Remote Access Policy

ACME Evil Anvil Corporation

January 2019

Contents

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	CC6.1, CC6.2, CC6.7

Table 2: Document history

Date	Comment
Jun 1 2018	Initial document

1 Purpose and Scope

a. The purpose of this policy is to define requirements for connecting to the organization's systems and networks from remote hosts, including personally-owned devices, in order to minimize data loss/exposure.

b. This policy applies to all users of information systems within the organization. This typically includes employees and contractors, as well as any external parties that come into contact with systems and information controlled by the organization (hereinafter referred to as "users"). This policy must be made readily accessible to all users.

2 Background

a. The intent of this policy is to minimize the organization's exposure to damages which may result from the unauthorized remote use of resources, including but not limited to: the loss of sensitive, company confidential data and intellectual property; damage to the organization's public image; damage to the organization's internal systems; and fines and/or other financial liabilities incurred as a result of such losses.

b. Within this policy, the following definitions apply:

   i. *Mobile computing equipment:* includes portable computers, mobile phones, smart phones, memory cards and other mobile equipment used for storage, processing and transfer of data.

   ii. *Remote host:* is defined as an information system, node or network that is not under direct control of the organization.

   iii. *Telework:* the act of using mobile computing equipment and remote hosts to perform work outside the organization's physical premises. Teleworking does not include the use of mobile phones.

3 Policy

a. *Security Requirements for Remote Hosts and Mobile Computing Equipment*

   i. Caution must be exercised when mobile computing equipment is placed or used in uncontrolled spaces such as vehicles, public spaces, hotel rooms, meeting places, conference centers, and other unprotected areas outside the organization's premises.

   ii. When using remote hosts and mobile computing equipment, users must take care that information on the device (e.g. displayed on the screen) cannot be read by unauthorized persons if the device is

being used to connect to the organization's systems or work with the organization's data.

iii. Remote hosts must be updated and patched for the latest security updates on at least a monthly basis.

iv. Remote hosts must have endpoint protection software (e.g. malware scanner) installed and updated at all times.

v. Persons using mobile computing equipment off-premises are responsible for regular backups of organizational data that resides on the the device.

vi. Access to the organization's systems must be done through an encrypted and authenticated VPN connection with multi-factor authentication enabled. All users requiring remote access must be provisioned with VPN credentials from the organization's information technology team. VPN keys must be rotated at least twice per year. Revocation of VPN keys must be included in the Offboarding Policy.

vii. Information stored on mobile computing equipment must be encrypted using hard drive full disk encryption.

b. *Security Requirements for Telework*

i. Employees must be specifically authorized for telework in writing from their hiring manager .

ii. Only device's assigned owner is permitted to use remote nodes and mobile computing equipment. Unauthorized users (such as others living or working at the location where telework is performed) are not permitted to use such devices.

iii. Devices must be authorized using certificates

iv. Users performing telework are responsible for the appropriate configuration of the local network used for connecting to the Internet at their telework location.

v. Users performing telework must protect the organization's intellectual property rights, either for software or other materials that are present on remote nodes and mobile computing equipment.