Device's Usage and Configuration Policy

Description

- This policy regards the use of unauthorized devices and software to access any work-related data, servers, and networks. As well as the necessary configurations to maintain your work device secure.

Scope

- This policy is aimed to all staff and personnel.

Policy Elements

- **Policy Element 1**
- Risk: The use of unauthorized devices to access any work-related data, networks, and servers.
- Impact: The device might not be protected with firewalls and other security measures. If the device is compromised that could lead to an attack or an exploitation. Using unauthorized devices could also result in confidential data being left stored on a public device for anyone to access it.
- Policy: Only use the company's devices to access the network and any related data.
- Reference: CIS Control 1.

- **Policy Element 2**
- Risk: The use of unauthorized software to access work-related data, servers, and network.
- Impact: The software might not be secure enough to keep the data protected which is a vulnerability to data breaches. The software could already be compromised which can lead to an attack or any exploitation on the network, server, and data.
- Policy: Only use authorized software to access work-related data, servers, and network.
- Reference: CIS Control 2.

- **Policy Element 3**
- Risk: Connecting work devices to unauthorized networks and servers.
- Impact: Accessing unauthorized networks and servers can lead to the device being compromised, which opens the doors to a variety of attacks and exploitations.
- Policy: Only connect your device to authorized networks and servers.
- Reference: CIS Control 3.

- **Policy Element 4**
- Risk: The download and access of unsafe links.
- Impact: Downloading and/or accessing unsafe links is a vulnerability. It could lead to your device being compromised by a virus or any other form of attack and breach.
- Policy: Be careful with what you download and access on the company's device.
- Reference: CIS Control 3.

- **Policy Element 5**
- Risk: Not updating device's systems and software.
- Impact: Not updating software and systems on work devices is a vulnerability. Many updates are released because of security breaches, and not updating them might lead to being hacked and/or exploited.
- Policy: Always update the software and systems on work devices. Also, research for newer and better options in case the current ones have shown vulnerability.
- Reference: CIS Control 3.

Consequences

Those that fail to uphold the policy will be subjected to consequences within the company and the law. The consequences are based on the degree/extent of their actions. The following are possible outcomes:

- The employee is placed in disciplinary training.

- The employee is fined.

- The employee has its employment status reviewed.

Definitions

Term	Definition with example
Exploitation	It is the act of selfishly taking advantage of someone or a group of people to profit from them or benefit oneself.
Vulnerability	It is the state of being exposed to the possibility of being attacked or harmed.
Compromised	To expose or make vulnerable to danger; jeopardize.

Author: Samuel Monteiro Basso

Date: 2022-10-23