Remote and Mobile Computing Policy

Instructions

This template is a starting point to enable you to create a Remote and Mobile Computing Policy tailored to meet the needs of your organization.

Perform a full document replacement of **<Organization>** with the proper name of your organization.

When you have customized the policy to your satisfaction, you can simply delete these instructions and paste the remaining text into your own policy document format. Alternatively, you may modify the footer in this document to suit your organization.

Policy Change Log

Date	Change	Edited by:	Approved by:
	Policy creation		

Table of Content

Purpose of the Policy

This policy provides specific information regarding remote and mobile computing mechanisms for information systems at <Organization>.

Remote Information Processing refers to performing information processing activities in a remote location other than a <Organization> controlled facility. It includes the following sites:

- fixed locations (such as a residence)
- mobile locations (such as a hotel or airport)
- third-party locations (such as manufacturing partners, test facilities or contractor agencies)

Responsibility for Policy Implementation

The <Organization> Security Officer or other authorized representative shall be responsible for ensuring implementation of all items listed in the Policy Requirements section. Responsibility for the creation and implementation of specific procedures may be assigned to internal staff or contractors as appropriate.

Policy Requirements

The <Organization> Security Officer or other authorized representative shall ensure compliance with the following standards:

Mobility

Theft Prevention

<Organization> Users are required to implement company-approved measures to prevent the theft of <Organization> owned/leased desktop and mobile computing devices.

Types of Mobile Devices

Mobile computing devices include any computing device or media that is easily transportable outside of <Organization> premises, such as but not limited to the following:

- laptop computers
- USB mass storage devices
- mobile phones
- external hard drives
- optical media (CD/DVD/Blu-ray)

Accidental loss or theft incurs numerous hard and soft costs including the following:

- replacement cost of hardware
- re-licensing of software (operating systems/applications)
- incident reporting
- lost productivity
- exposure of proprietary information, perhaps to competitors
- exposure of sensitive employee information
- exposure of sensitive or confidential customer information
- potential federal, state and local fines associated with exposure of confidential employee or customer information
- damage to the reputation, brand, and market share of <Organization>
- misuse of <Organization> resources (for example, to commit a crime or harass <Organization> Users/customers)
- risk to <Organization> networks due to access to remote dialup scripts, email addresses, and passwords

Mobile Phones

Definitions

Mobile Phones – Any portable phone device (smart or otherwise) that, in addition to having the capability to make and receive phone calls, is also capable of receiving, transmitting and/or storing confidential information. Examples of mobile phones may include, but are not limited to: cell phones and smartphones.

Confidential Information – Any individual's Personally Identifiable Information (PII); financial, operating or other proprietary <Organization> information; and other <Organization> information that is confidential in nature (e.g., employee compensation, benefit and disciplinary records).

External Storage Devices – any device that connects to an external interface of a computer, or to which data can be transferred. This including, but is not limited to USB, eSata, Firewire, Bluetooth, and wireless devices.

Remote Access – any network access that uses any network that is not owned and controlled by <Organization> as part of the connection. This includes home networks and public networks, as defined below.

Public Networks – any network that is located in a public location and allows patrons, customers, or other, non-authenticated users to connect to the network.

Mobile Phone Usage Standards and Policy
Only <Organization> mobile phones are permitted for conducting business requiring the use of a mobile phone. The use of a personal mobile phone for conducting <Organization> business is strictly prohibited unless the use of a personal mobile phone has been approved by an employee's leader.

General Provisions

All <Organization> computer equipment security requirements are in effect for mobile phones as well. These requirements include, but are not limited to:

- Strong authentication using password, PIN and/or biometric security
- Prohibition of installing unauthorized software
- Prohibition of modifying configuration settings

Other Requirements – The portable nature of mobile phones requires procedures which may not be applicable for workstations or similar computer equipment. Your mobile phone training will include these mobile phone specific requirements. These requirements include, but are not limited to:

- Report a lost or stolen mobile phone immediately
- Keep your mobile phone in a secure location when not in use and never leave it unattended
- Lock the device with a password or Personal Identification Number (PIN)
- Install Apps only from trusted sources
- Back up your data
- Keep your system updated
- Do not hack (jail-break, root) your device
- Remember to log out of banking and shopping sites
- Turn off Wi-Fi and Bluetooth services when not in use
- Avoid sending personal information via Text or Email
- Be careful what you click
- Do not send confidential data over insecure (HTTP) connections
- Do not connect to company resources from public networks (coffee shops, restaurants, libraries, airports, etc.)

Mobile Data

Stored Data
Appropriate measures to protect Data stored on remote or mobile devices must be implemented.

Precautions for Data Protection
Precautions to protect the data must apply regardless of the following:

- storage media on which information is recorded
- locations where the information is stored
- systems used to process the information
- individuals who have access to the information
- processes by which the information is handled

Locations
<Organization> Users shall use approved connection methods only when connecting from remote locations, including home networks, hotels, and public networks.

Minimizing Data Storage
Minimizing data storage on mobile devices will minimize the risk to data loss.

Remote Access Restrictions

<Organization> reserves the right to restrict, prevent, or otherwise control remote access to its network if <Organization> believes that such remote access is not being used in accordance with this directive, any directive, or supporting documents, or is otherwise detrimental to the interests of <Organization>.

Approved Hardware and Software

Hardware and software configurations for remote access computers must meet the same requirements as set out for equipment used on <Organization> premises. In particular, hardware and/or software that do not meet <Organization> business requirements must not be installed. Any workstation, either laptop or desktop, with non-approved hardware/ software configurations must not connect to <Organization> networks.

Security Breach

Any suspected security breach relating to remote access must be immediately reported to a <Organization> leader.

Remote Access

Access to Remote Information Processing Facilities

Access to any remote information processing facilities must be through VPN and in conformance with <Organization> policies.

VPN Cryptography

Remote access VPN must employ cryptography which is in conformance with good computing practices.

Remote Access Logging

Remote access connection activity must be logged and have an audit trail. This is necessary for the security of <Organization> networks.

Additional Restrictions

[Instructions: Use this section to add policy provisions specific to your organization. Some examples of additional restrictions are shown below. Delete any items that do not apply to your desired policy and add any others that are appropriate.]

Allowed Devices

Only the following types of mobile devices shall be connected to <Organization> networks:

- List specific types, brands, models, etc. that should be allowed. Examples would be IOS devices only, laptops only, etc.
- Devices that have been approved by <Organization>'s Security Team

The following types of devices shall not be connected to any <Organization> network.

- List any types of devices that you do NOT want to allow to connect. Examples might be USB storage devices, Android devices, etc.

Allowed connection methods

Mobile devices connecting to <Organization's> networks shall use the following connection methods only:

- List specific connection methods that you want to allow. If you wish to restrict connections to a specific VPN or remote access application, you can list it here.
- If you email service supports plain-text email (a dangerous practice in any case), you might want to prohibit its use.

Data storage restrictions

The following data types shall not be stored on mobile devices:

- List any specific types of data that you do not want users to store on mobile devices. This may include patient records, client lists, financial records, etc.

Mobile Device Management

All mobile devices connecting to <Organization> networks shall have <Organization>'s Mobile Device Management (MDM) software installed. Mobile devices shall be subject to the following restrictions:

- Devices with operating system modifications (e.g. "rooted" or "jail-broken" devices) shall not be allowed to connect.
- All devices shall have the following applications installed:
  - List applications that are required.
- Any devices with the following applications installed shall not be connected to any <Organization> network. If found on a device, these applications may be remotely uninstalled.

- Device location may be tracked by <Organization> via the device's Global Positioning System (GPS) feature. Disabling the GPS feature is prohibited.
- You must immediately report any device that has been lost, stolen, misplaced, or is no longer under your direct control
- If a device is lost or stolen, data may be remotely deleted from the device. This may include any personal data that has been stored on the device.

Exceptions

[Instructions: Add any exceptions to the policy that you may want to include here. For example, certain persons or departments may be exempt from certain provisions.

Implementation

[Instructions: Use this section to refer to any additional informational or procedural documents required for proper implementation of the policy. For example, there may be a "how-to" document describing the process for connecting to remotely to local resources via a VPN connection, etc.]