



S T A T E O F M A R Y L A N D  
DEPARTMENT OF INFORMATION TECHNOLOGY

## **Microcomputer/PC/Laptop Security Standard**

Agencies must ensure that all microcomputer (i.e., workstation, desktop computers, laptops computers, PDA's, and any other portable device that processes/stores data) are secured against unauthorized access. The level of controls should be commensurate with the information accessed, stored, or processed on these devices. To help accomplish this each agency must establish at a minimum the following:

- General controls;
- Virus protection;
- Software licensing and use controls;
- Laptop security and mobile computing controls;
- Protection from personally owned microcomputers and portable storage devices.

### **General Controls**

All microcomputers that store and/or access nonpublic information must implement the following controls:

- User identification and password to control access at logon;
- Encryption to protect directories, sub-directories, and/or files containing nonpublic information;
- Virus Protection.

### **Virus protection**

Standard virus protection programs must be installed, updated, and maintained on all microcomputers, LAN servers, and mail servers. These programs must:

- Be configured to run checks for viruses at startup and operate in memory-resident mode to check for viruses during normal processing;
- Be updated as soon as updates are available from the vendor;
- Be configured to prevent connection to the network unless the accessing microcomputer has the latest version of the virus product and update installed.

### **Software Licenses and Use**

Unless specifically approved by the Agency CIT and the agency head, personal or corporate IT equipment shall not have State licensed software installed and shall not be used to process or transmit nonpublic data. Only State owned and authorized computer software is to be used on standalone or networked computer equipment. The State will provide legally acquired software to meet legitimate software needs in a timely fashion and in sufficient quantities to satisfy those needs.

Authorized software packages are those approved by the Agency CIT. Executable modules cannot be downloaded from the Internet unless authorized by the Agency CIT and agency network administrator. Agencies should designate a single point of contact for inquiries about copyright violations, pursuant to federal law.

### **Laptop Security and Mobile Computing**

Laptops and mobile computing devices are not authorized to process or store nonpublic information unless approved in writing by the agency network support administrator, the Agency CIT and the agency head. Laptops and mobile computing devices which include personal digital assistants approved for processing nonpublic information cannot be connected to State networks or systems unless the network or system is certified and accredited for that function. In such cases the IT Security Program will identify the devices that can be used to access the network or the system, the purposes for the access, and the security controls for the connection.

### **Personally Owned Data Processing Equipment**

Personal or contractor owned data processing and data storage equipment (i.e., not owned by the State) are prohibited from accessing systems with nonpublic information and processing or storing nonpublic information unless approved by the agency network support administrator and the Agency CIT.