Bandhan

Hope for the Poor

DATA SECURITY POLICY

Bandhan Konnagar

Table of Contents

Policy Statement

All identified business data at Bandhan-Konnagar (BK) shall be controlled and protected in all phases of its life cycle including collection, processing, transmission, storage, exchange and retirement.

Roles and Responsibilities

Information Owner

Vice President shall be the Information Owner and shall be overall responsible for all business information assets. Responsibilities would include, but not be limited to:

i. Nominate Information Sub-owners for each Development Program under BK.
ii. Assigning business information classification and periodically reviewing the classification to ensure it still meets business needs

Information Sub-owner

Deputy Vice President or Program Director, shall act as Information Sub-Owners and shall be responsible for following:

i. Ensuring security controls are in place commensurate with the classification
ii. Reviewing and ensuring currency of the access rights associated with information assets they own
iii. Determining security requirements, access criteria and backup requirements for the information assets they own

Data Protection Officer

Assistant Vice President or Program Managers will primarily be the Data Protection Officer (DPO) for protection of information managed at the head office and the branch managers for respective branches

i. As DPO, he/she shall be responsible for implementation of this policy for Data Identification and Data Inventory Management.
ii. DPO should maintain a Data Distribution list, of all identified data, having details of users who have been approved for access of these data. Details should include User, Data and Access Time Period.

Data Consumer (End User)

The end users shall be any employees including program officers and branch staff, contractors or vendors of BK who use information systems resources as part of their job. Responsibilities include:

i. Maintaining confidentiality of log-in password(s)
ii. Ensuring security of information entrusted to them as a part of job responsibility
iii. Using information assets and resources for management approved purposes only
iv. Adhering to all information security policies, procedures, standards and guidelines
v. Promptly reporting security incidents to management

IT System Administrators

IT System administrators shall be responsible for day-to-day operational management of information systems including performing backups, restoration, administration of user IDs and access rights, reporting and following up on security violation reports etc.

Information Security Officer

Information Security Officer shall be responsible for:

i. Consulting the application owners for implementation of appropriate security controls and regular review of implementation of the same.
ii. Understanding different data environments and the impact of granting access to them

Data Classification

Based on its sensitivity to business operations, all identified data should be classified under one of the following categories:

Classification	Description	Examples
Public	Information that is available to the general public and intended for distribution outside the organization. This information may be freely disseminated without potential harm.	- Information available on the organization's website - Information in program brochures, reports
Internal	Information that is deemed sensitive due to financial or legal ramifications and which is for use only by authorized BK employees and auditors, consultants, vendor personnel, legal and regulatory authorities.	- Organizations policy documents - Standard operating procedure documents - Minutes of the meetings
Confidential	Information that is proprietary to the BK and its unauthorized disclosure could adversely impact the organization, its employees and other stakeholders.	- Beneficiaries' and employees' personal identification information - Beneficiaries' account information
Top Secret	Information that is so confidential that leak of such information can severely impact the organization, its employees and all the relevant stakeholders	- Organization's financial information - Information related to key IT Infrastructure

Data Protection and Sharing

Following controls should be implemented for the protection of data:

1. Access to data should be controlled based on classification of data and need to know basis.
2. Access to electronic data, stored on system, should be provided after user authentication at least with unique user ID and Password based on a clearly defined password policy.
3. Access to electronic data, stored on system, should be limited to appropriate privilege level according to job responsibilities as per business requirement.
4. Access to data for consultants/third party users should be provided on need to know basis

Data Storage

1. Data Storage and Retention should be done with measures adequate to its classification.
2. Confidential data should only be stored in locations which are approved by DPO.
3. Password protection should be used for files/folders and email accounts on users

4. Confidential papers/printed documents should be kept in cabinets with lock and key mechanism in fire proof safe. Only authorized persons should have access to such documents. Key allocation should be recorded in a key maintenance register and key access should be reviewed by data protection owners.

Data Retention and Retirement

1. Information owner/ sub-owners should define the data retention period based on operational need.
2. After expiry of defined retention period, data should be disposed or discarded with appropriate methods based on data classification.

Data Exchange and Disclosure

1. A Non-disclosure agreement should be signed prior to exchanging data with third parties, applicability of which will be decided by BK management.

2. All information security requirements must be defined clearly in the service agreement with third-party for data protection.
3. Only the relevant and minimum amount of data necessary should be shared with third parties.
4. Such agreement should also cover the acceptance of third-party for full co-operation and assistance in case of any incident or fraud detection

Monitoring and Review

1. All access to, modification or deletion of data by users should be logged. Logging methods and levels should be decided based on data classification.
2. All privileged access to data stores should be logged and monitored. These should be reviewed by overseeing authority on regular basis.
3. BK should conduct annual compliance audit to verify compliance to this policy and applicable legal, regulatory and industry requirements for data protection.