OFFICE OF STATE FIRE MARSHAL
HAZARDOUS MATERIALS EMERGENCY RESPONSE TEAMS
STANDARD OPERATING GUIDELINE

SUBJECT: STATE OWNED COMPUTER EQUIPMENT	**Number: T-019**
OBJECTIVE: To provide Office of State Fire Marshal Policy on the security of state owned computers on loan by agreement to Regional Hazardous Materials Teams	**OSFM Approved:** Signature on file at OSFM Robert T. Panuccio State Fire Marshal **Adoption Date:** 1/9/98 **Revision Date:** **November 4, 1999**

SCOPE This guideline applies to all Regional Hazardous Materials Response Teams utilizing state owned computer equipment as agreed between the Contractor and the State of Oregon, Office of State Fire Marshal.

GENERAL State owned computer equipment on loan to Contractor's are subject to the same policies and procedures as that equipment located within a state agency. See Attachment #2, which includes OAR 291-038, OSP Policy 705.1, and DAS Policy 03-08. This guideline provides direction on the following policies:

- Authorized Software Installation on State Owned Computers
- State Owned Computer Protection for Computer Viruses
- Use of Personal Software on State Owned Computers
- Use of State Owned Computers for Personal Purposes

All Contractor's personnel utilizing state owned computer equipment must submit a computer security form (Attachment 1) to the OSFM Team Computer Support Administrator, acknowledging that they have read and agree to the guidelines.

I. AUTHORIZED SOFTWARE INSTALLATION ON STATE OWNED COMPUTERS

All software purchased or obtained by OSFM will be delivered to the OSFM System Administrator or the OSFM Team Resource Coordinator before being installed on state owned

computer equipment located at the regional team location. All documentation, including registration material, user manuals, etc. will also be delivered at this time.

Any software purchased by the Contractor's personnel, for installation on state owned computer located at the regional team location will be delivered to the OSFM System Administrator or the OSFM Team Resource Coordinator prior to installation. All documentation, including registration material, user manuals, etc. will also be delivered at this time.

Upon receipt, software will be checked for viruses. OSFM System Administrator or OSFM Team Resource Coordinator will insure software is registered, and an entry will be made on the team inventory indicating the software has been checked and authorized for installation on state owned computer equipment. New software will be evaluated for possible use by all teams.

On a periodic basis, the OSFM System Administrator or the OSFM Team Resource Coordinator will perform physical inventory checks of state owned team computers to insure that only authorized software is installed.

Each Contractor is responsible for the software installed on the computer at their work location. If during periodic inspections, unauthorized computer software is found on state owned computers, this software will be immediately removed and a determination of the person responsible for introducing the software will be made. The person responsible for introducing non-authorized software shall be disciplined in accordance with local policy governing this issue. If the contractor's local agency does not have a policy, the contractor will be responsible for any legal action brought against the State as a result of the use of illegal software. The Contractor shall also be responsible for all costs associated with the removal of unauthorized software, as well as for the costs of any repairs caused by damage related the installation of that software.

REFERENCE: ORS 291.038, DAS Policy 03-08, and OSP Policy 705.1 (Attachment 2)

II. COMPUTER PROTECTION FROM COMPUTER VIRUSES

Any Contractor personnel receiving **software** from any outside source will send that disk to the OSFM System Administrator or OSFM Team Resource Coordinator prior to placing that disk in any state owned computer.

The OSFM System Administrator or OSFM Team Resource Coordinator will use all available virus checking procedures to insure the disk is free of computer viruses before releasing the disk to the user.

Any Contractor personnel receiving a **data disk** from any outside source will forward that disk to the team training officer, or team computer support person to insure the disk is checked for viruses and provide a briefing on the contents of the disk.

If Contractor personnel receives any indication that a virus is present on their computer, they will immediately stop all operations on that computer and report the incident to the OSFM System

Administrator or the OSFM Team Resource Coordinator. The computer will not be used until the machine has been released by one of the above individuals. The computer operator should not, under any conditions, remove a suspect disk from their computer and install it in another computer.

The Contractor will be held financially responsible for any damage to the state owned computer equipment resulting from the introduction of a computer virus.

III. USE OF PERSONAL SOFTWARE ON STATE OWNED COMPUTERS

Use of personally owned, or other non-state owned software, on an agency computer is not permitted.

If during periodic inspections, unauthorized computer software is found on agency computers, this software will be immediately removed and a determination of the person responsible for introducing the software will be made. The person responsible for introducing non-authorized software shall be disciplined in accordance with local policy governing this issue. The Contractor shall also be responsible for all costs associated with the removal of unauthorized software, as well as for the costs of any repairs caused by damage related the installation of that software.

IV. USE OF STATE OWNED COMPUTERS FOR PERSONAL PURPOSES.

Use of state owned computers for personal purposes is prohibited.

As stated in the general section of this SOG, state owned computer equipment on loan to Contractor's are subject to the same policies and procedures as equipment located within a state agency. Included in these policies and procedures is the Department of State Police policy 705.1 subject, microcomputers. Rule #3 of this policy states: "Personal Use: The use of Department microcomputer equipment including hardware, software, documentation, and data is limited only to the support of agency functions. Any unauthorized personal use is strictly prohibited.

In applying this policy to the use of state computers on loan to Regional Hazardous Materials Teams Contractors the following guidelines are provided: State owned computers can be used to support team training, preplanning and response activities. Personal use of state owned computers by any Contractor personnel is strictly prohibited.

ATTACHMENT 1

Office of State Fire Marshal
3565 Trelstad Ave SE
Salem, OR 97317

ACKNOWLEDGMENT OF COMPUTER POLICIES OF THE OFFICE OF STATE FIRE MARSHAL

I, the undersigned, acknowledge that I have read and will comply with the Regional Hazardous Materials Emergency Response Teams SOG-T019 and its attached policies.

I understand personal use of computer equipment owned by the State of Oregon is prohibited.

I also understand that non-compliance with these SOG's may result in discipline in accordance with local policy governing this issue. If the Contractor's local agency does not have a policy, the contractor will be responsible for any legal action brought against the State as a result of the use of illegal software.

Signature	Date
Printed Name	Team Number