Purpose
The purpose of this Standard is to meet security requirements regarding protection of ASU against malware on devices and servers.

Applicability
This Standard applies to all Users of ASU’s computing, internet, and communications resources, including all students, faculty, staff (including student employees), contractors, vendors, consultants, temporary, and other workers for ASU and its Component Units (Users). This Standard also applies to all User devices, servers and embedded systems that operate on behalf of ASU or ASU’s computing, Internet and communication resources.

Standard

User Devices
All devices that use ASU’s technology network, operate on behalf of ASU, or connect to an ASU service must have a supported and current version of anti-malware software installed. This software must be configured to auto-update to protect ASU and its computing, Internet, and communication resources. Use ASU enterprise anti-malware software as appropriate. Encrypted traffic through a security appliance or WAF will need to be decrypted for malicious traffic inspection.

Servers and other Embedded Systems
In addition to the required controls listed above, it is highly recommended that endpoints, servers and other embedded systems use ASU’s network-based sub-controls to defend against malware threats. To meet ASU server security standards and/or ASU data handling standards these additional controls should be implemented as applicable:

- Inspecting network traffic for malware will require a network routing table that funnels traffic through a network security appliance or web application firewall (WAF).
- Configure systems so that they automatically conduct an anti-malware scan of removable media when inserted.
- Use automated monitoring tools for behavior-based anomaly detection to complement traditional signature-based detection.
- Use network-based anti-malware tools to identify executables in all network traffic and use techniques other than signature-based detection to identify and filter out malicious content before it arrives at the endpoint.

Resources
- All ASU Information Security Offices Standards fall under the umbrella ASU Policy ACD 125: Computer, Internet, and Electronic Communications Information Management Policy, which can be found here: http://www.asu.edu/aad/manuals/acd/acd125.html.
- Information about malware protection and anti-malware software can be found at: https://getprotected.asu.edu
- ASU Server Security Standard
- ASU Data Handling Standard

Violations and Enforcement
Enforcement may include removal of systems from the ASU network or removal of access privileges to ASU’s computing, Internet and communication resources, until requirements are met. Violations of this Standard may lead to disciplinary actions or contract termination as applicable.

In a circumstance where compliance may not be immediately possible, the ASU academic or business units must confer with the Information Security Office to develop a plan for moving into compliance within a reasonable amount of time.
Standard Revision
This Standard is subject to review and revision at the direction of, and only after approval by, Chief Information Security Officer. To offer suggestions and/or recommendations, contact the ASU Information Security Office at infosec@asu.edu.