LIAISON

Information Security Policy

General Security

Introduction

Liaison International LLC (“Liaison”) continuously implements technological solutions and network innovations to increase efficiency and better serve our customers. To guard against security breaches and minimize exposure to risk, Liaison has developed this information security policy of supporting standards and procedures (the “Information Security Policy”).

The information security policy applies to employees, consultants, contractors, temporary employees, vendors, third-party partners, and all others who have access to Liaison systems and client information. Liaison is responsible for revising, updating, and redistributing the information security policy when appropriate. It is the responsibility of Liaison’s information security team to ensure that the information security policy is maintained and communicated to, and followed by, all employees, consultants, contractors, temporary employees, vendors, third-party partners.

Each new employee will receive a copy of the information security policy. Each new employee must sign the information security policy, which will be placed in the employee’s personnel file. Contractors, consultants, and temporary help must review and comply with the information security policy and subsequent policies as a condition of any contract.

Purpose

This information security policy defines the technical controls and security configurations users and information technology (IT) administrators are required to implement in order to ensure the integrity and availability of the data environment at Liaison, hereinafter, referred to as the practice. It serves as a central policy document with which all employees, consultant, contractors, temporary employees, vendors and third-party partners must be familiar, and defines actions and prohibitions that all users must follow. The information security policy provides employees, consultant, contractors, temporary employees, vendors and third-party partners with guidelines concerning the acceptable use of practice technology equipment, e-mail, internet connections, voice-mail, facsimile, future technology resources and information processing.

The policy requirements and restrictions defined in this document shall apply to network infrastructures, databases, external media, encryption, hardcopy reports, films, slides, models, wireless, telecommunication, conversations, and any other methods used to convey knowledge and ideas across all hardware, software, and data transmission mechanisms. This policy must be adhered to by all practice employees or temporary workers at all Liaison locations and by contractors working with the Practice as subcontractors.

Policy/Procedures

All employees including contractors, contractors, temporary employees, vendors and third-party partners who process, store, transmit, or otherwise use confidential personal information entrusted to Liaison are required to notify immediately the information security team in the event of a suspected or actual breach of the confidentiality of such information.

Personal information that is lawfully available to the public from a government record is not subject to this breach notification policy. In addition, personal information rendered unreadable to an unauthorized party through use of encryption is not subject to this breach notification policy. Accordingly, all computers and other electronic data storage devices on which confidential personal information may reside must be encrypted.

Personnel Security

Non-Disclosure and Confidentiality Agreements

Employees and contractors are required to sign a non-disclosure or confidentiality agreement prior to accessing Liaison's protected information assets.

Background Checks

Liaison's Human Resources team performs standard background checks on all employee candidates prior to employment

Training and Awareness

Liaison employees and, where relevant, third party users, receive appropriate training and regular updates in organizational policies and procedures. This includes security requirements and education, legal responsibilities, business controls, as well as training in the correct use of information processing facilities (e.g., log-on procedures) and use of software packages.

Physical Security

Visitors

Visitors to secure areas at Liaison's various locations are supervised or cleared by an appropriate Liaison employee and the date and time of entry and departure are recorded. They are only granted access for specific, authorized purposes, and are supervised during their visit.

Access to Sensitive Areas

Physical security for customer facing systems is controlled by Liaison's Data Center provider, AT&T. Access to AT&T's AEHS SOC 1 compliant IDC (Internet Data Center) is limited to AT&T support staff and authorized customer representatives only. Access to the AT&T Data Center is very tightly controlled by on-site security and can only be granted to authorize customer representatives with a photo ID. Access to the data center floor is restricted and controlled via ID badges. Additionally, Liaison's equipment is kept in locked server cabinets only accessible via an ID badge.

Network Security

Liaison utilizes the industry standard technology in firewalls and network security. Liaison's information security team enforces a least-privileged model of network traffic, allowing only required traffic to traverse the firewalls. Periodic reviews of firewall configurations are performed with any discrepancies identified and reported to security management for timely remediation

Account Security

Access to all information systems is controlled via an assigned username/password, and is granted on a "need to know" basis. Primary user accounts have system-enforced limits on minimum password length, maximum age, and level of complexity. In addition, accounts are automatically locked after five unsuccessful login attempts. User accounts are removed promptly upon a users' termination. This process is outlined in the "Procedure for Termination of an Employee" policy.

All accounts are monitored for unauthorized access. All accounts follow security guidelines and have access limited to their immediate needs.

Encryption

Transit

To protect sensitive information as it is transmitted across network infrastructure, Liaison uses a combination of secure protocols, including SSL, SSH, and SFTP where appropriate. Liaison's policy is to support and comply with customer requirements and to implement controls designed to permit customers the transmission of sensitive data across trust zones using appropriate encryption protecting confidentiality and integrity.

Laptops Security

To help mitigate potential data exposure or data loss from electronic storage devices such as laptops and hard drives, Liaison incorporates strong password controls and full-drive encryption on laptops. In the event that one of our devices is either lost or stolen, the data is protected with AES 256-bit industry-standard encryption.

Communications and Operations

Data Transfer Standards and Requirements

Data transfers related to client data must be encrypted. By default, Liaison does not allow clear text or unencrypted data communication protocols. SSH, SFTP, SSL, and IPsec communications are required for administrative duties.

End Point Security Workstations and Servers

Liaison uses a layered approach to protecting our information assets from viruses and malicious software. We implemented scanning technology to protect email, and operating systems.

Physical Penetration Assessments

Liaison’s information security team conducts periodic physical security reviews of Liaison’s physical facilities on a periodic basis. High-risk items are addressed in a timely manner.

Device Decommissioning

Liaison laptops, desktops and servers that exceed their useful life are securely wiped in our decommissioning process. The entire drive is over-written using industry-standard methods, which render any previous data unrecoverable. Devices, which may have contained client data used to power Liaison’s services, are securely destroyed or undergo secure deletion of data similar to those outlined in NIST 800-88.

Firewalls

Liaison utilizes the industry-leading technology in firewalls and network security. Liaison’s information security team enforces a least-privileged model of network traffic, allowing only required traffic to traverse the firewalls. Periodic reviews of firewall configurations are performed with any discrepancies identified and reported to security management for timely remediation.

Intrusion Detection Systems

Liaison has implemented both preventative and detective controls to protect data. World-class firewall infrastructure and monitoring solutions are in place to prevent and alert Liaison’s information security and IT teams to threats to data confidentiality, integrity, and availability.

Log Management and log retention

System, application, and security logs generated by servers and other network and security devices, including applications, databases and file activity logs whenever available or deemed necessary are centralized and retained for a period of time.

Systems Development and Maintenance

Patch Management

Liaison production systems are built with the most up to date security patches and software versions at installation. New software versions and patches are tested in our test and QA environment prior to deployment in production. Software patches are applied when they can help to remove or reduce security weaknesses. Liaison's process of code deployment, includes the automated installation of all new or outstanding security patches and hot-fixes, which helps Liaison maintain current security posture within the production environment.

Operating System Hardening

Production systems are built from pre-configured and hardened images reviewed and approved by Liaison's information security team. Approval requires adherence to Liaison's documented minimum baseline security configuration standards.

Application Security Code Review

Code reviews are performed as part of our Systems Development Life Cycle prior to implementation. Liaison incorporates appropriate peer review and automated security testing in development and QA processes. Liaison's training and awareness program helps to encourage secure programming practices, including secure input/output handling, and awareness of OWASP top 10 items

Business Continuity/Disaster Recovery

Liaison's critical systems are automatically backed-up on a nightly basis. Back-ups are stored in multiple on-line distributed data centers. In the event of a restoration event, Customer data can be quickly retrieved from current back-ups and installed on readily available systems as appropriate. Liaison's backup process can be adjusted to take more frequent backups as necessary to support client needs or policies. The data center facility itself is equipped with redundant network connections, battery backup power and line conditioning, diesel generators, redundant A/C systems, redundant humidity controls, and fire suppression systems.

Additional Controls`

Risk Identification and Profiling

Liaison incorporates various methodologies in the risk identification process, including technical assessments, threat and vulnerability assessments. Liaison conduct internal and external information security assessments of both client-facing applications and our corporate infrastructure. Risks identified through any method are prioritized and recorded for management review. Managing a risk inventory process helps the information security team prioritize the efforts of Security, development, monitoring, QA, and Operations teams and tune the execution of the information security strategy and roadmap.

Security Policy Implementation

The Security Policy establishes the controls necessary to protect electronic information and physical environments. It is important that all users know and follow the information security policy and its procedures.

Failure to follow the information security policy, either inadvertently or intentionally, may subject an employee to corrective action, up to and including the termination of employment. When appropriate, third parties should also be made aware of and required to adhere to the information security policy and its procedures.

It is important to continuously assess and follow the information security policy within all functional areas of Liaison and at any other facility in which information is stored, processed, or transmitted. All users shall receive and read the relevant portions of the information security policy and should understand the policies relevant to their roles prior to obtaining access to information systems. Thereafter, users will be required to periodically review the information security policy.

Policy creation date	**Last updated**	**Created by**	**Reviewed by**	**Signed off by**
6/15/2015	6/15/2015	Belkacem Abdessemed Security Manager	Naeem Taj Director of IT and IS	Jim Pluntze CFO

To Contact The Information Security Team:
Email: informationsecurity@liaison-intl.com
Telephone: 617-612-2000 x4357
www.liaison-intl.com