Summary for Members

Security Overview

December 2017

Public Statement on Information Security

Alloya recognizes that our members have an interest in knowing that Alloya's physical and information assets are appropriately managed and protected. This statement is intended to provide visibility into Alloya's approach to information security and offer assurance that Alloya 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's approach to Information Security.

Information Security Policy and Program

Alloya'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'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.

Transaction Risk Committee

The Transaction Risk Committee (TRC) 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 TRC determines risk acceptance thresholds based on the specific application or asset being assessed.

Information Security Risk Assessments

To guide employees and the organization in effectively and efficiently managing information security risk, Alloya has implemented an Information Security Risk Assessment (ISRA) process as part of the organization's comprehensive Information Security Program. Third party service providers are also reviewed based on the critically of the service provided.

Data Classification

Alloya 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's information security strategy requires multiple layers of security controls and testing to establish several lines of defense between a potential attacker and our assets. To successfully attack the system/data, each security layer would need to be penetrated. With each penetration, the probability of detecting the attacker increases. Alloya utilizes various preventive, detective and technical controls to support our layered security approach to information security.

Cyber Security
Financial organizations are continued targets of various cyber security threats. To combat these ongoing threats, Alloya has implemented various enterprise level security controls to protect the organization. In general, these controls include various in house and third party defenses which are designed to detect, and prevent cyber security threats from impacting the organization. Alloya has also implemented various DDoS and 24x7 system monitoring tools to ensure that we are doing all we can to stay ahead of these threats.

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, one-time use passwords, complex passwords, encryption and client certificates are some of the controls in place to protect information assets from unauthorized access.

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

Training
All employees play a role in protecting the safety of our information assets. Alloya requires that employees complete information security training on an annual basis. This training provides employees with information regarding the latest security threats and techniques, information security best practices. Annual training also includes a simulation and testing component. In addition security notifications are sent to staff periodically throughout the year. Alloya also offers security awareness training to members throughout the year,

Audit and Third Party Review
On an annual basis Alloya contracts with independent third parties to perform network penetration testing and conduct a review of the effectiveness of our information security controls. Additionally, Alloya is subject to annual review by the NCUA to ensure compliance with various regulatory requirements relating to information security.