

Southeast Corporate Federal Credit Union Information Security Disclosure Statement

Southeast Corporate FCU maintains electronic and hardcopy information assets that are essential to performing services for our member credit unions. Similar to any other capital resources owned by the Corporate, these resources are viewed as valuable assets over which the Corporate has both rights and obligations to manage, protect, secure, and control. Southeast Corporate FCU employees, contractors, and other affiliates are required to utilize these information assets for only legitimate business purposes while assuring the Confidentiality, Integrity and Availability of the assets.

The Board and management of Southeast Corporate FCU are committed to preserving the confidentiality, integrity and availability of all the physical and electronic information assets throughout the organization in order to preserve its legal, regulatory and contractual compliance, competitive edge and commercial image. The Information Security Management System is the enabling mechanism to address and incorporate the guidance provided by the Federal Financial Institutions Examination Council (FFIEC), the National Credit Union Administration (NCUA) and the best practices defined in ISO/IEC 27002:2005 for information sharing, electronic operations, e-commerce and for reducing information security related risks to acceptable levels.

The purpose of this Disclosure Statement is to overview the elements of Southeast Corporate FCU's Information Security Management System that allows for the protection of information assets from all threats, whether internal or external, deliberate or accidental.

Elements of Southeast Corporate FCU's Information Security Management System include:

Security Policy

Southeast Corporate FCU management has set a clear policy direction in line with business objectives and demonstrates support for and commitment to information security through the establishment of a Security Committee and the issue and maintenance of information security policies, procedures and instructions.

Organization of Information Security

Southeast Corporate FCU has established a management framework to initiate and control the implementation of information security within the Corporate. Management, through the Security Committee, approves information security policies, assigns security roles and reviews the implementation of security across the organization. Management has established the Information Assurance department to focus specifically on information security at the operational, technical and management levels of the Corporate.

Asset Management

Southeast Corporate FCU has established and implemented policies and procedures to achieve and maintain appropriate protection of organizational information assets including a data classification procedure defining the proper handling for each data classification level; Secret, Confidential (GLBA), Sensitive and Public.

Human Resources Security

Southeast Corporate FCU has established and implemented policies and procedures to ensure employees, contractors and third party users understand their security responsibilities and are suitable for the roles they will perform. All Southeast Corporate FCU personnel undergo reference/background checks and drug testing at the time of hire.

Physical & Environmental Security

Southeast Corporate FCU has established and implemented policies and procedures to prevent unauthorized physical access, damage and interference to the Corporate's premises and information. Southeast Corporate FCU has deployed a layered security defense with the most sensitive information residing in the inner most layer.

Communications & Operations Management

Southeast Corporate FCU utilizes industry standard guidelines and best practices for the configuration of servers and systems that create, store or transmit secret and confidential – GLBA data. All unnecessary access points and services have been removed or disabled. Logs of critical system operations are created, retained, monitored, and analyzed. Southeast Corporate FCU uses multiple firewall devices and layers to protect servers and databases.

Access Control

Southeast Corporate FCU has established and implemented policies and procedures to prevent unauthorized access to information systems including strong authentication methods requiring a user ID, complex passwords, certificates, mutual authentication and clear desk and clear screen. Only authorized and authenticated users are allowed to access or modify data and only as appropriate to their job function. Applications are protected from unauthorized access through a multi-factor authentication mechanism.

Information Systems Acquisition, Development & Maintenance

Southeast Corporate FCU has established and implemented policies and procedures to ensure that security is an integral part of information systems. New information systems and changes to existing systems or software are reviewed for required security controls. Changes to information systems are controlled by formal change control procedures.

Information Security Incident Management

Southeast Corporate FCU has established and implemented policies and procedures to ensure that information security events and weaknesses are reported in a timely manner to support effective corrective and preventive action as well as appropriate notifications to interested parties.

Compliance

Southeast Corporate FCU has established and implemented policies and procedures to avoid breaches of any statutory, regulatory or contractual obligations as well as security requirements. Corporate management has set a clear policy and direction to conduct security assessments through the Information Security Risk Assessment department and internal compliance audits through the Office of Audit & Compliance. Technical compliance checks are performed through monthly vulnerability and penetration scans of the information assets.

Privacy

While Southeast Corporate FCU is committed to providing our member credit unions with the highest quality service and convenience, we are also committed to our members' privacy. All information gathered during normal business transactions and from visitors to our website is used for internal purposes only and nonpublic information about members will never be given, sold or disclosed in any way to any third party or outside entity; except as permitted or required by law. Southeast Corporate FCU limits the information gathered to that, which is necessary to provide the highest level of service to our members.

For more information – If you have questions about Southeast Corporate FCU's Information Security Management System, you can contact the Information Assurance department at 800-342-0203. The information provided in this disclosure is for informational purposes only and is subject to change in response to changing operational, legislative, regulatory and contractual requirements.

Last updated: October 2008