8-504. Minimum workstation configuration.

Improperly configured workstations are at risk to be compromised. Without proper adherence to these workstation security standards, the state is at increased risk to have data lost, stolen, or destroyed. This standard is necessary to protect the state from unauthorized data or activity residing or occurring on state equipment. It is also necessary to reduce the likelihood of malicious activity propagating throughout the state networks or launching other attacks. All managed workstations that connect to the state's network are required to meet these standards. The Office of the CIO is responsible for maintaining these standards and for configuring and managing the hardware, software, and imaging processes for all managed workstations. Workstation standards should be securely maintained and stored in a centralized documentation library. The degree of protection of the workstation should be commensurate with the data classification of the resources stored, accessed, or processed from this computer. The following are minimum workstation configuration standards:

(1) Endpoint security (anti-virus) software, approved by the Office of the CIO, must be installed and enabled;

(2) The host-based firewall must be enabled if the workstation is removed from the state network;

(3) The operating system must be configured to receive automated updates;

(4) The system must be configured to enforce password complexity standards on accounts;

(5) Application software should only be installed if there is an expectation that it will be used for state business purposes. Application software not in use should be uninstalled;

(6) All application software must have security updates applied as defined by patch management standards;

(7) Web browsers settings should be selected or disabled as appropriate to increase security and limit vulnerability to intrusion;

(8) Shared login accounts are prohibited unless approved in advance and configured by IT. Shared login accounts are only acceptable if approved through the policy exception process and alternate mechanisms or access layers exist to ensure the ability to individually identify personnel accessing non-public information;

(9) Shared login accounts are forbidden on multi-user systems where the manipulation and storage of CONFIDENTIAL or RESTRICTED information takes place;

(10) Users need to lock their desktops when not in use. The system must automatically lock a workstation after 5 minutes of inactivity;

(11) Users are required to store all CONFIDENTIAL or RESTRICTED information on IT managed servers, and not the local hard drive of the computer. Local storage may only be used for temporary purposes when the data stored is not sensitive, and where loss of the information will not have any detrimental impact on the state;

(12) All workstations shall be re-imaged with standard load images prior to re-assignment; and

(13) Equipment scheduled for disposal or recycling must be cleansed following agency media disposal guidelines.

--

History: Adopted on July 12, 2017.
URL: https://nitc.nebraska.gov/standards/8-504.pdf