Andrew Nakamura and Joseph Tsai
CSS 517 A – Assignment: Write an IA Policy

Information Security Policy

1. Purpose

The purpose of this policy is to protect GenCo information resources from accidental or intentional unauthorized access, modification, or damage, while allowing public data for open information sharing. The expectations described within this policy adhere to the availability, confidentiality and integrity requirements as described within the Information Security Program Charter.

2. Scope

This policy applies to all staff that are granted the use of GenCo's information. All GenCo staff shall take reasonable steps as defined within this policy and the related documents to ensure all information is managed and held securely. Such action shall be taken in accordance with common law and regulatory requirements which support business functions and activities.

3. Roles and Responsibilities of Those Affected

This section details the overview of information security organizational roles and responsibilities in GenCo, with further details described within the Roles and Responsibilities policy.

3.1 **Executive Leadership** is responsible for appointing the Chief Information Security Officer (CISO) and ensuring that security policy adheres to law and regulatory requirements.

3.2 **The CISO** is responsible for overseeing processes to reduce information security risks, resolve disputes related to security policy incidents, and establish standards and controls of security policies. The CISO shall communicate risks to executive leadership and work with the Information Security Office (ISO) to develop expected controls and spread awareness of security policies.

3.3 **The Information Security Office (ISO)** is responsible for conducting risk assessments and maintaining a listing of data elements used within each business unit. The ISO also establishes information security standards, processes, and frameworks to be used in the classification and handling of any GenCo data. The ISO is also responsible for escalating violations of policy to the CISO and coordinating with GenCo management to ensure correct handling of data elements.

3.4 **All GenCo Staff** are responsible for protecting the privacy and security of all information in their control, as well as reporting any violations of the Information Security Policy to the ISO.

4. Data Classifications/Data Handling Requirements

All data is given a classification which is determined by the sensitivity and risks associated with potential disclosure of such data. The classification for any piece of data determines the corresponding security measures which must be used to protect the data.

Requirements for protection measures at each level of classification are described in further detail within the Information Security Protection Standard. The following are the data classifications and data handling requirements used by GenCo:

4.1 **Restricted** data poses high levels of security, financial, and reputational risk to GenCo upon potential disclosure of the information. Restricted data can only be shared in cases where it is absolutely necessary to perform business functions.

Sharing of Restricted data in any regard with outside parties must be first approved by General Counsel, with documented written consent from the outside party to abide by any conditions posed by the General Counsel pertaining to treatment of the data.

4.2 **Confidential** data presents minor risks to GenCo's security and reputation upon potential disclosure of the information. Such data must only be shared for purposes of business needs, and access to such data must be disclosed in cases where the data is regulated.

4.3 **Public** data is information which GenCo has intentionally made available or has intentionally published with clear instruction for the data to be used by the general public.

4.4 **GenCo Data Handling** requires that combining any data will result in the data being classified and handled at the stricter classification. A complete listing of data elements for each classification can be found within the Data Classification Standard. Sharing of any GenCo data must also abide by the Acceptable Use and Vendor Management policies.

5. Enforcement

Any violation of this policy can or may result in disciplinary action, including and up to termination of employment. Law enforcement may also be provided in the case that a given violation gives indication to a potential crime, as determined by the Information Security Committee.

6. Obtaining Exceptions to the Policy

Requests for exceptions to the policy must be brought to the attention of the ISO. The ISO will assign a review to the CISO, stating the risks and reasons for the exception. Only once both the CISO and ISO approve the action, the user may proceed as requested.

7. Related Documents

1. Information Security Program Charter
2. Roles and Responsibilities Policy
3. Security Governance Policy
4. Information Security Protection Standard
5. Data Classification Standard
6. Acceptable Use Policy
7. Vendor Management Policy