Wolters Kluwer Financial Services
Information Security Program
September 2013
(Public Version)

Introduction

Information, and the storage and processing of such information within Wolters Kluwer Financial Services (WKFS) are critical components for the livelihood of our business. As a result, information security must be a critical part of the WKFS business environment.

The Gramm Leach Bliley Act (GLBA) requires financial institutions and service providers to develop, implement, and maintain a comprehensive written information security program to protect non-public information about the institution's customers ("Restricted Information"). The program should contain administrative, technical, and physical safeguards appropriate to the size and complexity of the institution, the nature and scope of its activities, and the sensitivity of any customer information issue. WKFS currently has a comprehensive information security program with several coordination roles, procedures, and resources already established.

Objectives

The objectives of this information security program are to protect the confidentiality, integrity and availability of Restricted Information:
 Against any unauthorized access, inappropriate use, or unauthorized change of such information that could result in substantial harm or inconvenience
 Against any threat or hazard to the ability to access the information when required

Program Coordination and Support

WKFS Executive Team has overall responsibility for:
 Overseeing the development, implementation, and maintenance of WKFS' security program
 Approving WKFS' security policies and practices

WKFS Corporate Governance Committee is responsible for:

 Championing security practices at WKFS
 Developing workable information security policies and practices with consideration of the needs of various users, custodians, and owners

 Directing periodic risk assessments to determine the threats imposed on data, to identify potential vulnerabilities that can be mitigated, and to determine if there are areas where security can be improved by technology, procedures, or policies
 Overseeing Incidents and Incident Response Teams
 Receiving, investigating and determining the disposition of violation reports
 Resolving background check issues

WKFS Information Security is responsible for:

 Defining information system security standards, guidelines, procedures, other requirements applicable to the entire organization
 Monitoring the security of information systems
 Providing management with reports about the current state of information system security
 Providing information security training and awareness content to WK HR for delivery to WKFS employees, developers and contractors
 Ensuring WKFS' security requirements are represented to WK's Security Council
 Working in tandem with the WKFS Risk Officer to assess and reduce risk
 Managing external audits

WKFS Incident Response Team (IRT) is responsible for**:**

 Follows incident response procedures when responding to virus infections, potential security breaches, system outages, suspicious activity and similar security concerns
 Defines and classifies incidents
 Develops and maintains Incident Management procedures
 Escalates as necessary to the WKFS Corporate Governance Committee
 Isolates the affected system(s) if required
 Ensures that malicious software is purged from a system and validates that system integrity has been restored following an attack

WK North American Law Department is responsible for**:**

 Provides legal advice on security issues
 Provides record retention schedules
 Participates in an annual review of the information security program
 Provides the interface and protocol for when and how external entities should be involved in a security incident

WKFS Risk Management and Internal Controls is responsible for**:**

 Implementation of a risk management approach and decision support system
 Periodically performing compliance checks to confirm that the information security requirements and policies are being consistently observed

 Coordinating and conducting an annual review of privacy and information security issues and submits a formal report to the Executive Team
 Participating in external audits
 Managing internal audits

Location Contacts at each WKFS facility are responsible for**:**

 Monitoring compliance with Information Security policies and standards
 Monitoring and managing physical security and report incidents
 Providing local incident management support

Policies and Training

WKFS operates under Information Security policies and procedures established by its parent companies. In addition, WKFS provides policies, standards, and guidelines with requirements specific to WKFS.
Currently, WKFS employees and contractors are informed through various media on security and privacy related guidelines, procedures, policies, principles, and other related important statutes. The WKFS internal SharePoint site is a single point of reference for WKFS with external information security resources, project plans, status reports, and opportunities for providing input and feedback.
Minimally, everyone is required to complete corporate training which addresses company's values, business principles, competition/anti-trust laws, anti-corruption and IT security.

Risk Assessment and Safeguards

Facilities Security
WKFS has installed electronic access controls and closed circuit video monitoring at key points in its facilities. In addition, policies and procedures have been established for access by employees, contractors, vendors, and visitors.

Information Classification
All information at WKFS must be classified in one of four categories; Public, Internal, Confidential, or Restricted. Information that is not categorized as Public must be protected in accordance with the rules and procedures set out in the WKFS Data Classification Standard.

Business Continuity and Disaster Recovery
 Established plan for recovery for staff and facilities
 Maintains an off-premises computing recovery site with facilities for ensuring operation of critical business systems
 Data backups are stored off premises

Data Destruction
WKFS has established policies and procedures for the destruction of information according to its classification.

Oversight of Third Parties and Contractors

Specific information security related language must be included in all RFP's and contracts with third parties. In addition, third-party audit reports and vendor management processes ensure proper oversight.

IT Systems

The following technologies are utilized to protect the security of WKFS' systems……..
 Data Loss prevention systems
 Intrusion prevention systems
 Regular vulnerability scanning and penetration testing
 Malware prevention systems
 Steady State monitoring of critical systems
 Virus protection and patch update services
 Virtual Private Network (VPN)