Information Security Key Elements

for

iRunway

Information Security

May 31, 2010

Public

Contents

1 Introduction

In light of the paramount importance of data security in the service line of Intellectual Property, iRunway India Pvt. Ltd has an ethical obligation and a legal and official mandate to protect the sensitive personal and business information it handles. Therefore, iRunway implements all necessary controls to ensure that clients' as well as its own data is secured from any unauthorized access. All the security measures are focused on the following three criteria:

1. **Confidentiality:** No data or information shall be disclosed to any person within or outside the organization, other than the persons who are authorized to use that data.
2. **Integrity:** No data/information or programs shall be allowed to be modified by anyone without proper authority.
3. **Availability:** All Information Systems including hardware, communication networks, software applications and the data they hold shall be available to users at all times to carry out business activities.

The iRunway security standards are based upon recommendations given by 'Earnst & Young' and are in line with the **'ISO 27001: 2005'** standards.

The key elements of the information security controls at iRunway are discussed in the next section of this document.

2 Key Elements of Controls for Information Security

2.1 Physical Elements

- A physical security system is in place with a 24X7 security guard and surveillance cameras.
- Highly confidential work is carried out in separate, isolated, secure zones. Access to these zones in the office is restricted by proximity cards and biometric access system.
- Use of camera devices (camera phones etc.) is not allowed inside the office. Personal memory devices (USB ports, CDs etc.) are also not allowed.
- All network activities pass through the company's firewall and proxy gateway server.
- All sites offering offensive or indecent contents are not accessible. URLs of web based emails are blocked.
- Downloading of certain type of files (viz. *.exe, *.mp3, etc.) is blocked.
- All the access rights given to an employee are revoked on the day he/she leaves the organization.
- Each terminal has a legal caption saying "No one shall use any iRunway computer or network facility without proper authorization. No one shall assist in, encourage, or conceal from authorities any unauthorized use, or attempt at unauthorized use, of any of the iRunway's computers or network facilities."
- All data transmitted from iRunway operations environment to a client is encrypted (on client's demand). As such, appropriate encryption technology and algorithms are used. The same applies for all confidential or restricted information being carried out of the office. Access to the encryption software is regulated.
- Every user takes appropriate steps to back up all data on his/her machine by maintaining on the server a copy of all important documents on his/her computer.
- All the data on the file server is backed up regularly and a copy of backup is stored at an off-site location. A corresponding chain of authorization is maintained for data recovery and backup restoration.
- A backup is performed for the email server on a daily basis.
- Visitors are briefed about security measures and are escorted at all times while inside the office.
- Printouts of client-confidential material can be taken only when it is necessary and only after proper approval from the management. Any such document is shredded when it is not required.
- No papers/media is taken in/out of the office without approval from management.
- No discussion about any project is done outside the office.
- Appropriate fire fighting equipments are kept in the office and employees are trained for such incidents.

2.2 System Elements

- All emails are scanned by an antivirus.
- A good virus and malicious software detection solution is installed at all possible entry points for virus or malicious software. The software is updated on a regular basis. Virus scans are done on a regular basis on each system and each diskette being used.
- Appropriate measures are taken to remove the infected files, isolate the infected system from other systems in the organization and safe recovery of all the data from the infected systems.
- Each terminal is password protected and gets automatically locked if left idle for five minutes. Each user locks his/her terminal before leaving it. Passwords are of minimum 8 characters and must contain at least one alphabet, one numeral and one special character.
- All user passwords and other critical passwords are changed regularly.
- All the user machines have a user account and an administrator account. All the configuration changes are done through the administrator account only password of which is known only to the IT Operations team.
- User accounts inactive for a specific period of time are disabled e.g. when a person goes on a long leave, his/her account is disabled.
- USB ports and CD Drives are disabled in all the user machines to avoid any unwanted data transfer and virus infection through such devices.
- The user terminals are not configured for any type of LAN sharing. Any sharing of data is done only through a central file server to avoid any virus spread over the network.
- Access to various system utilities and data (i.e. privilege management) is controlled so that a user does not have more information than what is necessary for him/her to do his job.
- Network activities by users are logged. Similarly, all activities at the terminals or by the user accounts are also logged and reviewed randomly.

2.3 Process Elements

- Any information stored or generated in iRunway is given a confidentiality rating and appropriate measures are taken to make sure that it is accessible to only those who are authorized to do so. Integrity of a document is always maintained.
- 'Service Level Agreement' and 'Non-disclosure / Confidentiality Agreement' are signed with all the employees and vendors/third parties in all cases where an employee or a third party is given access to any sensitive information.
- Formal agreements regarding 'Exchange of Information' are established for all critical business information with both outside organizations and employees of the company. These agreements include both physical and electronic exchange, reflect the sensitivity of the information, and outline any protection requirements. It also identifies management responsibility, encryption requirements, etc.
- The teams working for a particular client are bound by "Chinese Walls".
- An IT Operations team is formed for handling and managing all software and hardware functionalities e.g. installing software and its updates, manage all the databases, etc. Similarly, teams are in place to monitor the usage and status of non-IT equipments in the office.
- A detailed list of all the software and their usage is maintained. The list has the name of the software, vendor's name, serial key for installation, version number, hardware on which it is installed, total number of installations, warranty period and any documentation associated with the software. A similar list is maintained for all the hardware in the company.
- A proper segregation of duties for all operational procedure is implemented. Where segregation is not possible, proper monitoring and review of all activities is done.
- A log entry for everybody is maintained. The log encompasses all user activity, faults in the system, photocopy or printout, etc. All user activities are logged on to a system and are continuously monitored.
- All log data can be accessed by authorized personnel only and it is reviewed on a regular basis.
- iRunway has requisition forms for different purposes (e.g. access to file server, access to secured zone or for creation of a new user account etc.). These requisition forms are used for making such request and a proper action is taken only upon approval from management. All such actions are recorded.
- A formal procedure is maintained for executing and monitoring the changes to information security policies.
- Operating Procedures for all the activities are developed, documented and maintained for all IT processes.
- Extensive Training is provided to all the members of the organization regarding information security and the measures to be followed.
- Extensive background checks are conducted for the new joiners.
- Any problem related to network which might lead to delay or stopping of business activities is treated as an "Incident". An 'Incident Management Committee' takes appropriate actions in case of an incident.
- Continuity of work is ensured in case of a major incident causing a disruption in the work. A business continuity plan is in place for such potential incidents.
- Teams are formed and responsibilities are assigned to individuals to ensure compliance with the information security policies and procedures.
- Information security is reviewed by the Information Security Core Group periodically and necessary changes are done to ensure that it is up to the industry standards.
- Periodic audits are conducted in the organization to ensure compliance with the information security measures in the organization.

United States

Texas
Barton Oaks Plaza One, Suite 300,
901 S Mopac Expressway,
Austin, TX 78746
Tel: +1 512 329 2765

California
Suite 200,
530 Lytton Avenue,
Palo Alto, CA 94301

India

iRunway India Pvt. Ltd.
First Floor, AMR Tech Park I
Annex, No. 23 and 24,
Hongasandra, Hosur Road,
Bangalore – 560068

Phone: +91 804 058 4000
Fax: +91 804 058 4010

The preparers of the information in this document are not engaged in rendering legal or other professional advice, and nothing in this document should be construed as such. iRunway exists to provide technical research, analysis and reporting capability to its clients.

iRunway never makes determinations that would require applying laws to any specific set of circumstances. Our clients are strongly encouraged to seek licensed counsel to provide legal interpretations and courses of action based upon the technical information that we have provided hereunder.