

HEALTH SCIENCE CENTER HANDBOOK OF OPERATING PROCEDURES

Chapter 5	Information Management & Services	Effective:	July 2003
Section 5.8	Information Security	Revised:	May 2011
Policy 5.8.9	Computer Virus Protection Policy	Responsibility:	Chief Information Security Officer

COMPUTER VIRUS PROTECTION POLICY

Policy

All workstations, whether connected to the Health Science Center network or standalone, must use the Health Science Center information security approved virus protection software and configuration. Use of other virus protection/detection software is not authorized, unless validated by the Department of Information Security and Assurance (ISA), prior to installation on Health Science Center systems. For users who log onto the Health Science Center network with home or other personal systems, or if removable media is shared between home/personal systems and Health Science Center systems, up-to-date, anti-virus protection software on home/personal system is required. The "Acceptable Use of Information Resources", [Section 5.8.10](#), in the *Handbook of Operating Procedures* (HOP), under the "General Standards" section states personnel authorized to access University resources from home, remote, or other designated systems are subject to the same policies as if they were accessing from their office workstation.

The virus protection software must not be disabled or bypassed. Deans, Chairs and Directors are the point of accountability for ensuring that personnel adhere to this policy. Verification of server and desktop virus protection software configuration, signature files, or engine files will be completed by the centralized anti-virus control system, or through normal information security monitoring practices as defined in the HOP, [Section 5.8.13](#), "Security Monitoring".

The settings for the virus protection software must not be altered in a manner that will reduce the effectiveness of the software.

The automatic update frequency of the virus protection software must not be altered to reduce the frequency of updates, unless approved in advance by ISA.

Each file server attached to the University network must utilize the Health Science Center Information Security approved virus protection software and set-up to detect and clean viruses that may infect file shares.

HEALTH SCIENCE CENTER HANDBOOK OF OPERATING PROCEDURES

Chapter 5	Information Management & Services	Effective:	July 2003
Section 5.8	Information Security	Revised:	May 2011
Policy 5.8.9	Computer Virus Protection Policy	Responsibility:	Chief Information Security Officer

Each e-mail gateway must utilize Health Science Center approved e-mail virus protection software and must adhere to the information security rules for the setup and use of this software.

A virus not discovered by the virus protection software constitutes a security incident and must be reported to the [IMS Service Desk](#).

Accountability

Departmental

Deans, Chairs, and Directors are accountable for ensuring that their department remains in compliance with all applicable local, state, and federal information security policies as described in [Section 4.9.2](#) of the HOP, "Management's Responsibilities". If it is determined that the University's network, systems, data, or mission have been put at risk due to a willful or negligent lack of compliance with information security policies, IMS personnel are authorized to terminate service as appropriate to mitigate the risk. Additionally, IMS is authorized to assess the department a service fee for security remediation and/or reconnection of services. The service fee will be charged to the department's state funds account.

Individual

Violations of this policy are subject to disciplinary action as described in [Section 2.1.2](#), of the HOP, "Handbook of Operating Procedures".
