PNU IT

Information Asset Management Policy

Version: 1.4

جامعة الأميرة نورة بنت عبدالرحمن
Princess Nourah Bint Abdulrahman University
PNU, Saudi Arabia

Contents

Document Management Information

Document Title: Information Asset Management Policy

Document Owner: PNU ISM

Security Classification: Internal

The "Information Asset Management Policy" is released for the use in Princess Nourah Bint Abdulrahman University (PNU), henceforth referred to as PNU. PNU holds all the rights on this document. No part or full of this document should be replicated or copied. The intended users of this document are all the relevant departments of PNU, the PNU Information Security Committee (PNUISC) and any other support groups who are responsible for Information Security in PNU. This document is subject to the PNU document control procedures. Comments, suggestions, and queries should be addressed to PNUISC/ ISM (Information Security Manager) using the email "ITC-Security@pnu.edu.sa.

1 Purpose

The purpose of the Information Asset Management Policy is to ensure the PNU's assets are accounted for, managed appropriately, and maintain control over information assets. The objective of this policy is to classify assets, define ownership and develop procedure for information asset governance.

2 Scope

The scope of this policy applies to all information assets owned by PNU and all entities under PNU .

The assets which are connected to PNU internal network. This policy is applicable to internal employees, third parties, contract employees and vendor employees who are utilizing, managing, and supporting the assets within PNU.

3 Responsibility

3.1 Asset Owner

The Asset owner is defined as the one who owns and classifies the asset. Asset owners are responsible for identification, classification, labelling (of tangible information assets) and protection of information assets, and keeping the asset register of their business function up-to-date. They are also responsible for communicating and reviewing the implementation of necessary controls required for protecting their assets.

The asset owners shall in consultation with business heads identify asset custodians for each information asset owned by them.

3.2 Asset Custodian

The Asset Custodian shall hold the responsibility of the maintenance and protection of information asset. Based on the request from the Asset Owner, Asset Custodian shall provide the information management services like performing regular backups of data, implementing security mechanisms, restoring data from backup media, and fulfilling the requirements as per security policies to ensure data protection.

3.3 Inventory Controller

The Inventory Controller is defined as the one who allocates, tracks, releases and reallocates the assets.

3.4 User

- User shall be considered as any individual who routinely accesses Information Systems and uses the information for executing business related tasks.
- Information Assets shall be classified in groups with appropriate owners designated for each group of assets.
- The Owners and custodians for Software assets shall be defined in asset management procedure.

4 Policy Statement

Information assets of PNU are of utmost importance, and confidentiality, integrity and availability of these shall be maintained appropriately.

The objectives of this policy are to:

- Identify and prepare inventory of all information assets;
- Ensure that for every asset an appropriate owner, custodian and user has been identified and recorded;
- Classify assets in terms of its confidentiality(C), integrity(I) and availability(A) to the business operations of PNU; and
- Conduct risk assessment of information assets as per documented Risk Assessment Methodology, and thereof take actions to ensure that residual risk is dealt with as per risk acceptance criteria.

4.1 Inventory of Assets

- All Information assets (information, software, physical, services and people assets) hosted in PNU shall be identified across all departments and shall be recorded in an information asset register.
- The asset register shall be reviewed on a quarterly basis.

- The asset register shall cover details as listed below:
  - Serial Number
  - Department
  - Asset Group
  - Asset ID
  - Asset Name
  - Asset Type
  - Asset Owner (Role)
  - Asset Custodian (Role)
  - Asset Classification
  - Confidentiality Rating
  - Integrity Rating
  - Availability Rating
  - Asset Criticality Rating

4.2 Asset Tracking

- Initial classification of assets shall be taken care of in the procurement procedures.
- Initial asset allocation shall be done as per the respective department procedure, as applicable.
- The respective inventory controller shall maintain the updated database of the assets.
- Inventory of systems & devices processing sensitive information (such as Personal Data, Personally Identifiable Information, and Payment Card related information) and users authorized to access such systems & devices shall be maintained.
- Stock verification of key assets shall be done as per respective departmental procedures.
- Any discrepancies, exceptions during the stock verification shall be reported to the custodian as per Security Incident Management procedure

- In case of inventory controller and custodian being the same, the discrepancy shall be reported to the department head.

4.3 Information Classification Levels

- The four classification levels that identify the level of protection that shall be given to the data assets are:
  - **Public**: Non-Sensitive information that is freely available and can be distributed within and outside PNU.
  - **Internal**: Information that is generally distributed to everyone within PNU only and not to outsiders.
  - **Confidential**: Information that is sensitive within a department/project within PNU is intended for use only within that department/project.
  - **Restricted**: Highly sensitive information that is intended for use only by specified persons.
- It is the responsibility of the respective Asset Owners to appropriately classify their data.
- The data classification process shall be completed for existing data and shall be undertaken for any new application development project at the time of designing the new application or generation of data.

4.4 Asset Labelling

- All physically and electronically stored information shall be labeled to ensure that the information is handled according to the sensitivity of information.
- Physical labeling of documents, hardware items and removable media shall include security classifications
- Wherever possible password controls and/ or cryptography/ check-summing shall be used for restricted /confidential information

4.5 Asset Allocation/ Release/Reallocation

- Allocation, Release & Re-Allocation of assets shall be done as per respective department procedures, as applicable.

- All Software master licenses and media shall be stored in central data repository in a secured place.

4.6 Disposal of Assets

- All computer equipment and media shall be erased/ demagnetized before sending for repairs or disposal to prevent retrieval of any data from such media
- When sensitive information is erased from a disk, tape or other magnetic storage media, it shall be followed by a repeated overwrite operation which prevents the data from later being scavenged
- Disposal of information systems equipment shall proceed in accordance with procedures established by IT Ops Team.

5 Point of contact

For any clarification or further information on this policy contact Chief Information Security Officer at "ITC-SIM@pnu.edu.sa".

6 Enforcement

- This policy applies to all information assets within PNU.
- All users shall read and abide by this Information Asset Management Policy.
- Any employee found in violation to this policy shall be subjected to disciplinary action.

7 References

- ISO 27001:2013: A.8.1.1 Inventory of assets
- ISO 27001:2013: A.8.1.2 Ownership of assets
- ISO 27001:2013: A.8.1.3 Acceptable use of assets
- ISO 27001:2013: A 8.2.1 Classification of Information
- ISO 27001:2013: A8.2.2 Labelling of Information