Asset Classification and Categorization

1. Purpose

This document defines the approach for the classification and categorization of organizational assets to ensure consistent handling, protection, and management in accordance with their value, sensitivity, and criticality.

2. Asset Classification Table

Asset Category	Asset Example	Classification	Description
Information	Design Documents, Source Code, Client Data	Confidential	High sensitivity, access strictly controlled
Systems	Application Servers, Databases	Critical	Essential for daily operations and service delivery
Physical Assets	Laptops, USB Drives, Phones	Internal Use	Used by employees, restricted from public access
Network Assets	Routers, Firewalls	Restricted	Supports protected connectivity; access limited
Personnel	Staff Records, Payroll Data	Sensitive	Contains personal data, regulated by law

3. Asset Categorization Levels

- **Confidential**: Exposure could cause significant harm to organization or clients.
- **Sensitive**: Access is limited, disclosure could result in moderate repercussions.
- **Internal Use**: Information meant for use only within the organization.
- **Public**: Approved for public disclosure and distribution.

4. Important Notes

- Asset classification must be reviewed and updated regularly or when significant changes occur.
- Staff must be trained on the importance of asset classification and handling procedures.
- Misclassification can lead to legal, financial, and reputational risks.
- Access to assets should be limited based on their classification level.
- Document versioning should indicate the date and status of the latest review.