DATA CLASIFICATION AND PROTECTION POLICY [DCP]

Version 1.0

August 01, 2014

TRADEJINI

Document Version Control

Sr. No.	Version No.	Change Description	Effective Date	Prepared By	Reviewer By	Approved By
1.	1.0	Draft Policy Issued	01-08-14	Kunal Anand	Vikram A V	Dinesh Kumar M

Scope

This policy can be used to classify and protect any data that are stored, processed, or transmitted by the organization. The standard applies to all types of data but not limited to following:

- Electronic Data,
- Data recorded on paper; and
- Information shared orally, visually or by other means

This Policy will be applicable to all the Employees, Contractors and Vendors of the Tradejini Financial Services Pvt Ltd and would cover all the information processing systems, and related equipment's in use which are vulnerable from the view point of the Organization.

Objective

The purpose of this policy is to establish a framework for classifying and handling organizational data based on its level of sensitivity, value and criticality to the organization as required. Classification of data will aid in determining baseline security controls for the protection of data.

Policy Statement

Data Classification Scheme

Match any data that need to be classified to the one of the four categories which best describes its need for confidentiality and its risk profile. The four categories are Public, Internal, Confidential, and Restricted.

Classification Category	Description & Examples
Public	Data can be disclosed without restriction. Examples – Company Broachers, Advertisements, Press Release, Information on company's website, etc.
Internal	Confidentiality of data is preferred, but information contained in data may be subject to open records disclosure. Examples – Internal Circulars, Telephone numbers, Email Address Directories, Manuals, Training Materials, Policies, SOPs, Intranet Website, etc.
Confidential	Data that needs to be restricted to a limited set of users – internal or external. Unauthorized disclosure, modification, or destruction of such data may result in significant damage to the business. Examples – All Customer Details, Loan details, Audit Reports, etc.
Restricted	Restricted data requires privacy and security protections. Special authorization may be required for use and collection. Examples – Sensitive Financial Information, Business Information Reports, Business strategy and forecasts,

Classification Category	Description & Examples
	Intellectual Property Rights, etc.

Data Protection Scheme

Asset Category	Public	Internal	Confidential	Restricted
Media/Paper Documents Physical Access	No special security measures.	Should be stored out of sight when unattended.	Media must be stored in a secure environment when unattended. Systems storing such information must be housed in a secure environment.	Must not be left unattended. Media must be stored in secure environment when not in use or being worked on. Systems storing such information must be segregated from other systems and housed in an area with enhanced physical security controls.
Copies and Distribution	No need for control of distribution.	Copies must contain the same classification mark as the original.	Must only be available to named individuals or distribution lists. Printing/Copying processes must be physically controlled by the user, to ensure that no information remains left in the printers or copying machines. Copies must contain the same classification mark as the original.	Must only be available to named individuals in agreement with the information owner. Printing/Copying processes must be physically controlled by the user, to ensure that no information remains left in the printers or copying machines. Copies must contain the same classification mark as the original.
Electronic Storage	No need for additional protection.	Must be stored on systems which are only accessible to employees or authorized support staff.	Must be stored on systems which are in secure environment and accessible only to employees and authorized support staff.	Must be stored on systems which are in segregated secure environment and accessible only to employees and authorized support staff. Encryption should be

Asset Category	Public	Internal	Confidential	Restricted
				used to protect such information if stored on portable device or if there is requirement to store it in non-secure environment. Operating system or database access controls must be correctly configured to ensure authorized access.
Electronic Transfer	No need for additional protection.	Must be password protected if transferred via an external network.	Information must be encrypted if transferred via an external network.	Information must be encrypted if transferred via an external network.
Physical Transfer	No need for additional protection.	Paper documents must be transferred in a sealed container / envelope that prevent the information from being read.	Paper documents must be transferred in a sealed container / envelope which contain a clear indication that the document must be delivered by hand to the named individual.	Paper documents must be transferred in a security sealed tamper evident container / envelope with a clear indication that the document must be delivered by hand to the named individual. Such paper documents must be transferred by an employee or a trusted third party.
Change Control & Audit	Secure publishing / release of public information e.g. use of restricted PDF settings to ensure information released to the public cannot be modified and re-published once in the public domain'.	Standard version control should apply.	Standard Version control should apply.	Standard Version control should apply. Access to such information should always be recorded on a secure audit trail.
Destruction of physical media	No need for additional protection.	No need for additional protection.	All printed material and media must be shredded prior to disposal.	All printed material and media must be shredded prior to disposal. In addition, the shredded documentation must

Asset Category	Public	Internal	Confidential	Restricted
				be incinerated.
Destruction of electronic information	No need for additional protection.	No need for additional protection.	All such information is subjected to degaussing or secure erase by using specialized tools.	All such information is subjected to secure erase by using specialized tools.

Responsibilities

- It is the responsibility of the IT Department to ensure that owners are identified for each information asset.
- The asset owners are responsible for identifying, classifying, labeling and ensuring the protection of their respective information assets as per the guidelines set above.
- The asset owners are responsible for ensuring the implementation of the required controls for the protection of information assets.
- All employees and third party staff are responsible for handling information assets as per the classification of the asset.

Review and Update

- The policy shall be reviewed annually or as and when significant changes occur to ensure its continuing suitability, adequacy and effectiveness.
- Management approval for revised policy shall be obtained and maintained by the IT Department of the company.

End of Document ■