Matthew Austin

Information Security

Karen Quagliata

November 2016

Homework 5: Security Procedure Updates

**Security Procedure Update Policy**

***1. Overview***

This Social Engineering Awareness Policy is meant to assist policy owners, co-owners and designees in the Policy creation, management, and updating process.

***2. Purpose***

This policy is meant to ensure that the policy owners, co-owners and designees policies and procedures are updated on constant basis. This will help in reducing risks associated such as:

1. Policy Misunderstanding (due to it being outdated)
2. Policy non-compliance (rule breaking)
3. Potential fines and penalties (due to to legal requirements)

In the event of creating a new policy a person must follow the set of procedures for developing, updating and reviewing policies and procedures that the CIO has created.

When creating a policy and employee is responsible for updating and reviewing the policies and procedures relevant to their department within the organization, once it is approved by the CIO. Development of new policies and procedures can be undertaken by any employee, as needs arise.

***3. Scope***

This policy applies to all employees of our organization, excluding temporary/full-time contractors participating in any action within the organization.

***4. Policy***

4.1 *Identifying Purpose/Need for Policy Update*

* 4.1.1 *The Reasons for a new policy may include:*
  + There is a decision that the organization needs to handle under the organization's legislation
  + There is need for develop a policy for a new aspect of business or there is a new or significant risk
* 4.1.2 *The Reasons for a new procedure may include:*
  + To help a staff member create and/or implement a new policy
  + To clarify particular roles or and responsibilities or to ensure consistency in the organization's work processes.
* 4.1.3 *You may need a new work instructions for several reason*

4.2 *The Process of Implementing a new policy*

* 4.2.1 At the start of a work day, in order for a new or revised policy or procedure to be approved, a folder should be created within the organizations secure shared drive within the organization's server in the Draft Policies and Draft Procedure for Approval folders.
* 4.2.2 Before starting work on a new policy or procedure , check with the CIO because there may be an existing policy or procedure that can be used to address all the needs you wanted to address.
* 4.2.3 After sharing your document in the Draft Policies and Draft Procedure for Approval folders, depending on the nature of the document, you may need to meet with other directorates or stakeholders first. It is usually best to provide a draft (printed copy) before the meeting to focus discussion. During this meeting or consultation, you should aim to agree on a version of your policy or procedure that will satisfy operational, legal and policy objectives that the directorates or stakeholders want to implement.
* 4.2.4 All policies and procedures must be reviewed by the organizations directorate for a final check for consistency and quality.
* 4.2.5 If the policy or procedure is approved and finalized, the CIO or directorate should create a way to communicate the change with the rest of the employees and assess changes to training. The CIO or directorate should send a mass email to all employees that the new policy procedure affects (its recommend that you send it to all employees regardless or department)

4.3 *The Developing a new policy or procedure*

* 4.3.1 The new policy or procedure must follow the same temples that the CIO or directorate provides.
* 4.3.2 Policies, just like all of the organization's documents should be drafted using English, following the organization's style using the organization's Style Guide and a list of commonly used terms and definitions.

**Reference**

Campus Information Technology Security Policy. (2016). Retrieved August 22, 2016,

from <https://security.berkeley.edu/campus-information-technology-security-policy>

<https://www.sophos.com/en-us/medialibrary/PDFs/other/sophos-example-data-security-policies-na.pdf?la=en>

The University Policy Manual. (2016). Retrieved August 22, 2016, from

<https://policy.uncg.edu/university-policies/data/>

Secure The Breach | Get Ready For A Security Breach. (n.d.). Retrieved August 30,

2016, from <http://www.securethebreach.com/encryption.html>

Information Security | Washington University in St. Louis. (2016). Retrieved August 22,

2016, from <https://wustl.edu/about/compliance-policies/computers-in>

Kissel, Richard. *Glossary of Key Information Security Terms*. N.p.: n.p., n.d.*Glossary of Key*

*Information Security Terms*. NVL Publications. Web. 32 Oct. 2016. <<http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf>>.

SANS. "Social Engineering." *Consensus Policy Resource Community*. SANS, n.d. Web. 23 Oct.

2016. <<https://www.sans.org/security-resources/policies/retired/pdf/social-engineering-awareness-policy>>.