INDOSWIFT SAFE AND SECURE DATA SECURITY MEASURES

Indoswift ensures that all the information it shares with its clients in the form of audio/video or text must be secure. We ensure that we regularly update our security measures with the latest technological developments in the cyber world. At Indoswift, data security is an important area of concern and we adhere to stringent steps, detailed below:

1. **Usage of strong passwords**

Indoswift has adapted a strong policy of using the passwords, which is the basic thing we do to strengthen data security. Our passwords are real hard to crack as we use a combination of capital and lower-case letters, numbers, and symbols and keep them 8 to 12 characters long. We avoid using any personal data (such as birth date), common words spelled backwards and sequences of characters or numbers, or those that are close together on the keyboard. We change the passwords every 90 days or earlier.

2. **Putting up of strong firewall**

In order to ensure that our network is properly protected, we have firewalls in place to ensure that our network is protected by controlling internet traffic coming into and flowing out of our system. We use McAfee firewall.

3. **Antivirus protection**

We do have installed McAfee antivirus and anti-malware software to protect the last line of defence from an unwanted attack to our network.

4. **Regular update of installed programs**

To make sure our computers are abreast with latest updates, we keep our security applications updated with recent updates. At Indoswift, we understand that updates are highly important to protect your data and do not ignore this fact.

5. **Monitor diligently**

The network is updated with monitoring tools or in other words data-leakage prevention software, which is set up at key network touchpoints to look for specific information coming out of internal network, if any. It is configured to look for any bit of information relevant to the business that would indicate a breach.

6. **E-mail, IM and surfing the Web**

Internet access to the computers is restricted to the extent that staff can only view secure HTML pages and pre approved websites on their computers with limited access to some relevant web pages only. Our staff is not permitted to upload or download any of the file(s) on their respective PCs. The hardware lock is in place. Emailing from personal nodes, chatting through any IM, is strictly prohibited and the administrator ensures that any IM software is not installed on their PCs. We have also installed various networking tools, which let us know the work log each computer including time frames.

7. Securing laptops

Being laptops are portable in nature, they are at a higher risk of being lost or stolen. It's important to take some extra steps to make certain that the data is protected. Though, only managers are authorised and provided the laptops and they are not allowed to keep the transcription data on the hard drives. We use encryption software to make sure that the information can't be read out without the correct password.

In our routine office meetings, we stress the importance of handling the laptops including never leaving the laptop in the car, taking them to the restaurants, etc.

8. Regular Backups

We have scheduled regular backups to an external hard drive to ensure that all the data is stored safely.

9. Employee Education

We believe in teaching the employees about safe online habits and proactive defence. Educating the employees about what they are doing and why it is dangerous is a more effective strategy than expecting the IT security staff to constantly react to end users' bad decisions. We train our employees regularly and make sure that employees understand how important the company's data is, and all the measures they must take to protect it.

10. Physical Surveillance

Every inch of our premise is being monitored by CCTV and we keep the recording back up of three months. Mobile phones are prohibited in the production areas. Electronic equipments are installed at the entry and exit points.

11. Others:

- File transfer via 128 bit encryption based platforms.
- Developing educational/training systems to train Techno Legal Compliancy to the Managers and Supervisors.
- Trail of accountability in case of any legal issues.

- Most of the hiring is through referrals from current employees, which helps us in getting people whose credentials, can be easily verified.
- Employee checks from university records to the last employment.
- Signs non disclosure agreements with clients whenever required.