Information Security Policy

Matthew Austin

Fontbonne University

Quagliata

2016

Information security policies are the blueprints and guidelines to a safe, secure, and strong organization, which is fundamental to it’s success and growth. Policies, of course, will differ from one another depending on the organization and its objective. For example a Fortune 500 company’s objectives are greatly different from a college/university. The security policy that will be analyzed will be the information security policy from The University of North Carolina Greensboro. To fully assess and extract the requirements for implementing the policy in the organization, its purpose, scope, policy, enforcement and other related attributes will be restated, reviewed and then finally improved upon.

The first thing stated in the policy is its purpose, which defines how the security requirements and enforcement help the company reach or maintain its current objective. The University of North Carolina’s (UNC) purpose states “This policy specifies the principles and requirements the University of North Carolina at Greensboro (hereinafter "University") has established to protect information assets owned by or in the care of the University.” To ensure that the policies purpose is up to date the policy has to be updated regularly. Unfortunately for the UNC their policy was first approved by the Chancellor, Security Networks and Data, and Wireless Communications since 2004. The policy was then approved again in 2010 and finally in 2012. For a policy to be effective it has to be updated. Before having requirements for implementing the policy in the organization effectively, its policy has to be updated at least yearly as the purpose of the organization has have changed dramatically.

Second the scope states who the policy affects and what assets it affects as well. The UNC’s policy states “This policy applies to all faculty, staff, students, and any parties who interact with, access, or store University information assets or information assets in the University's care.” The scope thought broad covers anyone who attends, works, or is a guest and have access to any type of information that the it has available pertaining to the level of access that the individual has. To effectively implement this policy regarding the scope, the policy has to address ways to not only keep every individual's information secure but to also restrict the individual's access to a level that ensures their safety and prevent them negatively affecting others.

Thirdly, the policy states and address the goals that it will take to achieve its purpose while utilizing the information that it stated in its scope. The UNCs policy states:

The University will work toward achieving these goals:

1. The University is committed to protecting information assets.
2. The University shall act as a responsible conservator of information assets entrusted to its care.
3. The University shall comply with federal and state law, contractual obligations, and UNC System policies related to information security.
4. University business processes shall be consistent with the above principles, and, unless contrary to law, University policies or UNC System Policies, shall follow the UNCG Information Security Management Standards and procedures for implementation of those standards.
5. All University leadership, faculty, staff, and students, and relevant affiliates are required to actively support the above principles and are expected to take reasonable measures to protect information assets in their care.

The policy states that it will work towards achieving protecting information assets, this information can range from student and faculty usernames and passwords to more private and confidential information such as SSNs and licences. The policy then continues to state that it will act as a responsible conserver of the information that it has while complying with federal state and law obligations. The policy finally states that all of the students, faculty and any other party or affiliate must support its principles to ensure their information is protected.

Finally after effectively assess and review all of the principles that the policy stated, the requirements for implementing the policy in the organization can be extracted. By sticking the to the same style that the policy presents the policy will again restate that everyone will have to follow the principles to ensure their safety. To finally make sure that the principles are followed the any student that violates them will be subject to the repressions that it student handbook presents. If the UNC’s employees violate the principles in the policy, EPA, and SPA, will be referred for criminal prosecution and termination from the company. By broadly stating its intentions the policy covers all that it will protect what it can disclose in this public policy. Though not very detailed it is moderately effective at addressing what it work to achieve.