Information Security Policy Document

iDisha Info Labs Pvt. Ltd.

7/1/2019

Change History

Date	Author	Version	Change History
June 1st, 2019	Vishal Lavti	0.1	Creation of the policy document
June 12th, 2019	Shobhana Sriram	1.0	Final document

Table of Contents

1. Introduction

This Policy Document encompasses all aspects of security surrounding confidential company information. All iDisha info Labs Pvt. Ltd. employees are required to read this document in its entirety and sign the form confirming they have read and understand this policy fully. This document will be reviewed and updated by Management on an annual basis or when relevant to include newly developed security standards into the policy and distribute it all employees and contracts as applicable.

2. Information Security Policy

iDisha Info Labs Pvt. Ltd. commits to respecting the privacy of all its customers and to protecting any data about customers from outside parties. The company and management are committed to maintaining a secure environment in which to process personal information so that we can meet these promises. Employees handling customer data should ensure:

- Limit personal use of the Company information and telecommunication systems and ensure it doesn't interfere with your job performance;
- The Company reserves the right to monitor, access, review, audit, copy, store, or delete any electronic communications, equipment, systems and network traffic for any purpose;
- Do not use e-mail, internet and other Company resources to engage in any action that is offensive, threatening, discriminatory, defamatory, slanderous, pornographic, obscene, harassing or illegal; Do not disclose personnel information unless authorized;
- Keep passwords and accounts secure;
- Request approval from management prior to establishing any new software or hardware, third party connections, etc.;
- Do not install unauthorized software or hardware, including modems unless you have explicit management approval;
- Always leave desks clear of sensitive cardholder data and lock computer screens when unattended;
- Information security incidents must be reported, without delay, to the individual responsible for the security as mention in reporting section below in this document.
- We each have a responsibility for ensuring our company's systems and data are protected from unauthorized access and improper use.

If you are unclear about any of the policies detailed herein you should seek advice and guidance from your line manager.

3. Acceptable Use Policy

All iDisha employees should follow AUP as outlined below:

- Employees are responsible for exercising good judgment regarding the reasonableness of personal use.
- Employees should ensure that they have appropriate credentials and are authenticated for the use of technologies
- Employees should take all necessary steps to prevent unauthorized access to any confidential data.
- Keep passwords secure and do not share accounts.
- Authorized users are responsible for the security of their passwords and accounts.
- All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature.
- Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

4. Physical Security

All the company assets like workstation, printers, modem, documents and building access must be protected to prevent unauthorized access. Below are the guidelines with respect to physical security:

- Access to sensitive information in both hard and soft media format must be physically restricted to prevent unauthorized individuals from obtaining sensitive data.
- Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts.
- Media containing sensitive cardholder information must be handled and distributed in a secure manner by trusted individuals. Media is defined as any printed or handwritten paper, received faxes, floppy disks, back-up tapes, computer hard drive, etc.
- Visitors must always be escorted by a trusted employee. A “visitor” is defined as a vendor, guest of an employee, service personnel, or anyone who needs to enter the premises for a short duration, usually not more than one day.
- Access to any company asset to a visitor should be approved by management in advance.
- Employees should ensure that they have appropriate credentials and are authenticated for the use of technologies
- Employees are responsible for exercising good judgment regarding the reasonableness of personal use.

5. Internet Usage

All Employees shall have access to internet to perform business related activities Individual Internet usage is monitored, and if an employee is found to be spending an excessive amount of time or consuming large amounts of bandwidth for personal use, disciplinary action will be taken.

Here are the guidelines which must be followed by employees of iDisha Info Labs Pvt. Ltd:

- The Internet access provided should not be used for entertainment, listening to music, viewing the sports highlight of the day, games, movies, etc.
- Do not use the Internet as a radio or to constantly monitor the weather or stock market results.
- Software cannot be downloaded from internet. All software requirements must be communicated to administrator who would procure the license after obtaining necessary approvals.
- Employees are required to adhere to OSS policy and any use of OSS must be approved by CTO of the company.
- Employees may not install or download any software (applications, screen savers, etc.). If employees have a need for additional software, the user is to contact their supervisor;
- Any employee visiting non-business related sites will be disciplined and may be terminated.

6. Transfer of Sensitive/Confidential Information

When confidential or sensitive information from one individual is received by another individual while conducting official business, the receiving individual shall maintain the confidentiality or sensitivity of the information in accordance with the conditions imposed by the providing individual. All employees must recognize the sensitive nature of data maintained by the Practice and hold all data in the strictest confidence. Any purposeful release of data to which an employee may have access is a violation of Practice policy and will result in personnel action, and may result in legal action.

7. Password Policy

7.1 User Logon IDs

Individual users shall have unique logon ids and passwords. An access control system shall identify each user and prevent unauthorized users from entering / using information resources. Security requirements for user identification include: Employess shall be responsible for the use/misuse of their individual logon id.

7.2 Password Policy

User ids and passwords are required in order to gain access to all system workstations.

- Password length must of at least 6 characters.
- The password must contain a combination of upper and lower case alphabetic characters, numeric characters, and special characters.
- Password must be changed every 90 days.
- Passwords shall not be shared, or written down on paper, or stored within a file or database on a workstation, and must be kept confidential.
- Passwords are stored in an encrypted format.

8. Reporting Process

8.1 System Malfunctioning

All employees should inform the administrator when the software does not appear to be functioning correctly. The malfunction - whether accidental or deliberate - may pose an information security risk. Below these steps should be taken immediately:

- Stop using the computer
- Do not carry out any commands, including commands to <Save> data.
- Do not close any of the computer's windows or programs.
- Do not turn off the computer or peripheral devices.
- If possible, physically disconnect the computer from networks to which it is attached.
- Inform the administrator as soon as possible with details of unusual behavior of the computer (screen messages, unexpected disk access, unusual responses to commands) and the time when they were first noticed.
- Write down any changes in hardware, software, or software use that preceded the malfunction.
- Do not attempt to remove a suspected virus unless authorized. This would be addressed by administrator with careful analysis.

8.2 Security Incident Reporting

Employees are to formally report all security incidents or violations of the security policy immediately to their immediate supervisor, or to their department head. Any security incident must be reported immediately to below personnel.

Level	Name	Role
1st	Mohammed Khizer	Administrator
2nd	Shobhana Sriram	CTO
2nd	Vishal Lavti	VP –Engineering
3rd	KNM Rao	CEO

9. Disciplinary Action Violation

Violation of the standards, policies and procedures presented in this document by an employee will result in disciplinary action, from warnings or reprimands up to and including termination of employment. Claims of ignorance, good intentions or using poor judgment will not be used as excuses for non compliance.