1.0 Purpose

The purpose of this policy is to assist agencies with the growing number of mobile devices in the workplace. The use of mobile handheld devices, such as Personal Digital Assistants (PDAs), tablet computers and laptops within the workplace, is expanding rapidly. These devices are no longer viewed as coveted gadgets for early technology adopters, but instead have become indispensable tools that offer business advantages for the mobile workforce. While providing productivity benefits, the ability of these devices to store and transmit information though both wired and wireless networks poses potential risks to an organization's security. This policy describes a framework for managing mobile and handheld devices.

2.0 Scope

This policy applies to all state agencies that fall under the Executive Branch of Rhode Island state government.

3.0 Background

Approximately 1,600 notebooks are stolen daily in the United States. The rate of notebook theft has nearly doubled in three years and is expected to accelerate as mobile PCs proliferate. According to the information collected by the FBI and the Computer Security Institute, average reported financial losses due to laptop theft are in excess of $100,000 per incident.

The Division of Information Technology (DoIT) has not estimated financial losses to our organization due to computer theft; however, DoIT considers the accidental loss or theft of mobile computing devices to be a significant risk.

Computer loss or theft incurs numerous hard and soft costs, such as the following:

- Replacement cost of computer 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 State's reputation;
- Misuse of the State's computers, such as to commit a crime or harass employees or customers; and
- Risks to the State's network due to access to remote dial up scripts, email addresses, and passwords;

Consequently, the State of Rhode Island, its employees, and its constituents cannot afford the loss of the state's computer hardware.

4.0 History

This policy shall supersede all previous "State" Mobile Device Security Policies and shall be effective for all state employees, contractors, subcontractors, that have mobile devices that interface or contain state data.

5.0 References

Data Encryption Policy	05-03
Data Categorization Policy	05-02
Hard Drive Encryption for Laptops and Tablets	TOI 10-01

6.0 Definition

Mobile Devices – For the purposes of this policy, includes Pocket PCs, Tablet PCs, Laptop PCs, Notebook Devices, Personal Digital Assistants (PDAs) and other mobile computing devices.

7.0 General Security Overview

Basic mobile device security policies:

7.1 Mobile devices connected to agency equipment should be password protected.

7.2 The wireless port on mobile devices should be disabled when not in use.

7.3 All mobile devices should have installed anti-virus software.

7.4 Mobile devices that do not have up-to-date anti-virus software should be scanned for viruses prior to connecting to the agency network.

7.5 Mobile devices are not considered a secure. It is recommended that only non-confidential information be stored on the device. If Confidential and Sensitive data (Data Categorization Policy - 05-02) must be stored on the device is not permitted unless it is encrypted.

7.6 Mobile devices should have the latest security patches installed on their operating system.

7.7 Privately owned mobile devices are not to be used for storing Confidential, Sensitive and Critical data (Data Categorization Policy – 05-02).

8.0 Physical Security

8.1 The Division of Information Technology (DoIT) will provide a locking security cable and key to every employee issued a mobile device. DoIT will instruct employees in the appropriate use of the locking security cable. At all times, users must:

- Physically secure the device with a cable lock attached to an immoveable device and/or
- Lock it away in a cabinet or alternatively lock the door of an individually occupied office
- If for any reason the mobile device cannot be physically attached to an immovable object using a locking security cable, access to the device must be restricted physically

8.2 Mobile devices must not be :

- Left in a vehicle overnight
- Left in view in an unattended vehicle, even for a short period of time. If

you must do so temporarily, the computer must be placed in the automobile's trunk.

- Positioned so that they are visible from outside a ground floor window unless there is no alternative.

8.3 A mobile device displaying sensitive information in a public place, e.g. train, aircraft or bus, must whenever possible be positioned so that the screen cannot be viewed by others.

9.0 Device Security

9.1 Devices, when unattended, should have some type of screen saver with the password protection or keyboard locking program enabled.

9.2 Any software installed on mobile devices that uses a script file should not contain a user ID or password for the State's computer system

9.3 All mobile devices should be updated with the latest security patches, virus scanning software and data files. Agencies are responsible for installing the patches, virus scanning software and virus data files on their devices. Patches and updates to virus data files should be installed through an automated process if applicable. Agencies should install patches for high-risk vulnerabilities with forty-eight (48) hours of notification of availability.

9.4 Mobile device users must notify the appropriate authorities immediately if their mobile device is lost or stolen.

10.0 Data Security

10.1 Backup data frequently, whenever possible data should be stored on agency file server.

10.2 Mobile devices containing Confidential and Sensitive information (Data Categorization Policy - 05-02), must use a product that will encrypt the entire hard disk, so that the computer cannot be booted up by anyone who does not have the password (Hard Drive Encryption for Laptops and Tablets TOI 10-01).

10.3 Use good judgment about the amount of sensitive data you store on your mobile device. Only store data that is needed, this will minimize the risk if your mobile device is lost or stolen.

11.0 Reporting Procedures

If an employee believes a computer in his or her control is lost or has been stolen, that employee must report this incident immediately by calling the following:

Contact Point	Contact Information
DoIT Service Desk	(401) 222-5709
Chief Information Security Officer	(401) 222-1283
Immediate Supervisor	

Within one hour of reporting the incident a written explanation of the incident must be sent to the Director of IT Operations.

Please return a signed copy the attached user agreement, signifying that you have read and understand this policy.

12.0 APPROVALS

Assistant Director of Planning, Policy & Technology	1/9/07 Date
Director of Operations	1/9/07 Date
Chief Information Officer	1/22/07 Date
Director, Department of Administration	2/7/07 Date

STATE OF RHODE ISLAND

Mobile Device Security Policy

User Agreement Acknowledgement

As a user of State of Rhode Island data and resources, I agree to abide by the Mobile Device Security Policy and the following promises and guidelines as they relate to the policy established:

1. I will protect State assets, confidential data, facilities and systems against unauthorized disclosure and/or use.
2. I will maintain all computer access codes in the strictest of confidence; immediately change them if I suspect their secrecy has been compromised, and will report activity that is contrary to the provisions of this agreement to my supervisor or a State-authorized Security Administrator.
3. I agree to report the loss of my mobile computer to the Division of Information Technology (DoIT) Service Desk.

I acknowledge that I must adhere to this policy as a condition for receiving a mobile computer and access to State of Rhode Island data and resources.

I understand the willful violation or disregard of any of these guidelines, statute or policies may result in disciplinary action, up to and including termination of my employment, and any other appropriate legal action, including possible prosecution.

I have read and agree to comply with the policy set forth herein.

Type or Print Name	Last 4 digits of Social Security Number
Signature	Date