Equity Express

- INFORMATION TECHNOLOGY
- CVGRL – IT
- Data Privacy and Protection Policy

Equity Express

Overview

All employees and person that have access to organizational data must adhere to the IT Data Privacy Policy defined below in order to protect the security of the data, protect data integrity.

Goal of the Data Privacy Policy

The goal of the IT Data Privacy is to ensure that the…

a. Confidentiality,

b. Integrity

c. Availability

d. Security

Of each piece of information owned by or entrusted to Equity Express is protected in a manner that is consistent with…

a. The value attributed to it by the Organization,

b. The risk the Organization is willing to accept and

c. The cost the Organization is willing to pay Wherever it resides, i.e.:

d. On printed media (e.g., forms, reports, microfilm, microfiche, books),
e. On computers,
f. On networks,
g. On magnetic or optical storage media (e.g., hard drive, diskette, tape, CD),
h. In physical storage environments (e.g., offices, filing cabinets, drawers),
i. In a person's memory, etc.

Purpose

The purpose of this document is to define the principles to which all employees and staff must adhere when handling information owned by or entrusted to Equity Express in any form. The principles cover the following areas:

a. Defining the confidentiality, integrity and availability requirements for information used to support the Organization's objectives,

b. Ensuring that those requirements are effectively communicated to individuals who come in contact with such information, and

c. Using, managing and distributing such information – in any form, electronic or physical - in a manner that is consistent with those requirements.

This policy describes in general terms the Information Security Policy of the Organization, which is also embodied in various policies developed by the guardians of specific information.

Definition of Data privacy violation

A data breach is an incident in which sensitive, protected or confidential data has potentially been stolen or used by an individual unauthorized to do so. Data breaches may involve personally identifiable information (PII), trade secrets or intellectual property.

Summary of Personal Responsibilities

While much of this policy document focuses on our legal obligations and the process of determining and communicating the sensitivity of information owned by or entrusted to the Organization, it also contains a number of requirements to which anyone who handles such information must adhere. In summary:

a. You are responsible for your use or misuse of confidential information.

b. You must not in any way divulge copy, release, sell, loan, review, alter or destroy any information except as properly authorized within the scope of your professional activities.

c. You must take appropriate measures to protect confidential information wherever it is located, e.g., held on physical documents, stored on computer media, communicated over voice or data networks, exchanged in conversation, etc.

d. You must safeguard any physical key, ID card or computer/network account that allows you to access confidential information. This includes creating computer passwords that are difficult to guess.

e. You must render unusable confidential information held on any physical document or computer storage medium (e.g., diskette, CD, magnetic tape, hard disk) that is being discarded.

f. You must report any activities that you suspect may compromise confidential information to your immediate supervisor or to the Organization IT Security Officer.

General Principles

Accountability

All information gathered and maintained by employees of Equity Express for the purpose of conducting Organization business is considered institutional information and, as such, each individual who uses, stores, processes, transfers, administers and/or maintains this information is responsible and held accountable for its appropriate use

Information Collections and the Responsibilities of Information Guardians

Organization information must be protected against unauthorized exposure, tampering, loss and destruction, wherever it is found, in a manner that is consistent with applicable laws and with the information's significance to the Organization and any individual whose information is collected. Achieving this objective requires that Organization information be segregated into logical collections (e.g., Customer personal documents, employee benefit data, payroll data, personal data regarding, and financial records), and that each collection be associated with an individual known as an "Information Guardian" who must…

1. Define the collection's requirements for confidentiality, integrity, availability and security.
2. Convey the collection's requirements in writing to the managers of departments that will have access to the collection,
3. Work with Office Heads to determine what users, groups, roles or job functions are authorized to access the information in the collection and in what manner (e.g., who can view the information, who can update the information).

The guardian of a logical information collection is typically the head of the department on whose behalf the information is collected or that is most closely associated with such information. Each Information Guardian may designate one or more individuals on his or her staff to perform the above duties. However, the Information Guardian retains ultimate responsibility for their actions.

Responsibilities of Office Heads

Office Heads are required to:

1. Understand the security-related requirements for the information collections used within their respective departments by working with the appropriate Information Guardians and their designates.
2. Develop procedures that support the objectives for confidentiality, integrity, availability and security defined by the Information Guardians and designate, and ensure that those procedures are followed.
3. Effectively communicate any restrictions to those who use, administer, process, store or transfer the information in any form, physical or electronic.
4. Ensure that each staff member understands his or her information security-related responsibilities and acknowledges that he or she understands and intends to comply with those requirements.
5. Report any evidence that information has been compromised or any suspicious activity that could potentially expose, corrupt or destroy information to the Organization IT Security Officer.

User Responsibilities

a. Protecting Information Wherever It Is Located

Each individual who has access to information owned by or entrusted to the Organization is expected to know and understand its security requirements and to take measures to protect the information in a manner that is consistent with the requirements defined by its Information Guardian, wherever the information is located, i.e.,

1. On printed media (e.g., forms, reports, microfilm, microfiche, books),
2. On computers,
3. On networks (data and voice),
4. On magnetic or optical storage media (e.g., hard drive, diskette, tape, CD),
5. In physical storage environments (e.g., offices, filing cabinets, drawers),

If an authorized user is not aware of the security requirements for information to which he or she has access, he or she must provide that information with maximum protection until its requirements can be ascertained. Any individual who has been given a physical key, ID card or logical identifier (e.g., computer or network account) that enables him or her to access information is responsible for all activities performed by anyone using that key or identifier. Therefore, each individual must be diligent in protecting his or her physical keys and ID cards against theft, and his or her computer and network accounts against unauthorized use.

Passwords created for computer and network accounts should be difficult to guess. Furthermore, passwords should never be shared or recorded and stored in a location that is easily accessible by others. Stolen keys and ID cards, and computer and network accounts suspected of being compromised should be reported to the appropriate authorities immediately. The assignment of a single network or system account to a group of individuals sharing the same password is highly discouraged and may only occur in cases where there is no reasonable, technical alternative.

b. Information Associated with "Identity Theft"

Identity theft is a serious and growing problem in our society. Anyone who can obtain certain pieces of information about an individual can open credit cards, take out loans, create forged documents or steal assets in the individual's name. Being sensitive to the identity theft threat, the Organization requires that extra precaution be taken when collecting, using and storing non- public "personally identifiable" information, such as:

a. Date of birth,
b. Place of birth,
c. Mother's maiden name,
d. Credit card numbers,
e. Bank account numbers,
f. Income tax records

Collection and use of any of the above pieces of information should be limited to situations where there is legitimate business need and **no reasonable alternative**. Managers must ensure that their employees understand the need to safeguard this information, and that adequate procedures are in place to minimize this risk. Access to such information may only be granted to authorize individuals on a need to know basis.

c. Limitations on Sharing Personally Identifying Information

All non-public information gathered and maintained by employees of Organization, for the purpose of conducting Organization business, that personally identifies any living or deceased individual – names and other personal information pertaining to individual employees, clients, contractors, subcontractors etc. – is considered "confidential" unless otherwise specified by this document or by the appropriate Information Guardian or designate.

Implementation

- Implement the provisions of the policy.
- Ensure that staffs that handle, or have access to, personal data are fully familiar with the policy.

Monitoring

- Check that the policy is being implemented (e.g. by conducting periodic audits of data protection procedures) and identify any issues arising.

Review, Evaluation and Revision

- Review and evaluate the impact of the policy at a pre-determined time, taking into account feedback from other developments.
- Revise as necessary, in light of the review and evaluation process.

Penalty Norms

Direct termination of service if someone is found to be violating the norms.

Conclusion

All the employee of Equity Express including work from home or carries the work/system out of office must to adhere the IT Data Privacy policy and ensure all the confidential information such as customer name, contact numbers and any customer personal information remain within Equity Express premises only.

All the employees are restricted to take out the customer personal data and document in form of any medium like electronic media or printed copy outside the Organization premises.

Thank You