DATA GOVERNANCE, CLASSIFICATION & PRIVACY POLICY

Version: V1 (Initial)
Date: July 19, 2021

SCOPE

This policy will apply to the Joint Industry Board of the Electrical Industry (JIBEI) and all affiliates, including JIB Medical, P.C.

PURPOSE

The purpose of this policy is to identify the different types of data and to establish a framework for classifying organizational data based on its level of sensitivity, value, and criticality to JIBEI.

POLICY

This policy is to help ensure the governance, classification, and protection of JIBEI data from unauthorized access, damage, alteration, or disclosure while preserving the ability of authorized users to access and use JIBEI data for appropriate business purposes. This policy refers to all JIBEI data, electronic as well as paper. This policy is applicable to all data storage locations and is applicable to all data used to conduct the business of the JIBEI.

Data governance is a discipline for assessing, managing, using, improving, monitoring, maintaining, and protecting organizational data. Data governance is used by organizations to exercise control over processes and methods used by their Data Stewards and Data Custodians in order to improve data quality and integrity. When data is created the Data Trustee must classify the data and establish a governance framework for the data that corresponds to the university rules for that data type and applicable federal and state laws.

Data Classification and Data Types

This policy describes the actions necessary to secure and protect JIBEI data defined as Personal Identifiable Information (PII), which includes but not limited to Personal Health Information (PHI), Confidential data, Internal Use data, and Public data.

(i) Personal Identifiable Information (PII):

a. (PII) is defined as: Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means. Further, PII is defined as information: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors). Additionally, information permitting the physical or online contacting of a specific individual is the same as personally identifiable information.

b. In addition, JIBEI defines PII to include PHI. Protected health information is the term given to health data created, received, stored, or transmitted by HIPAA-covered entities and their business associates in relation to the provision of healthcare, healthcare operations and payment for healthcare services. Protected health information includes all individually identifiable health information, including demographic data, medical histories, test results, insurance information, and other information used to identify a patient or provide healthcare services or healthcare coverage. 'Protected' means the information is protected under the HIPAA Privacy Rule.

c. Users of PII data must follow all safeguards for Confidential data plus additional safeguards High levels of security safeguards must be applied to PII

(ii) Confidential:

a. Data is classified as restricted when the unauthorized disclosure, alteration or destruction of that data could cause a significant level of risk to JIBEI, or its affiliates. Some examples of Confidential data include Financial Statements or information or Human Resources information.

b. Users of Confidential data must follow all safeguards for Internal data plus additional safeguards. High levels of security safeguards must be applied to Confidential data.

(iii) Internal:

a. Data is classified as Controlled when the unauthorized disclosure, alteration or destruction of that data could result in a moderate level of risk to the JIBEI affiliates. By default, all JIBEI data that is not explicitly

classified as PII, Confidential or Public data must be treated as Internal data. An example of Internal data includes emails sent to or from JIBEI employees while conducting JIBEI business.

b. A reasonable level of security safeguards must be applied to internal data.

(iv) Public:

a. Data that is readily available to the public.

b. This data requires no confidentiality or integrity protection. Public data needs no additional protection.

Data Governance:

The following principles are set forth as minimum standards to govern the use of JIBEI data:

- JIBEI data is the property of JIBEI and shall be managed as a key asset.
- Unnecessary duplication of JIBEI data is discouraged.
- JIBEI data shall be protected.
- JIBEI data shall be accessible according to defined business needs and roles.
- Anyone granted access to JIBEI data will be held accountable to their roles and responsibilities.
- Data Stewards are responsible for the subset of data in their charge.

Roles Required to Govern Data

Several roles and responsibilities govern the management of, access to, and accountability for JIBEI data.

Data trustees: JIBEI senior management who have authority over policies and procedures regarding business definitions of data and the access and usage of that data.

Data Stewards: JIBEI management and/or supervisors that have direct operational-level responsibility for the management of one or more types of JIBEI data.

Data Custodians: System administrators responsible for the operation and management of systems and servers that collect, manage, and provide access to JIBEI data.

Data Users: Departments, Employees and others who have been granted access to JIBEI data in order to perform assigned duties or in fulfillment of assigned roles or functions within JIBEI.

Collectively these parties are responsible for identifying and implementing safeguards for the different data types.

Data File Storage

Only JIBEI IT approved storage may be used for data, other than public data. Data is not permitted to be exported and stored or shared via personal cloud-based file storage, remote/home storage, or removable storage. Refer to the Information Security policy for additional information.

REFERENCES

Other related JIBEI Policies and Procedures:

- Information Security Policy
- Access Controls Policy
- Data Backup Policy
- IT Controls Policy & Procedures (including User Provisioning and Guidelines for Privileged Users sections)
- Security Controls

Related Regulations:

- HIPAA
- New York General Business Law sections 899-aa and 899-bb
- Employee Retirement Income Security Act (ERISA)
- PCI DSS

REVISION HISTORY

Revision Tracking		
Version #	Revision Date	Revision Notes
V1	7/19/2021	Initial