Joseph Tsai and CSS peer (name redacted)
CSS 517 A – Assignment: Write an IA Policy

Information Security Policy

1. Purpose

The purpose of this policy is to protect the company's information resources from accidental or intentional unauthorized access, modification or damage, while allowing public data for open information sharing requirements.

2. Scope

The policy applies to all workers, interns, and staff that are granted the use of company assets. This document defines the responsibility for the protection and appropriate use of company information within any company application, computer system, network, or business relationship.

3. Roles and Responsibilities of Those Affected

CEO, CISO, and General Counsel

1. Appoints the members of the Information Security Committee

Information Security Committee

1. Defines classification of data elements
2. Reviews standards, procedures, and guidelines related to the policy on an annual basis
3. Resolves any disputes related to this policy upon notification of the dispute
4. At the end of each fiscal quarter, gives a review of policy to current employees

Security Administrators

1. Maintains the list of sensitive data elements within their respective business unit
2. Ensures that the appropriate standards for information and data access are established
3. Ensures that governance is consistent with FISMA
4. Escalate violations of the policy to the Information Security Committee

Employees

1. Protect the privacy and security of data and information in compliance with this policy as it pertains to the network and security systems under their control
2. Reports violations of policy to the security administrator

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 used by the company:

Restricted

The following data is considered Restricted:

- Social security number
- Bank Account number
- Credit card number
- Any HIPPA regulated health information
- Driver's license number
- State identity card number

Restricted data can be shared only in cases where it is absolutely necessary to perform business functions. Sharing of this 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.

Confidential

Confidential data presents minor risks to the company'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. Sharing of Confidential data must abide by policies including: Acceptable Use, Vendor Management, and Employee Rights.

Public

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

Utilizing multiple pieces of data or combining the data will result in the data being classified at the stricter classification.

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.

6. Getting Exceptions to the Policy

Requests for exceptions to the policy must be brought to the attention of the security administrator. The security administrator will assign a review to the general counsel. Once both the general counsel and security administrator approve the action, the user may proceed as requested.