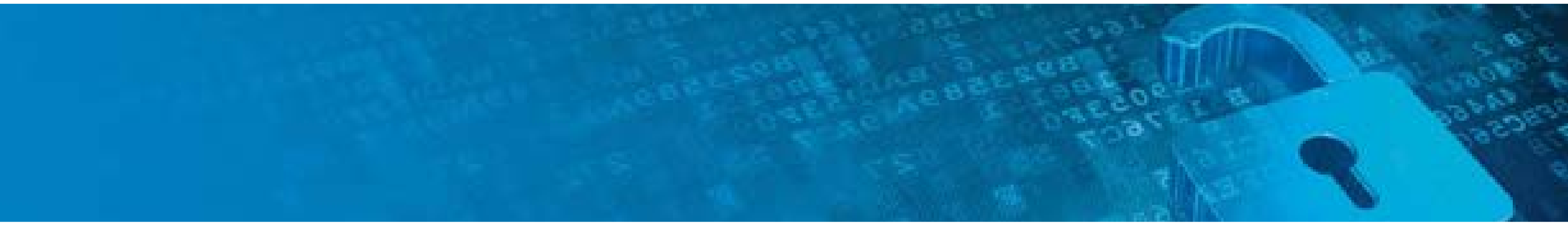
Wolters Kluwer

When you have to be right



Lien Solutions

Security Program Overview

Lien Solutions is committed to safeguarding the confidentiality, integrity, and availability of our clients' data through the implementation of a comprehensive, in-depth security program.

External/Internal Reviews, Audits, and/or Certifications

A SOC 1, Type 2 Audit is performed by RSM US LLP for Lien Solutions products annually. In addition, Wolters Kluwer has implemented an Internal Control Office ("ICO") that performs annual audits of Lien Solutions. The Internal Control Framework ("ICF") is based on the Committee of Sponsoring Organizations of the Treadway Commission ("COSO") framework.

Business Continuity and Disaster Recovery Policies & Procedures

Lien Solutions recognizes the importance of providing continuous, uninterrupted support to our customer base. Lien Solutions has a 24-hour Recovery Time Objective (RTO) and a 4-hour Recovery Point Objective (RPO). Our Enterprise Disaster Recovery and Business Continuity Program is designed to meet these objectives. This program supports Lien Solutions' customer-centric, value-added, mission-critical services. The Lien Solutions Enterprise Disaster Recovery ("DR") and Business Continuity Program adheres to industry best practices for disaster recovery and business continuity services.

The Lien Solutions Enterprise Program includes:

- Oversight through the BCP/DR Steering Committee, sponsored and attended by members of senior management
- Local system recovery e.g. fault-tolerant and redundant system configurations, service center reciprocal agreements
- Data center disaster recovery
- Data replication to standby data center
- Service operations business continuity support
- Business resumption planning
- Pandemic plan

In the event of a temporary outage at our service centers, Lien Solutions' order management and fulfillment functions can be dynamically re-configured to re-route orders to alternate service centers.

Lien Solutions' recovery processes are tested annually. Senior Management is required to identify and approve the testing of specific business recovery scenarios. IT Management is required to support all of the recovery requirements of the approved business scenarios. Test scenarios are coordinated and documented through the use of DR testing and "lessons learned" templates ensuring accurate and consistent testing over a continuous period of time.

3rd Party Management Policies & Procedures

Access to Lien Solutions information or IT resources by external or third parties is a necessary part of business activities. Access may include physical and/or electronic access by customers, product vendors, outsourced data center operators or other managed service providers. In order to control this process, a 3rd party management program has been implemented to ensure that 3rd parties meet their contractual obligations, including but not limited to operational support, security, and business continuity requirements. The program includes initial due diligence and ongoing oversight of our 3rd party relationships.

Human Resource Policies & Procedures

Lien Solutions has a comprehensive set of HR policies and procedures that outline the requirements for employee, confidentiality/non-disclosure agreements, background checks, and termination procedures. Background checks are required for all employees, contractors, and consultants. Part of the termination process includes the returning of all Lien Solutions assets (hardware, software, manuals) and Lien Solutions internal, confidential, and restricted data. Employees are provided with an initial orientation when they are hired to inform them of their obligations.

Physical Security Policies & Procedures

The Lien Solutions Physical Security Program encompasses employee, data, and equipment security, including but not limited to badge access readers, CCTV, fire suppression systems, and supporting utilities. Network and other sensitive equipment are maintained in controlled areas, limiting access to only authorized individuals.

Access Control Security Policies & Procedures

Lien Solutions employs industry best practices as they relate to access controls for systems and data. Unique user IDs and passwords are required for access to Lien Solutions systems and data. Segregation of duties is enforced through a management and resource owner authorization process. A comprehensive backup and recovery strategy is employed for all server level applications and data. Encryption of data is enforced through our applications utilizing HTTPS/SSL.

Data Management Policies & Procedures

Lien Solutions has developed an information classification policy that outlines the required protection measures with respect to the reproduction and destruction of public, internal, confidential, and restricted data. This policy enforces Lien Solutions' commitment to control and protect data (including hard copies of documents) according to specified levels of security and protection.

Intrusion Detection and Incident Response/Notification Policies & Procedures

Lien Solutions enforces the monitoring of key systems and evaluates all security incidents. A corporate-level CIRT team is required to promptly analyze potential security incidents to assess any potential impact, determine if there is an immediate risk to Lien Solutions, and take immediate action to mitigate any potential damage. Local incidents are reported to the corporate level CIRT. Any employee found to have violated approved policies may be subject to disciplinary action, including termination of employment.

Network Security, Penetration Testing and Vulnerability Assessments

Lien Solutions network service agreements include security features, service levels, and management requirements. Firewalls are configured to protect all entry points into the Lien Solutions internal networks. Only approved network staff are authorized to administer corporate firewalls. Firewall policies are reviewed periodically. Remote access to Lien Solutions networks and systems is achieved through a VPN with multi-factor authentication. Network threat protection is deployed on all computers accessing the Lien Solutions network.

Network penetration testing and vulnerability assessments are performed on a recurring basis to ensure the security of Lien Solutions' products and services.

Software Product Development Methodology

Lien Solutions combines several processes and practices to provide an effective software product development methodology. From a process perspective, new development is based on the Scrum development framework which has been shown to reduce project risk through its focus on short, iteration cycles and frequent customer collaboration. The process framework is complimented with various technical practices such as test-driven development, test-automation, secure coding/scanning practices and adherence to object-oriented principles and design patterns coupled with regular code reviews.

The methodology ensures managed, incremental enhancements and bug fixes achieving availability and quality targets.

Quality Assurance and Quality Control

Lien Solutions is committed to a quality assurance and testing program that makes quality a fundamental and integral business principle. The strategy is based on customer satisfaction achieved by meeting our internal and external customer requirements. Conformance to our customer's requirements and expectations is the responsibility of all Lien Solutions employees. The quality assurance and testing program procedures and practices are developed, reviewed, and revised with the continuous participation of Lien Solutions employees. In addition, quality controls are built-in elements of Lien Solutions applications adding value to the overall user experience. The goal of the Lien Solutions quality assurance and testing program is to ensure the continued improvement of our products in support of our customers and employees.

Change Management Policies & Procedures

Lien Solutions employs a formal change management process to ensure a full life cycle for all changes, deployed to any IT environment, reducing impact to internal and external customers. The change management process ensures minimum disruption to IT services- risks to the production system are identified, assessed and managed, and changes are scheduled and approved for release through designated maintenance windows.

Contact information:
Wolters Kluwer
2929 Allen Parkway, Suite 33
Houston, TX 77019
713.533.4600 tel
713.942.7847 fax

Please visit **www.liensolutions.com**
for more information.