DATA PRIVACY POLICY

Data Classification

1.1 Purpose and overview

The Data of PFSPL is information generated by or for, owned by, or otherwise in the possession of PFSPL that is related to the company's activities. PFSPL Data may exist in any format (i.e. electronic, paper) and includes, but is not limited to, all business, administrative, and research data, as well as the computing infrastructure and program code that supports the business of PFSPL.

In order to effectively secure PFSPL Data, we must have a vocabulary that we can use to describe the data and quantify the amount of protection required. This policy defines four categories into which all University Data can be divided:

- *Public*
- *Internal*
- *Confidential*
- *Restricted Use*

PFSPL Data that is classified as Public may be disclosed to any person regardless of their affiliation with the company. All other PFSPL Data is considered Sensitive Information and must be protected appropriately. This document provides definitions for and examples of each of the four categories. Other policies – such as Data Privacy Policy and IT Policy - specify the security controls that are required for each category of data.

Some information could be classified differently at different times. For example, information that was once considered to be Confidential data may become Public data once it has been appropriately disclosed. Everyone with access to PFSPL Data should exercise good judgment in handling sensitive information and seek guidance from management as needed.

1.1. Scope

This classification scheme is to be applied to all PFSPL Data, both physical and electronic, throughout the organization. No data item is too small to be classified.

1.2. Classification Levels

Public

Public data is information that may be disclosed to any person regardless of their affiliation with the company. The Public classification is not limited to data that is of public interest or intended to be distributed to the public; the classification applies to data that do not require any level of protection from disclosure. While it may be necessary to protect original (source) documents from unauthorized modification, Public data may be shared with a broad audience both within and outside the PFSPL community and no steps need be taken to prevent its distribution. Examples of Public data include: information on the website of the company, policies and other documents that the company has to regulatorily place on its website, display required by applicable regulatory guidelines to be done at the offices and branches of the company, press releases, directory information, marketing materials, compliance standards, and other general information that is openly shared.

Internal

Internal data is information that is potentially sensitive and is not intended to be shared with the public. Internal data generally should not be disclosed outside of the PFSPL without the permission of the person or group that created the data. It is the responsibility of the data owner to treat the information as Internal where appropriate. If a staff has doubts about whether information is Internal or how to treat Internal data, the staff should talk to the concerned department head or the management.

Examples of Internal data include: Some memos, correspondence, and meeting minutes; contact lists that contain information that is not publicly available; and procedural documentation that should remain private.

Confidential

Confidential data is information that, if made available to unauthorized parties, may adversely affect individuals or the business of PFSPL. This classification also includes data that the company is required to keep confidential, either by law, or by regulatory requirements, or under a confidentiality agreement with a third party, such as a vendor. This information should be protected against unauthorized disclosure or modification. Confidential data should be used only when necessary for business purposes and should be protected both when it is in use and when it is being stored or transported.

Any unauthorized disclosure or loss of Confidential data must be reported to the immediate superior as well as the management.

Examples of Confidential data include:

- Data of the books of accounts
- Personally identifiable information of the customers, Board members and employees
- Individual employment information, including salary, benefits and performance appraisals for current, former, and prospective employees.
- Legally privileged information.
- Information that is the subject of a confidentiality agreement.

Restricted Use

Restricted Use data includes any information that PFSPL has a contractual, legal, or regulatory obligation to safeguard in the most stringent manner. In some cases, unauthorized disclosure or loss of this data would require the company to notify the affected individual and state or federal authorities. In some cases, modification of the data would require informing the affected individual.

PFSPL's obligations will depend on the particular data and the relevant contract or laws. The Data Privacy Policy of PFSPL sets a baseline for all Restricted Use data. Systems and processes protecting the following are the examples of the types of data need to meet that baseline:

- Unencrypted data used to authenticate or authorize individuals to use electronic resources, such as passwords, keys, and other electronic tokens. An Individual's

biometric data (e.g., fingerprints, face scans, etc.) stored for authentication purposes.

- "Criminal Background Data" that might be collected as part of an application form or a background check.
- Financial account numbers such as company credit card, bank account access detail etc.

Restricted Use data should be used only when no alternative exists and must be carefully protected. Any unauthorized disclosure, unauthorized modification, or loss of Restricted Use data must be reported to the immediate superior and the management.

1.3. Important

Failure to comply with the Data Classification Policy may result in harm to individuals, organizations or PFSPL. The unauthorized or unacceptable use of PFSPL Data, including the failure to comply with these standards, constitutes a violation of PFSPL policy and may subject the user to revocation of the privilege to use PFSPL Data or disciplinary action, up to and including termination of employment.