CONFIDENTIAL INFORMATION POLICY

TEKSER TOURISM AND TRAVEL INC.

Contents

Appendix

Introduction

In the course of business certain information; its storage, disposal and the controls governing its access and use is designated as confidential.

It is recognized that information designated as high-risk can be used for the purpose of identity theft and any information, if maliciously obtained and misused, carries a high risk of causing personal, financial, and reputational damage to its owner.

This policy outlines the approach taken by Tekser Tourism and Travel Inc. in relation to confidential information and is implemented through the accompanying *'Confidential Information Employee Declaration Agreement'*

Definition

This policy works on the principal of two definitions of confidential information: High Risk Confidential Information and Business Information in electronic or paper form.

High Risk Confidential Information (HRCI)

This information is classified as high risk because exposure could result in direct harm to an individual, business or organization; or it is specifically designated as information protected under an agreement or contract. Examples of such information are: credit card details, passport details and any other personally identifiable information

Business Confidential Information

This is any information specifically designated as confidential by Tekser Tourism and Travel Inc. or any of their clients or contractors in the course of business. Examples of such information are: contracts and agreements, client databases and all forms of databases maintained as a business tool, financial or accounting records.

Storage of High Risk Confidential Information

Tekser Travel and Tourism Inc. recognize responsibility to secure information stored, accessed, or shared by protecting storage of information and systems, and complying with any policies and procedures for use of those systems.

No employee of Tekser Tourism and Travel or any vendor is permitted to store HRCI on any individual personal use computer or portable storage device.

The following means of securing storage of high risk information will be considered where appropriate

- Encrypting all laptops, portable storage, and network connections used with confidential information.

- Protecting systems/servers used to access confidential information through the use of firewalls, virus scanners, and regular software updates.
- Using individual accounts, not sharing account information, and choosing strong passwords.
- Attaching only approved devices to the Tekser Tourism and Travel network.
- Disposing safely of confidential information through the use of approved, secure file-deletion and disk-cleaning tools
- Not sharing confidential information with people who are not approved to access it.
- Having an approval process for accessing information
- Non-electronic records containing high-risk confidential information are kept within locked storage areas, cabinets or containers except when in use.
- Where practicable, a 'clear desk' policy is maintained to ensure non-electronic (paper) records are removed from open view and securely stored when not in use.

Breach of Information

All employees of Tekser Tourism and Travel Inc. are informed, notify and agree as their own individual responsibility to immediately report to their department manager, general manager or human resources representative; if it becomes known or suspected that Confidential Information is been acquired or used by an unauthorized person for an unauthorized purpose.

Reportable breaches of information may include:

- Unauthorized access to a system that stores confidential information.
- Loss or theft of a system or a physical record that contains confidential information,
- Cases where computers have been hacked or compromised.
- Lost or stolen passwords compromised.

Target System Controllers

Systems containing HRCI could be of interest to hackers and as such may need special protections to include:

- System on private address space – locally firewalled – annual vulnerability testing done.
- Such systems should only be connected to the network if the is a business requirement and physical or virtual systems should be dedicated to a specific purpose rather than being shared by multiple applications.
- The firewalls should block all unneeded inbound and outbound traffic and only enable administrative access from those computers that are used by the system administrators

- All administrative access to such systems should be logged, logs should also be maintained of the activities of administrative users on the systems

Disposal and Destruction of Confidential Information Records

Physical or electronic records containing confidential information must be correctly disposed of so the information cannot be retrieved.

Most records are not kept permanently unless in the case of accounting records there are local law requirements, which Tekser Tourism and Travel is bound by.

Retention periods so far as client HRCI will be assessed on a case by case basis depending on the business need to hold such information. A 'Retention Period' is specified as the minimum period for which a record is retained before it is: transferred for archive or destroyed/deleted as soon as possible after the minimum required retention period.

The following guidelines will be used for disposal or destruction.

Paper Media Documents:

Shall be shredded or destroyed in such a way that the information contained on the paper media cannot be practically read or reconstructed. Tekser Tourism and Travel has a crosscut paper shredder for this purpose.

Electronic Media Documents:

Shall be destroyed or erased so that information cannot be practically read or reconstructed. This also includes electronic media stored on lap tops or personal computers when they are to be disposed of in any way, using a secure disk erasure application or physically destroying it.

Just removing a file or document in a computer does not mean it is destroyed or deleted since the data in the file is not actually removed from the disk. Applications that provide secure erasure from the disk are to be used. These applications are available for Windows and Mac computers.