UTEP Standard 8: Malware Prevention

8.1 UTEP Network Infrastructure and other Information Resources must be continuously protected from threats posed by Malware.

(a) Virus protection software must not be disabled or bypassed;

(b) Settings on the virus protection software must not be altered in a manner that will reduce the effectiveness of the software;

(c) Automatic update frequency of the virus protection software must not be altered to reduce the frequency of updates;

(d) Email gateways must utilize properly maintained email virus protection software that is UTEP-approved;

(e) Any server attached to UTEP Information Resources must utilize UTEP-approved virus protection software and must be set up to detect and clean viruses that may infect the server or files shares; and

(f) Any system identified as a security risk due to lack of virus protection may be disconnected from the network or the respective network account may be disabled until adequate protection is in place.

8.2 All computing devices owned, leased, or under the control of UTEP must, to the extent technology permits, execute and keep up to date all required protection software and adhere to any other protective measures as required by applicable Policies and Procedures;

8.3 Any personally owned Computing Device that contains Confidential University Data must be configured to comply with required University security controls while holding such Data;

8.4 Any system identified as a security risk due to a lack of virus protection may be disconnected from the network or the respective network account may be disabled until adequate protection is in place;

8.5 Submit exceptions to the UTEP CISO for approval by completing a Security Exception Request Form.

8.6 Revision History

First Draft:	April 4, 2002
Revised:	September 19, 2002
Revised:	September 10, 2003
Revised:	January 23, 2012
Revised:	May 9, 2017
Approved:	May 9, 2017
	Gerard D. Cochrane Jr., Chief Information Security Officer