Acceptable Use Policy

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

# Purpose

Defines acceptable use of Guatemaltek IT resources to protect against security risks, legal issues, and inappropriate use.

# Scope

All employees, contractors, and third parties using Guatemaltek IT resources.

# Policy

## General Use

1. IT resources are company property for business purposes
2. Limited personal use acceptable if it doesn't interfere with work
3. Users responsible for all activity under their accounts
4. Company may monitor all IT resource usage

## Security Requirements

1. Comply with Password Policy and security standards
2. Lock screen when leaving workstation (max 10 min)
3. Report security incidents immediately
4. No circumventing security controls
5. Use only approved software and services

## Prohibited Activities

1. Illegal activities or policy violations
2. Unauthorized access to systems or data
3. Sharing credentials or allowing unauthorized access
4. Installing unauthorized software
5. Connecting unauthorized devices
6. Storing/transmitting confidential data on personal devices
7. Bypassing security controls
8. Malicious software introduction
9. Excessive personal use interfering with duties
10. Harassment, discrimination, or offensive content

## Email and Communications

1. Professional tone in business communications
2. No spam or chain letters
3. Exercise caution with attachments and links
4. Company email signature required for external communication

## Internet Use

1. Business purposes primary; limited personal use acceptable
2. No accessing inappropriate content
3. No illegal downloading
4. Bandwidth-intensive personal use prohibited during business hours

## Social Media

1. Personal opinions must not represent company
2. No sharing confidential company information
3. No disparaging company, customers, or partners
4. Follow company social media guidelines

## Remote Work

1. Secure home network required
2. VPN mandatory for company resource access
3. Physical security of company equipment
4. No family/friend use of company devices

# Compliance

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