NITC 5-204 (DRAFT)

Technical Panel
of the
Nebraska Information Technology Commission

Standards and Guidelines

Draft Document
30-Day Comment Period

Title: Linking a Personal Portable Computing Device to the State Email System for Data Classified as "Internal Use Only" or "Unclassified/Public"

Notes to Readers:

1. The following document is a draft document under review by the Technical Panel of the Nebraska Information Technology Commission (NITC). This document is posted at http://nitc.ne.gov/standards/comment/.
2. If you have comments on this document, you can submit them by email to rick.becker@nebraska.gov, or call 402-471-7984 for more information on submitting comments.
3. The comment period for this document ends on January 31, 2011.
4. The Technical Panel will consider this document and any comments received at a public meeting following the comment period, currently scheduled for February 8, 2011. Information about this meeting will be posted on the NITC website at http://nitc.ne.gov/.

State of Nebraska
Nebraska Information Technology Commission
Standards and Guidelines

NITC 5-204 (Draft)

Title	Linking a Personal Portable Computing Device to the State Email System for Data Classified as "Internal Use Only" or "Unclassified/Public"
Category	Groupware Architecture
Applicability	Applies to all state government agencies, excluding higher education

1. Purpose

This standard provides for the requirements to connect a personal Portable Computing Device ("PCD") to the State's email system. This standard does not apply to PCDs provided by the agency.

2. Standard

2.1 Procedures for Requesting Authority to Connect a Personal PCD to the State's Email System

2.1.1 Prior to connecting any personal PCD to the State's email system, a request must be submitted to the State Information Security Officer ("SISO") for review. Attachment A is the form to be used to submit a request. Completed forms should be emailed to the SISO at siso@nebraska.gov.

2.1.2 The SISO will review each request. The SISO will either approve or deny a request and communicate the decision to the requesting agency within 14 days.

2.2 Requirements

2.2.1 **Only the Native Microsoft Exchange active-sync method will be used as the syncing method for devices accessing the State email system**.

2.2.2 **Password protection**: Personal smart devices must use a device password for access to the devices functionality. During the process of configuring the device for syncing to the State's email system, the password protection setting will be automatically enabled on the device. Other security controls may be enabled by the State email system at any time.

2.2.3 **Storage of sensitive information**: Personal devices cannot be used to process or store sensitive State related information.

2.2.4 **Physical safeguards**: Appropriate physical security measures should be taken to prevent theft of portable devices and media. Unattended portable computing devices and media must be physically secured.

2.2.5 **Theft or Loss**:

2.2.5.1 **Reporting**: Theft or loss of portable computing devices assumed to contain sensitive information must be reported immediately to the Office of the CIO. Please call the OCIO help desk at 402-471-4636 or 800-982-2468.
2.2.5.2 **Remote data delete**: All devices that are capable of native syncing to the State's email system support the remote data wipe feature. The user is required to take steps to safeguard data which should include initiating the remote wiping process in the case of theft or loss. Mobile email devices can be removed from email access or wiped using the "options/Mobile Devices" selection after logging into your Exchange email account using Outlook Web Access (OWA) at https://mail.nebraska.gov

2.2.6 **Disposal and Reuse**: Personal smart device users must follow the Data Disposal and Reuse policy to properly remove data and software from the PCD before its disposal or reuse.

2.2.7 **Support**: Personal device use is not supported by the State help desk or email team. No State system will be reconfigured in order to make a particular device work and there is no guarantee that a specific device will or will not work with the current system configuration. There is no obligation on the part of the State or Agency to support any personal device.

2.2.8 **Removal of Data**: All State information contained on a device must be removed on request by the Agency Director or State Information Security Officer. The device may be "wiped" or cleared of all information remotely by the State without recourse and without compensation for personal data loss (including but not limited to loss of personal contacts, music, messages and service unavailability).

3. Definitions

3.1 Portable Computing Device (PCD) includes but is not limited to notebook computers; tablet PCs; handheld devices such as Portable Digital Assistants (PDAs), Palm Pilots, Microsoft Pocket PCs, RIM (Blackberry); smart phones; and converged devices.

Attachment A: Request Form (Word Document)

VERSION DATE: Draft - December 14, 2010
HISTORY:
PDF FORMAT: (to be added)

FORM: Request to Link a Personal Portable Computing Device to the State Email System for Data Classified as "Internal Use Only" or "Unclassified/Public"

This is a request to use a personal portable computing device ("PCD") for the purpose of linking the device to the State's email system. The following State exchange email account will be used in conjunction with the access:

Exchange Account: _____

To the limits dictated by the State of Nebraska and Federal laws, agency data and system owners are responsible for determining how critical and sensitive information is for their applications to insure integrity, availability, and confidentiality.

Security Classification Levels:
The NITC Data Security Standard recognizes four basic levels of security classifications that are associated with varying degrees of known risks. (See NITC 8-RD-01: NITC Security Officer Instruction Guide). They can be summarized as follows:

HIGHLY RESTRICTED is for the most sensitive information intended strictly for use within your organization and controlled by special rules to specific personnel. It is highly critical and demands the highest possible security. Not allowed on personal devices.

CONFIDENTIAL is for less sensitive information intended for use within your organization, yet still requires a high level of security. It may be regulated for privacy considerations. (e.g. HIPAA) Do not use this form. Contact the State Information Security Officer.

INTERNAL USE ONLY is for non-sensitive information intended for use within your organization. The security is controlled, but not highly protected. Use this form.

UNCLASSIFIED/ PUBLIC is for information that requires minimal security and can be handled in the public domain. Use this form.

Standards:
All devices irrespective of device ownership that are syncing information with the State's email system must follow these standards:

1. **Only the Native Microsoft Exchange active-sync method will be used as the syncing method for devices accessing the State email system.**

2. **Password protection:** Personal smart devices must use a device password for access to the devices functionality. During the process of configuring the device for syncing to the State's email system, the password protection setting will be automatically enabled on the device. Other security controls may be enabled by the State email system at any time.

3. **Storage of sensitive information**: Personal devices cannot be used to process or store sensitive State related information.

4. **Physical safeguards**: Appropriate physical security measures should be taken to prevent theft of portable devices and media. Unattended portable computing devices and media must be physically secured.

5. **Theft or Loss:**
    a. **Reporting:** Theft or loss of *portable computing devices* assumed to contain *sensitive* information must be reported immediately to the Office of the CIO. Please call the OCIO help desk at 402-471-4636 or 800-982-2468.
    b. **Remote data delete:** All devices that are capable of native syncing to the State's email system support the remote data wipe feature. The user is required to take steps to safeguard data which should include initiating the remote wiping process in the case of theft or loss. Mobile email devices can be removed from email access or wiped using the "options/Mobile Devices" selection after logging into your Exchange email account using Outlook Web Access (OWA) at https://mail.nebraska.gov

6. **Disposal and Reuse**: Personal smart device users must follow the Data Disposal and Reuse policy to properly remove data and software from the PCD before its disposal or reuse.

7. **Support**: Personal device use is not supported by the State help desk or email team. No State system will be reconfigured in order to make a particular device work and there is no guarantee that a specific device will or will not work with the current system configuration. There is no obligation on the part of the State or Agency to support any personal device.

8. **Removal of Data**: All State information contained on a device must be removed on request by the Agency Director or State Information Security Officer. The device may be "wiped" or cleared of all information remotely by the State without recourse and without compensation for personal data loss (including but not limited to loss of personal contacts, music, messages and service unavailability).

Recommendations:

- If your PCD must store sensitive information, periodically delete unnecessary data or email
- If available, PCD users should employ a data delete function to delete information on a device that detects a password attack
- If available, arrange for a remote data deletion service which can remotely delete sensitive information if the device is lost or stolen
- Store PCDs in a secure location or keep physical possession at all times
- Be alert and report unauthorized or suspicious activity to the Nebraska State Patrol immediately
- Do not leave equipment and media taken off the premises unattended in public places.
- Carry PCDs as hand luggage when traveling
- **Tracking:** It is recommended that devices use remote tracking capabilities
- Approved wireless transmission protocols and encryption must be used when transmitting *sensitive* information. *Sensitive* data traveling to and from the PCD must be encrypted during transmission.
- Approved remote access services and protocols must be used when transmitting *sensitive* information. See Remote Access Standard: http://nitc.state.ne.us/standards/security/Remote_Access_Standard_v4_20070222.pdf.

Identified NITC policies that apply to use, access and protecting information:

7-101 Acceptable Use Policy http://nitc.ne.gov/standards/7-101.html

8-101 Information Security Policy http://nitc.ne.gov/standards/security/8-101.pdf

As a reminder: All employees are obligated to protect the data they have access to. The use of the device must conform to all State and Agency use policies.

Violations of policy can result in disciplinary action, up to and including termination.

Individual Justification

The undersigned State representative is requesting to use a personal device for the purpose of accessing and/or storing data with a **security classification level** of UNCLASSIFIED/PUBLIC or INTERNAL USE ONLY and includes the following as supporting justification:

_____

_____

_____ _____

Individual Date

_____ _____

Agency Director Date

Send completed form to the State Information Security Officer at siso@nebraska.gov.

_____ Approved _____ Denied

_____ _____

State Information Security Officer Date