STATE OF CONNECTICUT

ELECTRONIC MONITORING NOTICE

Pursuant to the requirements of Public Act 98-142, **An Act Requiring Notice to Employees of Electronic Monitoring by Employers,** state employees should recognize that their work activities and communications may be subject to electronic monitoring.

"Electronic monitoring" is defined by the Act as "the collection of information on an employer's premises concerning employees' activities or communications by any means other than direct observation, including the use of a computer, telephone, wire, radio, camera, electromagnetic, photoelectronic or photo-optical systems, but not including the collection of information for security purposes in common areas of the employer's premises which are held out for use by the public, or which is prohibited under state or federal law."

Employees may be subject to electronic monitoring or recording (including sound, voice or video devices) while in State facilities and other locations where State business is conducted, except that employees will not be subject to any such monitoring or recording in areas designed for the health or personal comfort of the employees or for safeguarding of their possessions, such as rest rooms, locker rooms or lounges.

Employees should understand that their activities involving State computer equipment and computer and/or electronic documents, data and communications, including e-mail and internet usage, are subject to being monitored, recorded and reviewed. Employees should be aware that the fact that a document, data or communication has been "deleted" by the employee does not mean that the item cannot be monitored or retrieved and reviewed.

Employees will not be subject to electronic monitoring or recording of the content of their direct telephone conversations, except as may be permitted under state and federal law.

(10/98)

Bureau of Enterprise Systems and Technology

Policy on Security for Mobile Computing and Storage Devices

Version: 1.0
Date Issued (revised): September 10, 2007
Date Effective: Immediately
Supersedes: n/a

Document Includes:

Purposes

The Chief Information Officer for the State of Connecticut Department of Information Technology (DOIT) has established this policy on the secure implementation and deployment of mobile computing and storage devices within State government for the protection of State data that may be stored on those devices.

This policy refers to and enhances State of Connecticut Network Security Policy and Procedures. The Policies should be read together to ensure a full understanding of State Policy.

Scope

This policy covers all State of Connecticut Executive Branch agencies and employees whether permanent or non-permanent, full or part-time, and all consultants or contracted individuals retained by an Executive Branch Agency with access to State data (herein referred to as "users").

This policy does not apply to the Judicial or Legislative Branches of government, or State institutions of higher education. However, these branches and institutions may consider adopting any or all parts of this policy.

This policy covers mobile computing devices and mobile storage devices (herein referred to as "mobile devices").

Authority

In accordance with Conn.Gen. Stat. §4d-2 (c) (1), the Chief Information Officer is responsible for developing and implementing policies pertaining to information and telecommunication systems for State Agencies.

Policy Statements

1. No confidential or restricted State data shall reside on any mobile devices except as set forth in paragraph 2. Agencies are required to utilize secure remote data access methods, as approved by DOIT, in support of mobile users.

2. In the event utilization of secure remote access methods are not possible, the Agency must adhere to the following restrictions and requirements:
   a. The Agency Head must authorize and certify in writing, in advance, that the storing of restricted and confidential State data on the mobile device is necessary to conduct Agency business operations;
   b. The Agency Head or their designee must determine and certify in writing that reasonable alternative means to provide the user with secure access to that State data do not exist;
   c. The Agency Head or their designee must assess the sensitivity of the data to reside on a secure

steal an individual's identity, violate the individual's right to privacy or otherwise harm the individual;

Organizational information that is not in the public domain and if improperly disclosed might: cause a significant or severe degradation in mission capability; result in significant or major damage to organizational assets; result in significant or major financial loss; or result in significant, severe or catastrophic harm to individuals.

In accordance with the State of Connecticut Network Security Policies and Procedures, each Agency is responsible for the assessment and categorization of their data as Confidential or Restricted in accordance with the definitions set forth in this policy.

Mobile Computing Devices

The term "mobile computing devices" refers to portable or mobile computing and telecommunications devices that can execute programs. This definition includes, but is not limited to, notebooks, palmtops, PDAs, IPods®, BlackBerry® devices, and cell phones with internet browsing capability.

Mobile Storage Devices

The term "mobile storage devices" includes but is not limited to, mobile computing devices, diskettes, magnetic tapes, external/removable hard drives, flash cards (e.g., SD, Compact Flash), thumb drives (USB keys), jump drives, compact disks, digital video disks, etc.

Secure Mobile Devices

A mobile device that has a sufficient level, as defined by this policy and DOIT standards, of access control, protection from malware and strong encryption capabilities to ensure the protection and privacy of State data that may be stored on the mobile device.