Business Continuity Policy

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

# Purpose

Ensures Guatemaltek can maintain or rapidly resume critical business operations following disruptive events.

# Scope

All Guatemaltek systems, data, personnel, and business processes.

# Policy

## Business Impact Analysis

Annual BIA identifies:

* Critical business functions
* Recovery Time Objectives (RTO)
* Recovery Point Objectives (RPO)
* Resource requirements
* Dependencies

## Recovery Objectives

* RTO: 4 hours - System must be operational
* RPO: 1 hour - Maximum acceptable data loss
* Examples: Customer database, email, production applications
* RTO: 24 hours
* RPO: 24 hours
* Examples: File servers, internal applications
* RTO: 72 hours
* RPO: 1 week
* Examples: Archives, non-production systems

## Backup Strategy (3-2-1 Rule)

* 3 copies of data (1 primary + 2 backups)
* 2 different storage media types
* 1 off-site backup copy
* Critical systems: Daily full backup + continuous/hourly incremental
* Important systems: Daily incremental, weekly full
* Standard systems: Weekly incremental, monthly full
* Critical systems: Quarterly restore test
* Important systems: Semi-annual restore test
* Standard systems: Annual restore test
* Document all test results

## Backup Retention

* Daily backups: 30 days
* Weekly backups: 90 days
* Monthly backups: 1 year
* Annual backups: 7 years (or per regulatory requirements)

## Disaster Recovery

* Emergency contact list (updated quarterly)
* System recovery procedures
* Alternative work locations
* Communication plans
* Vendor contact information
* Annual full DR test/exercise
* Semi-annual tabletop exercises
* Document lessons learned and improve

## Continuity Procedures

1. Activate Business Continuity Plan
2. Notify stakeholders per communication plan
3. Move to alternative location if needed
4. Restore systems per priority (Critical → Important → Standard)
5. Verify data integrity after restoration
6. Life safety (always first priority)
7. Critical systems restoration
8. Customer communication
9. Important systems restoration
10. Return to normal operations

## Alternate Processing

* Cloud-based backup and recovery infrastructure
* Work-from-home capabilities for all personnel
* Documented recovery procedures for each critical system

## Pandemic/Remote Work

* All employees equipped for remote work
* VPN capacity for 100% remote workforce
* Collaboration tools licensed for all personnel
* Regular remote work drills

# Compliance

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