Policy # **03-02**
Date Adopted:
02/04/2004

VIBRS Virus Protection Policy
Division of Criminal Justice Services

Approved By:
Francis X. Aumand III
for the VIBRS Advisory Board

Note: This is a **Mandatory Policy**.

1. PURPOSE

1.1. It is in the best interests of all participants in the VIBRS network that all systems are protected with effective virus protection.This policy is to ensure that VIBRS affiliated users (DPS, state agencies, local agencies, and federal) participate in a comprehensive antivirus program.

1.2. The threat from computer viruses continues to increase at an alarming rate. Recent virus outbreaks have spread rapidly, usually coving the entire Internet in less than a day.All available evidence indicates that this trend is likely to continue.Based on these facts, it is essential that proactive measures be taken to prevent the spread of viruses in the VIBRS network.

1.3. Agency/Department participation in the Centrally Managed Antivirus Program administered by Department of Public Safety/Division of Criminal Justice Services (VIBRS Staff) is encouraged but not specifically required. See section 3.2.

2. SCOPE

2.1. This policy applies to every workstation and server on the VIBRS Network. For the purpose of this policy the VIBRS Network consists of devices in the following address ranges:

159.105.1.0 through 159.105.14.255
159.105.245.0 through 159.105.249.255

Any device using private address space (ie. 192.168.nnn.nnn) directly connected to the VIBRS network.

Devices which have direct connectivity to these address ranges are also covered by this policy.

2.2. The word virus where used in this document includes: worms, trojans, viruses, and any other type of malicious software.

3. POLICIES

3.1. The VIBRS Staff shall be responsible for a Centrally Managed Antivirus Program in accordance with this policy.

3.2. An Agency/Department may choose to manage their own virus protection but must do so following the provisions of this policy.An Agency/Department choosing not to be part of the Centrally Managed Antivirus Program must submit a copy of their policy to CJS staff which shows compliance with these provisions.

3.3. The Agency/Department head of an agency not participating in the Centrally Managed Antivirus program shall ensure that all devices used by their agency are protected by an antivirus program which complies with this policy.Upon request by the VIBRS staff, proof of current virus definitions shall be provided.The VIBRS staff shall be allowed to audit compliance with this policy by verifying the following:

- All devices are running an approved anti-virus product.
- A subscription is in place for all devices to ensure that virus definitions remain current.
- Functionality described under section 3.4 is provided.

3.4. All devices on the VIBRS Network must be protected by supported antivirus software.The software must be configured to provide the following functionality:

- Real-time protection.
- Automatic scanning of removable media.
- Scheduled scans at least once a month.
- Automatic updates of virus definitions at least weekly.
- Ability to push out virus definition updates at any time.
- Users are prevented from disabling protection.

3.5. All email from external sources (addresses other than <user>@dps.state.vt.us) shall be scanned for viruses before delivery to the intended recipients inbox.

3.5.1. The centralized scanning of email shall utilize automatic updates of virus definitions.

3.6. Any workstation or server which becomes infected shall be immediately disconnected from the network.

3.7. The VIBRS staff shall be notified as soon as practical of all virus infections that were not quarantined.

3.8. Infected systems shall not be allowed to be reconnected until VIBRS staff has verified, through discussion with the Agency/Department Technical Liaison, that the system is free of all viruses.

3.9. This policy is written to be compliant with both the State of Vermont IT policies regarding anti-virus programs and the FBI CJIS Security policy, version 3.2 dated 9/2003.Changes to either of these policies which increase the level of protection required are automatically included in this policy by reference and will be distributed as necessary.

3.10. Review: This policy shall be reviewed and revised if necessary at least annually.

4. PROCEDURES

4.1. It is the responsibility of each Agency/Department head to ensure that the systems within their control are compliant with this policy.

4.2. A Centrally Managed Antivirus Program shall be available which meets the requirements of this policy.

4.3. The VIBRS Staff shall operate a Centrally Managed Antivirus Program which meets all of the provisions of this policy.All VIBRS participating Agency/Departments shall be allowed to utilize this program.Participation in this program will deem the agency/department in compliance with this policy, provided that they ensure that the VIBRS staff is made aware of all devices in their control.

4.4. The current version of antivirus products from the following vendors are approved:

- Symantec
- NAI
- Sophos
- An unlisted product may be approved by the VIBRS staff.Approval will not be withheld, provided the VIBRS staff can verify that protection is at least equal to the protection provided by the approved products.

4.5. This policy is effective immediately upon acceptance by the VIBRS Advisory board.Current agencies/departments not in compliance will have 30 days to become compliant.New agencies/departments will need to be compliant at the time of connection to the network.

4.6. Exceptions: Devices for which anti-virus software is not available such as print servers, switches, and routers are exempt from this policy.