20-411 Anti-virus

Previous Revision: ***First Issued:***	January 26, 2018 February 1, 2005	***Effective Date:*** July 11, 2024
Applies to	This policy applies to all computers and mobile devices directly or indirectly connected to the State Board of Administration (SBA) network, including employee owned computers and mobile devices.	
Purpose	The purpose of this Policy is to establish the requirements that must be met by all computers connected to the SBA network, either directly or indirectly (VPN or other remote access), to ensure effective virus detection and prevention.	
Policy	• All SBA computers will have a default standard licensed copy of anti-virus software installed and active. The most current available version of the anti-virus software package will be taken as the default standard. • All computers not managed by the SBA approved to connect to the SBA network must have standard, supported anti-virus software installed. This software must be active, be scheduled to perform virus checks at regular intervals, and have its virus definition files kept up to date. NOTE: Some anti-virus vendors allow their products to also be installed on employee owned devices but it is the personal and financial responsibility of the employee to ensure their devices have default standard anti-virus installed and active prior to connecting to an SBA Network. • Any activities with the intention to create and/or distribute malicious programs onto the SBA network (e.g. viruses, worms, Trojan horses, e-mail bombs, etc.) are strictly prohibited. • If an employee receives what he/she believes to be a virus or suspects that a computer is infected with a virus, it must be reported to the IT department immediately via SBA Support & Office Services. The following information should be reported (if known): virus name, virus symptoms, extent of infection, source of virus, and potential recipients of infected material. • No employee should attempt to destroy or remove a virus, or any evidence of that virus, without direction from the IT department. • Any virus-infected computer will be removed from the network until it is verified as virus-free.	
Governing Law	N/A	
Related Policies	N/A	
Guidelines/Implementation <u>Containment of Virus Incidents</u>		

IT will take appropriate action to contain, remove and recover from virus infections affecting the SBA's network. In order to prevent the spread of a virus, or to contain damage being caused by a virus, IT will remove a suspect computer from the network.

IT will assist with recovery from viruses. This includes advice on containment to stop the spread, help with removing viruses, taking note of information about the incident and advice on how to prevent a recurrence.

Compliance

The Senior Information Technology Officer (SITO) is the owner of this policy and is responsible for compliance. The SITO may develop additional procedures to implement this policy and will maintain sufficient documentation to demonstrate compliance with this policy.