Remote Access Policy

Fusion-IT

February 2021

Contents

Table 1: Control satisfaction

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

Table 2: Document history

Date	Comment
Feb 11 2021	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, to minimize data loss/exposure.

b. This policy applies to all users of information systems within the organization. This typically includes regular full-time, regular part-time, temporary, and provisional employees, 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. This policy intends to minimize the organization's exposure to damages that 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, 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 the 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. Never leave your mobile devices unattended in an area without the supervion of an authorized user or trusted third party.

iii. 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 user if the device is being used to connect to the organization's systems or work with the organization's data. Be aware of shoulder surfing in public areas.

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

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

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. Revocation of VPN keys must be included in the Offboarding Policy.

vii. Illegal activities and the use of pirated software is strictly prohibited.

b. *Security Requirements for Telework*

i. Full and part-time employees must be specifically authorized for telework in writing from their manager for a specific timeframe and location. If the request gets approved, the employee must put a note in his shared calendar to inform his colleagues that he will be working remotely for a specified period of time.

ii. Only the 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. Users performing telework are responsible for the appropriate configuration of the local network used for connecting to the Internet at their telework location. This includes but is not limited to the use of:

- WPA2-AES security for wifi networks with a password compliant to Fusion-IT password policy
- A single firewall with properly configured rules. Unsecured port forwarding must be avoided.

i. Users performing telework must ensure the remote host is not connected to any other network at the same time, except for personal networks that are under their complete control or under the complete control of an authorized user or third party.

ii. 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. It is prohibited

to publish any work-related assets that includes code, documentation, clients name, software used, or any information that is not explicitly labeled as for public use according to the Data Classification Policy.

4 Authorship and Approval

Last edit made by Lotana (louis.tant@gmail.com) on Thu, 11 Feb 2021 15:22:42 -0500.

Approved by Lotana (louis.tant@gmail.com) on Thu, 11 Feb 2021 15:22:42 -0500 in commit 22571f598c69c8148d7b37832a7a1061b39acc19.