**Network Capable Personal Electronic Devices in the Workplace ISSP**

Alice Mace

Computer Information Systems, Bellevue University

CIS 608: Information Security Management

Professor Kayleen Amerson

April 25, 2022

**Network Capable Personal Electronic Devices in the Workplace ISSP**

**Scope and Applicability**

The purpose of this security policy is to define the allowances and limitations on using personal electronic devices while connected to the corporate network. This policy is specific to devices that are capable of connecting to a network, wired or wirelessly (i.e., laptops, tablets, cell phones, etc.). It is the responsibility of the employee to ensure they are meeting and following company policy and each employee is required to review and agree to follow this policy on an annual basis.

**Authorized Access and Usage of Personal Devices**

While located in the office, employees are authorized to connect to the corporate network with personal devices using their corporate login credentials. It is expected that all company policies will be followed when connected to the corporate network on personal devices. The company will not store any personal information from employee-owned devices and will only record activity in accordance with the Systems Management section documented below.

**Prohibited Usage of Personal Devices**

The use of personal devices aligns with the company’s HR policy in that no disruptive behavior, misuse/criminal use of the corporate network, and/or any offensive or harassing materials will be tolerated. Reproduction or replication of official or proprietary information on personal devices is prohibited. If employees are reported to have used personal devices in the workplace while connected to the corporate network in a manner that is disruptive, criminal, or offensive, the employee may have their corporate network login credentials revoked and could face administrative action. The company has the right to seize and maintain control of any personal property when they have reports of illegal activity or illegally stored company material, with an appropriate law enforcement request, until the device can be properly expunged of any such material.

**Systems Management**

Employees are not authorized to store official or proprietary documents on personal devices. While a device is connected to the company network, the network activity is logged in accordance with the same procedures as other company systems. All employees must have a virus protection software downloaded on their device before connecting to the network. McAfee is preferred, but please see IT/Security for an expanded list of approved software. If devices are left unattended while connected to the network, they must be locked and have a minimum of a six-character password to prevent access from unauthorized users. Employees are not authorized to connect to company networks while not physically located in the work building.

**Violations of Policy**

If you see an employee not following this policy and/or you unintentionally violate this policy, please report to HR, the cyber help desk, or your immediate supervisor. They will assist in the proper documentation and mitigations or remedial actions to prevent the compromise of company data. Employees that are found to be in violation of this policy are subject to administrative actions, including potential termination of employment and/or subsequent legal action.

**Policy Review and Modification**

This policy will be reviewed a minimum of every five years and/or if new technology and office needs warrant another review within an earlier timeline. Employees may request a review of this policy through the IT/Security department if it is preventing or inhibiting the ability to complete duties and responsibilities in an efficient manner. Any modifications or updates to the policy will be published to the company and will require acknowledgement within one month of publication.

**References**

Department of Information and Communications Technology Republic of the Philippines. (n.d.). *INFORMATION SYSTEMS STRATEGIC PLAN 2018–2020*. DICT.Gov.Ph. Retrieved April 25, 2022, from https://dict.gov.ph/wp-content/uploads/2018/01/ISSP-Template.pdf?msclkid=92c888e4c4de11eca814481e4ef451e9

Federal Aviation Administration. (n.d.). *Develop Preliminary ISSP (Including Basic Security Policy) (c)*. Faa.Gov. Retrieved April 25, 2022, from https://www.faa.gov/about/office\_org/headquarters\_offices/ato/service\_units/operations/isse/items/c\_prelim\_issp?msclkid=92c9b335c4de11ec94c4c411f96d1562

Whitman, M. E., & Mattord, H. J. (2018). *Management of Information Security* (6th ed.). Cengage Learning.

York, A., & Thiessen, B. J. (2015, December 21). *Technology in the workplace - Top 9 issues for employers*. Lexology. https://www.lexology.com/library/detail.aspx?g=334b0532-1b94-4247-82d6-62dbfff0e19c&msclkid=12ae1eb4c4ed11ec9a2e343cd0291634

**Peer Review Recommendations**

1. Add in legal/law enforcement request to the section regarding company seizure of personal assets
2. Clarifying/consistent verb tense usage in Systems Management section
3. Rephrase/reorder of repercussions in the Violation of Policy section