8-403. Network architecture requirements.

The following are network architecture requirements:

(1) All devices that store, access, or process CONFIDENTIAL or RESTRICTED information must not reside in the public tier, and must be protected by at least two firewalls. Firewalls must be placed at perimeter locations so that all critical systems are protected by multiple firewalls and monitoring systems;

(2) All publicly accessible devices must be located in an access-controlled environment, and access credentials must be managed by authorized personnel;

(3) All network devices that contain or process CONFIDENTIAL or RESTRICTED data must be secured with a password-protected screen saver that automatically locks the session after no more than 15 minutes of inactivity;

(4) Devices that include native host-based firewall software in the operating system must have the firewall activated and properly configured, unless the active firewall software compromises the usability of critical applications, or lessens the posture of other security systems;

(5) The state network will have an annual verification of all open ports, protocols, and services for publicly accessible systems;

(6) Any requests for public IP addresses or for additional open ports must be approved by the state information security officer;

(7) Staff will follow approved change control and configuration management procedures for network devices. Patches and hot-fixes recommended by network hardware or software vendors must be installed as soon as practical after testing; and

(8) Services and applications that will not be used must be disabled or removed if such action will not negatively impact operations. Protocols such as telnet, VNC, RDP, or others that do not actively support approved encryption should only be used if they are performed over a secondary encryption channel, such as SSL or IPSEC.

--

History: Adopted on July 12, 2017.
URL: http://nitc.nebraska.gov/standards/8-403.pdf