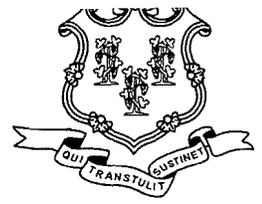




STATE OF CONNECTICUT  
**Department of  
Information Technology**



**Testimony**

**State of Connecticut  
Department of Information Technology  
Before the Government Administration and Elections Committee of the  
Connecticut General Assembly**

**March 12, 2008**

Chairpersons Slossberg and Caruso, and honorable members of the Government Administration and Elections Committee, my name is Diane S. Wallace and I am Chief Information Officer for the State of Connecticut Department of Information Technology (DOIT).

On behalf of our agency, I thank you for this opportunity to testify before you today in respectful opposition to SB 677 "AAC THE USE OF STATE COMPUTERS ON NONSTATE PROPERTY."

First, let me say that I am in complete agreement with the need to minimize the risk associated with allowing laptops with sensitive data to leave State facilities. This risk was highlighted last year by the theft of a State laptop computer containing the names and social security numbers of more than 100,000 state taxpayers. As one of those taxpayers, I can appreciate the urgency with which we seek to prevent something like this from happening again.

Last September, Governor Rell ordered agencies to purge sensitive data on laptop computers and portable storage devices if there was no compelling business need for the information to be stored on those devices.

In addition, while thousands of laptops and other mobile computing devices leave State offices each day, the majority -- more than 6,000 State laptop computers in 65 agencies -- are now encrypted due to reforms instituted last fall under Governor Rell's directive. This encryption took place as part of an unprecedented IT security mobilization led by DOIT and supported by IT professionals throughout all of our State agencies.

Our current encryption solution is so strong, that it would take 149 trillion years for a machine that types 255 characters per second to crack our security and access any private information. It uses AES (Federal standards), the Advanced Encryption Standard adopted by the Fed Government in 2002, after a 5 year standardization process.

**101 East River Drive • East Hartford, CT 06108-3274**

[www.state.ct.us](http://www.state.ct.us)

**An Equal Opportunity Employer**

An aggressive policy and accompanying procedures governing laptop and mobile device security was also launched and remains in place in all of our executive branch agencies. It includes new restrictions and accountability measures – including mandatory risk assessments and written authorization from the agency head – for any instance in which restricted or confidential data must reside on a mobile device for business reasons.

The new policy also requires any data residing on a mobile device under these controlled circumstances to be encrypted, limits the amount of data and length of time it may reside on the mobile device and requires protections from unauthorized access and disclosure.

In short, the reforms include measures designed to contain risk while at the same time not take away tools State employees need to get the job done. I applaud the intent behind SB 677 but fear the measures would cause an unnecessary burden on State employees who rely on mobile devices to carry out their work responsibilities.

I also fear the restriction called for in the legislation could hamper the State's business continuity planning efforts, which requires agencies to establish alternate work strategies in the event of a loss of a facility or portion of their work force. Many agencies use laptop computers as essential tools in these strategies and may require the inclusion of sensitive data on them in order to enable workers to continue to carry out their responsibilities.

In closing, let me say that in a perfect world, no sensitive information should ever reside on a mobile computing device. Our policy was written to minimize this occurrence, but includes provisions to accommodate cases where it is warranted or required such as in an emergency situation involving a public safety matter.

We believe the flexibility is warranted and wise and an outright prohibition could restrict agencies ability to execute their responsibilities.

For your review, I have attached the DOIT Policy on Security for Mobile Computing and Storage Devices to this testimony. It can be found at <http://www.ct.gov/doit/cwp/view.asp?a=1245&q=394672> .

Thank you for this opportunity to testify. I am available to answer any questions you may have at this time.

# Department of Information 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

Scope

Authority

Policy Statements

Definitions

### **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 mobile device and determine that the business need necessitating storage on the mobile device outweigh(s) the associated risk(s) of loss or compromise; and
  - d. The Agency Head or their designee must authorize, in writing, the storage of specific State data on a secure mobile device and the acceptance of all associated risk(s).
3. State data that an Agency Head has authorized to be stored on a secure mobile device shall be:
- a. the minimum data necessary to perform the business function necessitating storage on the mobile device;
  - b. stored only for the time needed to perform the business function;
  - c. encrypted using methods authorized by DOIT;
  - d. protected from any and all forms of unauthorized access and disclosure; and
  - e. stored only on secure mobile devices in accordance with DOIT Policies, Standards and Guidelines.
4. Any State data placed on a mobile device shall be documented, tracked, and audited by the authorizing Agency. The information tracked shall include the identification of the individual authorizing storage of the data on the mobile device, the authorized user of the mobile device, the asset tag of the mobile device, information about the stored data, and the final disposition of that data.
5. Agencies will configure mobile devices to allow only the minimum features, functions, and services needed to carry out Agency business requirements.
6. Agencies will ensure that mobile computing devices are configured with approved and properly updated software-based security mechanisms including anti-virus, anti-spyware, firewalls, and intrusion detection. Users shall not bypass or disable these security mechanisms under any circumstances.
7. Users in the possession of State owned mobile devices during transport or use in public places, meeting rooms and other unprotected areas must not leave these devices unattended at any time, and must take all reasonable and appropriate precautions to protect and control these devices from unauthorized physical access, tampering, loss or theft.
8. Agencies shall establish and document reporting, mitigation and remediation procedures for lost or stolen mobile devices containing State data and for State data that is compromised through accidental or non-authorized access or disclosure.
9. In the event that a mobile device containing State data is lost, stolen, or misplaced, and/or the user has determined unauthorized access has occurred, the user must immediately notify his or her Agency of the incident. The affected Agency must immediately notify the DOIT Help Desk of the incident in order to initiate effective and timely response and remediation.
10. Agencies shall develop and implement a formal, documented security awareness and training program sufficient to ensure compliance with this policy.
11. Agencies must obtain a signed, formal acknowledgement from users indicating that they have understood, and agreed to abide by the rules of this policy.
12. Agencies and users shall adhere to this security policy and associated procedures; failure to do so may result in sanctions.

## **Definitions**

### **Confidential or Restricted State Data**

Confidential or restricted State data includes but is not limited to;

Personally identifiable information that is not in the public domain and if improperly disclosed could be used to 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.

Content Last Modified on 9/18/2007 11:54:03 AM