8-805. Malicious software protection.

Software and associated controls must be implemented across agency systems, and logs monitored, to detect and prevent the introduction of malicious code into the state environment. The introduction of malicious code such as a computer virus, worm or Trojan horse can cause serious damage to networks, workstations and state data. Users must be made aware of the dangers of malicious code. The types of controls and frequency of updating signature files, is dependent on the value and sensitivity of the information that could be potentially at risk.

For workstations, virus signature files must be updated at least weekly. On host systems or servers, the signature files must be updated daily or when the virus software vendor's signature files are updated and published. Security patches for software will be applied as defined by the change management process, but all software must have security patches applied as soon as possible.

--

History: Adopted on July 12, 2017.
URL: http://nitc.nebraska.gov/standards/8-805.pdf