CorporateOne
FEDERAL CREDIT UNION

Security Practices

Security Practices

Table of Contents

CORPORATE ONE SECURITY PRACTICES

This document describes the security practices used by CORPORATE ONE FCU. Due to the constantly changing nature of security concerns and technologies, CORPORATE ONE reserves the right to modify this document as appropriate.

CORPORATE ONE SECURITY EMPLOYEES

CORPORATE ONE employs personnel who focus specifically on information security throughout all levels of the corporate at the technical, operational and management levels including in-house Certified Information Systems Security Professionals ("CISSP") in the information technology department and the risk management departments.

CORPORATE ONE EMPLOYEES

CORPORATE ONE performs criminal background checks and drug testing on all staff, before allowing them access to system information. Mandatory participation in Security Awareness Training is required of all employees on an annual basis. The corporate maintains high security awareness amongst staff throughout the year through its ongoing security awareness program. Employee orientation familiarizes new hires with the corporate's information security policies and practices.

INFORMATION SECURITY POLICIES

CORPORATE ONE maintains and practices Information Security policies covering such areas as Internet, E-Mail, Identification and Authentication, Virus Protection, Anti-Malware Protection, Records Retention and Physical Security policies and guidelines. All policies are approved and adopted by the Corporate's Board of Directors. Policies are reviewed and updated annually.

INFORMATION SECURITY RISK ASSESSMENT (ISRA) PROGRAM

CORPORATE ONE utilizes an internal ISRA program to strengthen security practices. The objective of performing risk management is to enable CORPORATE ONE to accomplish its mission(s) by improving security of the systems that store, process or transmit information.

SECURITY AUDITING PROGRAM

CORPORATE ONE conducts regular internal and external security audits as part of an on-going audit program.

VULNERABILITY AND PENETRATION TESTING

CORPORATE ONE identifies system and software vulnerabilities by conducting monthly internal and external scans. Vulnerability and Penetration tests are performed by CORPORATE ONE security personnel. On an annual basis a vulnerability and penetration test is conducted by a qualified third party. CORPORATE ONE security personnel also monitor industry and government alerts on a daily basis in order to respond as necessary to any exploitation of operating system vulnerabilities.

BUSINESS CONTINUITY PLAN

Each business unit and every application at the corporate is ranked as to its criticality and has contingency plans in place. These plans are exercised regularly to ensure uninterrupted service to members. The Corporate's written business continuity plan is maintained and exercised under the direction of the Business Continuity Department.

PHYSICAL SECURITY

Entrance to CORPORATE ONE facilities are secured via a card reader validation system.

Access to production systems is maintained in a segmented data center. Entry to this area requires a card reader validation. Production personnel are the only staff that have access to the data center hardware.

The Corporate's data centers in both Florida and Ohio are housed in secure colocation facilities providing power redundancy, high speed internal networks and disaster recovery services. The facilities in Florida are rated to withstand category 5 hurricane winds.

Additionally, generators are in place at all corporate locations to provide for continued operations should loss of power occur.

OPERATING SYSTEM AND NETWORK INFRASTRUCTURE

CORPORATE ONE utilizes network security standards and secure common operating system configurations:

- Standardized guidelines and best practices are followed on servers and systems that are exposed to the Internet.
- Each web server is isolated to reduce the risk of compromise between systems.
- All unnecessary access points and services are removed or disabled.
- Logs of critical system operations are created, retained, monitored, and analyzed.

FIREWALLS

CORPORATE ONE uses multiple firewall devices and layers to protect servers and databases.

AUTHORIZATION & AUTHENTICATION

CORPORATE ONE permits only authorized and authenticated users to access or modify data as appropriate to their job function. In addition, CORPORATE ONE utilizes strong authentication methods that require a user ID, complex passwords, certificates and mutual authentication.

INTRUSION DETECTION

CORPORATE ONE monitors (24 hours a day, 7 days a week) its systems for intrusion at the host and network levels. Security tools are utilized to monitor traffic on the network infrastructure to identify suspicious activity or potential attacks.

DISASTER RECOVERY TESTING

CORPORATE ONE conducts annual disaster recovery exercises. The Corporate One CBTS data center disaster recovery exercise took place on Friday, February 20th, 2015. Corporate One ran a full production day from our disaster recovery site. The Corporate One Cologix datacenter disaster recovery exercise occurred on December 5th, 2015. On that Saturday, the Corporate failed over all critical systems from its Jacksonville, Florida site (primary data center) to the Worthington, Ohio (secondary data center) site in order to test our ability to failover and run from normal production operations from our back-up systems.

APPLICATION SECURITY

CORPORATE ONE protects Internet applications through security practices including 'session timeouts', logging, change management, risk assessment, code review, security penetration testing, and vulnerability testing.