[INSERT FIRM LEGAL NAME]

Mobile Computing and Remote Working Policy

[Insert Firm Logo]

Version 1.0

[Insert Date]

Contents

Instructions

Documents are in a template format and are to be customized to fit the appropriate business and operational requirements. Use the sample as a foundation to build a bespoke policy for your business.

If any element of the following Sample/Template is not operationally feasible or appropriate for a particular business, be sure to delete that element from the company-specific document. **Otherwise, it would be a liability exposure to establish a policy and not to comply with it.**

The following recommendations are designed to limit, but will not eliminate, the security risks associated with the use of the policy subject. Businesses should deploy a defense-in-depth security model of technical, operational, and physical security controls.

Delete the instructions after finalizing and adopting the policy.

Policy Overview

As mobile devices in organizations become more prevalent with the rise of BYOD (Bring Your Own Device) policies, it is necessary to consider the security risks associated with these devices. This policy sets forth guidelines for how to properly secure mobile computing devices and storage media.

Mobile computing and storage devices include, but are not limited to: laptop computers, USB port devices, Compact Discs (CDs), Digital Versatile Discs (DVDs), flash drives, modems, and handheld wireless devices that may connect to or access the information systems. Risk analysis for each new media type shall be conducted and documented prior to its use or connection to the network unless the media type has already been approved by CIO. The CIO will maintain a list of approved mobile computing and storage devices.

Mobile computing devices are easily lost or stolen, presenting a high risk for unauthorized access and the introduction of malicious software to the network. These risks must be mitigated to acceptable levels by following current best practices for desktop computer management.

Portable computers and mobile storage devices must be protected by encrypted media. The password for the encryption technology should be complex and difficult to guess.

Downloading data from a database or portion thereof to a mobile computing or storage device, without the prior written approval of DSAC and the CISO, may result in the exposure of sensitive information to unauthorized internal and external users. In addition, the mobile computing device could be lost or stolen, resulting in the exposure of sensitive information. This policy applies to all employees.

Procedures

To report a lost or stolen mobile computing and storage device, call the Enterprise Help Desk in your organization's time zone. For further procedures on lost or stolen handheld wireless devices, please see the Procedures section.

The Desktop Standards Committee shall approve all new mobile computing and storage devices that may connect to information systems at the organization. The Committee will also review their respective vendor security assessments for the purpose of protecting against viruses, network intrusions, and data theft.

Any employee who chooses to use a non-departmental-owned device that may connect to the organization's network must first be approved by technical personnel such as those from Desktop Support.

Roles and Responsibilities

Users of mobile computing and storage devices must diligently protect such devices from loss of equipment and disclosure of private information belonging to or maintained by the organization. Before connecting a mobile computing or storage device to the network, users must ensure it is on the list of approved devices issued by the Information Services and Technology Department (ISD).

Any employee who is involved in a security incident, such as the loss or theft of a mobile device and/or loss of sensitive data on a computer, tablet, or mobile phone, must immediately notify the Enterprise Help Desk.

The Information Security Team is responsible for the mobile device policy and shall conduct a risk analysis to document safeguards for each media type to be used on the network or on equipment. The Information Security Team shall provide these safeguards in writing before a device is approved for use on the network. The Information Security Team shall ensure that these criteria are updated annually and whenever there are significant changes to either policy or approved devices.

The use of mobile computing and remote working is an emerging practice. As ISD develops a mobile computing and remote working policy, it will also develop procedures for implementing the policy. The standard device list will be made available on the intranet for all employees to have access to.

Scope and Purpose

Scope
Individuals who use mobile computers and storage devices on the network are required to follow these security policies.

Purpose
The purpose of this policy document is to establish the requirements that individuals using mobile computing and storage devices on the network must follow.

Compliance

The Information Security team will verify compliance with this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Exceptions

Any exception to the policy must be approved by the Information Security team in advance.

Definitions and Terms

None

Appendix

None

Revision Table

Revision History				
#	**Version #**	**Date**	**Updates/Changes**	**Owner**
1	1.0	2023	Initial Draft	Riskigy
2				