aid kits available
* Emergency lighting

## Emergency Procedures

1. Activate alarm
2. Evacuate per posted routes
3. Call 911
4. Account for all personnel at assembly point
5. Alert security/management
6. Call 911 if threat present
7. Evacuate if safe to do so
8. Document incident
9. Follow building emergency procedures
10. Activate Business Continuity Plan if needed
11. Ensure personnel safety first
12. Assess facility damage before re-entry

## Physical Security Incidents

* Unauthorized access attempts
* Lost/stolen equipment or badges
* Damage to facilities or equipment
* Safety hazards
* Suspicious persons/activity
* Security incident documented
* Review camera footage if applicable
* Determine root cause
* Implement corrective actions

## Responsibilities

# Compliance

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