

# **NETWORK SECURITY POLICY AND PROCEDURES**

## **Purpose**

The Chief Information Officer for the State of Connecticut and the Department of Information Technology (DOIT) have established this policy and reporting requirements along with associated standards to assure that critical information is protected and data flow is not interrupted by unauthorized access.

## **Policy Statements**

The following policy statements are abstracted from the official State of Connecticut Network Security Policy.

1. All information traveling over State computer networks that has not been specifically identified as the property of other parties will be treated as though it is a State asset. If there is no primary agency designated to administer this information, DOIT will become the steward of this data until another agency is designated. It is the policy of the State to prohibit unauthorized access, disclosure, duplication, modification, diversion, destruction, loss, misuse, or theft of this information.
2. In addition, it is the policy of the State to protect information belonging to third parties — that has been entrusted to the State in confidence — in the same manner as private sector trade secrets as well as in accordance with applicable contracts.
3. All computers permanently or intermittently connected to State of Connecticut networks, and all DOIT computers that intermittently or continuously connect to an internal or external network must employ password-based access controls. All users must be positively identified prior to being able to use any multi-user computer or communications system resources.
4. The computer and communications system privileges of all users, systems, and independently operating programs (such as "agents") must be restricted based on the need-to-know.
5. Participation in external networks as a provider of services that external parties rely on is expressly prohibited unless the Agency System Administrator has identified, in writing, the security risk involved and submitted those risks to the Security Oversight Committee, and the Chief Information Officer has expressly accepted these and other risks associated with the proposal.

6. Any modification in existing Network/Systems configurations that is in contrast to the statewide Security policy must be submitted for approval to the Security Oversight Committee.
7. Each agency that has existing dial-up lines/modems today must submit a request for consideration of approval to the Security Oversight Committee.
8. Wireless communications or other broadcast technologies must not be used for data transmission containing State "confidential" or "restricted" data unless the connection is encrypted and has an acceptable level user authentication.
9. Third-party vendors must **not** be given dial-up privileges to State computers and/or networks unless the involved system administrator determines that they have a bone fide need. These privileges must be enabled only for the time period required to accomplish the approved tasks (such as remote maintenance).
10. All users wishing to use the State internal networks, or multi-user systems that are connected to the State internal networks, must sign a compliance statement prior to being issued a user-ID.
11. Confidential or restricted data in unencrypted format is prohibited on State mobile computing and storage devices. Please see the State policy on mobile computing and storage devices for additional guidance and requirements.