Remote Administration of Internal Devices Standard

Comment 1

1.0 Standard

It is the responsibility of all State of Nebraska agencies to strictly control remote access from any device that connects from inside the State of Nebraska network to a desktop, server or network device elsewhere within the State of Nebraska network (e.g. from a 10.x.x.x device to a 10.x.x.x device) and ensure that employees, contractors, vendors and any other agent granted remote access privileges adhere to common methods of secure remote administration which shall include but are not limited to:

- Use of strong authentication mechanisms (e.g., strong passwords, public/private key pair, two factor authentication, etc.)
- Utilize device host access (by IP address) lists to restrict remote access
- Use of secure protocols that provide encryption of both passwords and data (e.g., SSL, HTTPS) when reasonable and appropriate, rather than insecure protocols (e.g., Telnet, FTP).
- Grant permissions to only those with a job related need.
- Implement concepts of least privilege to those who are granted permissions.
- Reset factory default device passwords and regularly change any default accounts or passwords for the remote administration utility or application.
- Disable remote capabilities of devices or device accounts if remote access is not employed by the agency.

Comment [JW1]: Does this standard include citizen access to purchase licenses, certificates etc?

Comment [JW2]: Not sure I'm following this statement. At first I thought it said "whoever grants permission has the least privileges in the application" but now I'm not sure what it says.

2.0 Purpose and Objectives

As employees utilize remote access connectivity to conduct business within and amongst the State of Nebraska networks, security becomes increasingly at risk. These standards are designed to minimize the potential exposure from damages which may result from unauthorized use of resources; which include loss of sensitive or confidential data, intellectual property, damage to public image or damage to critical internal systems, etc. The purpose of this document is to define standards for agencies that connect from any State of Nebraska network or device to any State of Nebraska network or device.

Objectives include:

- Provide guidance to State of Nebraska agencies employees, contractors, vendors and any other agent that access any State of Nebraska network or device.
- Provide a high level of security through industry standards and best practices.
- Ensure a solution that is scalable to meet the current and future needs of state agencies, their employees, clients and customers, and business partners.
- Meet federal security requirements for remote access control.

3.0 Applicability

3.1 State Government Agencies

All State agencies, boards, and commissions are required to comply with the standard listed in Section 1.0. All existing Agencies utilizing non-standard remote access applications must convert to the standard listed in Section 1.0 as soon as fiscally prudent, unless the application is exempt.

3.2 Exemption

Exemptions may be granted by the NITC Technical Panel upon request by an agency.

3.2.1 Exemption Process

Any agency may request an exemption from this standard by submitting a "Request for Exemption" to the NITC Technical Panel. Requests should state the reason for the exemption. Reasons for an exemption include, but are not limited to: statutory exclusion; federal government requirements; or financial hardship. Requests may be submitted to

Here is my response to the comments....

Comment1 [JW1] - Does this standard include citizen access to purchase licenses, certificates, etc?

No, this standard is for any remote administration originating on the state's internal network to another device on the state's internal network. Citizens would not have access to the internal state network (10.x.x.x)

Comment2[JW2] - Not sure I'm following this statement. At first I thought it said :whoever grants permission has the least privilege in the application" but I'm not sure what it says.

The concept of least privilege is that you only assign the minimum level of access in order to perform the given task. E.g. if a user has a need to view documents within an application, you grant 'Read-Only' access instead granting 'Full-Admin' access or perhaps 'Read/Write' access. This concept of least privilege is applied to the end user needing the access, not the administrator.

Thanks,

Steven W. Hartman
State of Nebraska
State Information Security Officer
(402) 471-7031 Office
(402) 416-3668 Cellular
steve.hartman@cio.ne.gov