System Change Policy

ACME Evil Anvil Corporation

January 2019

Contents

1 Purpose and Scope **2**

2 Background **2**

3 Policy **2**

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	CC8.1, CC3.4

Table 2: Document history

Date	Comment
Jun 1 2018	Initial document

1 Purpose and Scope

a. This information security policy defines how changes to information systems are planned and implemented

b. This policy applies to the entire information security program at the organization (i.e. to all information and communications technology, as well as related documentation).

c. All employees, contractors, part-time and temporary workers, service providers, and those employed by others to perform work for the organization, or who have been granted to the organization's information and communications technology, must comply with this policy.

2 Background

a. This policy defines specific requirements to ensure that changes to systems and applications are properly planned, evaluated, reviewed, approved, communicated, implemented, documented, and reviewed, thereby ensuring the greatest probability of success. Where changes are not successful, this document provides mechanisms for conducting post-implementation review such that future mistakes and errors can be prevented.

3 Policy

a. Any changes to the security architecture or customer data handling of a system must be formally requested in writing to the organization's Information Security Manager (ISM), and approved by the ISM and the Chief Information Officer (CIO).

b. All change requests must be documented.

c. All change requests must be prioritized in terms of benefits, urgency, effort required, and potential impacts to the organization's operations.

d. All implemented changes must be communicated to relevant users.

e. Change management must be conducted according to the following procedure:

   i. *Planning*: plan the change, including the implementation design, scheduling, and implementation of a communications plan, testing plan, and roll-back plan.

   ii. *Evaluation*: evaluate the change, including priority level of the service and risk that the proposed change introduces to the system; determine

the change type and the specific step-by-step process to implement the change.

iii. *Review*: review the change plan amongst the CIO, ISM, Engineering Lead, and, if applicable, Business Unit Manager.

iv. *Approval*: the CIO must approve the change plan.

v. *Communication*: communicate the change to all users of the system.

vi. *Implementation*: test and implement the change.

vii. *Documentation*: record the change and any post-implementation issues.

viii. *Post-change review*: conduct a post-implementation review to determine how the change is impacting the organization, either positively or negatively. Discuss and document any lessons learned.