Chapter 5	Information Management & Services	Effective:	July 2003
Section 5.8	Information Security	Revised:	October 2016
Policy 5.8.9	**Malware Prevention Policy**	Responsibility:	Chief Information Security Officer

MALWARE PREVENTION POLICY

Policy

UT Health San Antonio Information Resources and network infrastructure must be continuously protected from threats posed by Malware. All computing devices must be configured with an approved Malware protection software and configuration that is defined to detect and clean Malware that may infect the device or data it holds or accesses.

A. All computing devices owned, leased or under the control of UT Health San Antonio must, to the extent technology permits, execute and keep up to date Malware protection software and adhere to any other Malware prevention and protection measures as required by UT Health San Antonio policies, standards and procedures.

B. The Malware protection software must not be disabled or bypassed, its frequency of updates, modified or its configuration altered to an operating state that no longer meets UT Health San Antonio policies and standards.

C. Verification of Malware protection software configuration signature files or engine files will be performed by a centralized anti-malware administration system, or through other information security monitoring practices.

D. Use of Malware protection not defined in UT Health San Antonio policies or standards must be approved as an exception by the Chief Information Security Officer (CISO).

E. Malware not discovered by Malware protection software or configuration controls is considered a security incident and must be reported to the Chief Information Security Officer.

Email Malware Protection

All email gateways must execute and keep up to date Malware protection software and adhere to any other prevention and protection measures as required by UT Health San Antonio policies, standards and procedures.

Chapter 5	Information Management & Services	Effective:	July 2003
Section 5.8	Information Security	Revised:	October 2016
Policy 5.8.9	**Malware Prevention Policy**	Responsibility:	Chief Information Security Officer

References

- U.T. System Policy 165 Standard 8