8045.S200 Malicious Software Protection

Implements:	CSU Policy #8045.0
Policy Reference:	http://www.calstate.edu/icsuam/sections/8000/8045.0.shtml

1.0 Malicious Software Protection

1.1 All campus information systems must be secured with current versions of campus approved anti-malware software unless otherwise authorized by the campus.

1.2 Campus approved anti-malware software must

a) be capable of detecting, removing, and protecting against malicious software, including viruses, spyware, and adware

b) scan all data in “real time”, including data which is both stored and received by the information system, before data files are opened and before software is executed

c) be capable of tracking and reporting significant actions taken by the software (e.g., deleted or quarantined malware)

d) check for and install updates and signatures at least daily

1.3 Unless appropriately authorized, users must not bypass or turn-off anti-malware software installed on campus information systems.

1.4 Each campus must develop and implement controls to filter and limit unsolicited e-mail messages (e.g., spam, phishing, malware-infected, etc.).

REVISION CONTROL

Revision History

Revision Date	Revised By	Summary of Revisions	Section(s) Revised
11/15/2011	Macklin	Incorporation of ISAC Comments	All
1/3/2012	Moske	Formatted	All
1/11/2012	Macklin	Editing, formatting. Final Review	All
3/4/2013	Shaffer	Incorporated changes based on ISAC review	All
3/11/2013	Macklin	Numbering, Musts.	1

Review / Approval History

Review Date	Reviewed By	Action (Reviewed, Recommended or Approved)
5/21/2013	ISAC	Reviewed, approved and recommended for CISO review
3/3/2014	CISO	CISO Reviewed, approved. Posted