



Summary for Members
Security Overview

December 2011

Public Statement on Information Security

Alloya Corporate recognizes that our members have an interest in knowing that Alloya Corporate's physical and information assets are appropriately managed and protected. This statement is intended to provide visibility into Alloya Corporate's approach to information security and offer assurance that Alloya Corporate and its affiliates have implemented appropriate policies, procedures and controls to protect the confidentiality, integrity and availability of our information assets and member data.

This document provides a high-level overview of Alloya Corporate's approach to Information Security.

Information Security Policy and Program

Alloya Corporate's Information Security Policy and Information Security Program are the foundation of our approach to information security and protection.

The board of directors (board) is responsible for understanding and approving the Information Security Policy and for setting and/or delegating information security risk acceptance threshold definitions. The board approves information security policies.

Alloya Corporate's Information Security Program provides an overall framework for managing information security processes. The Information Security Program establishes standards pertaining to the configuration, integration, use and management of information assets. The standards defined in the Information Security Program are intended to be consistent and congruent with all NCUA, FFIEC and OCCU regulations and guidelines governing information systems and assets, including Part 748 of the NCUA rules and regulations.

Information Security Committee

The Information Security Committee (ISC) is responsible for administering the Information Security Policy and Information Security Program. The committee directly oversees the development of related policies, standards and procedures. They review information security risk assessment reports and determine risk management strategies. The ISC determines risk acceptance thresholds based on the specific application or asset being assessed.

Information Security Risk Assessment

To guide employees in effectively and efficiently managing information security risk, Alloya Corporate has implemented an Information Security Risk Assessment (ISRA) process as part of the organization's comprehensive Information Security Program.

Data Classification

Alloya Corporate has created a data classification scheme in order to appropriately classify and protect information assets. All employees are responsible for implementing appropriate managerial, operational, physical and technical controls for access, transmission, retention, protection and disposal of data.

Layered Security

Alloya Corporate utilizes various preventive, detective and technical controls to support our layered security approach to information security.

Authentication, Authorization and Access

Policies and procedures have been implemented to support the principle of least privilege for authorization and access to corporate resources. Multifactor authentication, complex passwords and client certificates are some of the controls in place to protect information assets from unauthorized access.

Physical and Environmental Security

Alloya Corporate has various controls in place to prevent unauthorized access to its physical locations. Physical and environmental security monitoring is conducted 24 hours a day, 7 days a week by internal and external systems and resources.

Backup and Recovery

Alloya Corporate has implemented various data protection solutions including nightly backups, remote data replication and data encryption. Business continuity testing is conducted annually.