DRAFT

State of Nebraska
Nebraska Information Technology Commission
Standards and Guidelines

NITC 5-204

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.~~ Attachment A is the request form to be used for data classified as “Internal Use” or “Unclassified/Public” and Attachment B is the request form to be used for data classified as “Confidential”. 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 confidential information**: Appropriate safeguards must be utilized when processing or storing sensitive information. At no time shall confidential information received be transferred or stored in a system not meeting required safeguards for information control and storage.

~~**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 ("OCIO"). 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, Removal of data and Reuse**: Personal PCD users must follow the State Data Disposal and Reuse policy to properly remove data and software from the PCD before its disposal and any State and Agency policies that may be implemented must be followed. All State information contained on a device must be removed on request by the Agency Director or State Information Security Officer. Section 5 of NITC Standard 8-101 identifies base requirements for disposal and re-use. The removal of confidential information must be validated. The device may be "wiped" or cleared of all information remotely by the State without recourse and without compensation for personal data loss or the loss of service availability (including but not limited to the loss of personal contacts, music, messages, information and configuration).

~~**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 OCIO. 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 ~~2.2.8~~ **Liability**: The owner of the PCD is potentially liable for all criminal and civil penalties due to loss, theft or misuse of the confidential information accessed and stored on the personal device. The owner of the PCD may also be held liable for cost incurred by the State due to loss, theft, or misuse of confidential information accessed and stored on the personal device.**~~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).~~

2.2.9 **Encryption**: All reasonable attempts must be made to encrypt all confidential information stored on the device. Encryption must be enabled for primary and secondary storage of confidential data if the device includes that functionality.

2.2.10 All information must be protected to the extent required based on applicable State and Federal laws and regulations, and agency policies.

2.2.11 No "jail broken" or devices modified beyond manufacturers expectations will be used to process or store sensitive information.

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.

4. Related Documents

4.1 Acceptable Use Policy (NITC 7-101)

4.2 Information Security Policy (NITC 8-101) (See Secure Disposal or Re-use of Storage Media and Equipment, Section 5; and Asset Classification, Section 6)

4.3 Data Security Standard (NITC 8-102)

Attachment A: FORM: Request to Link a Personal Portable Computing Device to the State Email System for Data Classified as "Internal Use Only" or "Unclassified/Public" ~~Request Form~~ (Word Document)

Attachment B: FORM: Request to Link a Personal Portable Computing Device to the State Email System for Data Classified as "Confidential" (Word Document)

HISTORY: Adopted on March 1, 2011. DRAFT REVISED on May 13, 2011.
PDF FORMAT:

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 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 http://nitc.ne.gov/standards/security/so_guide.pdf). 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.~~Use Attachment B NITC Standard 5-204

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 the standards listed in NITC Standard 5-204: http://nitc.ne.gov/standards/5-204.html~~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 device before its disposal or reuse. Section 5 of NITC standard 8-101 identifies requirements for disposal and re-use.

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:

- Federal and commercial privacy and security safeguards may not allow personal devices to contain certain types of information.
- Periodically delete unnecessary data and email
- If available, the device should employ a data delete function to wipe information from the device after multiple incorrect passwords/PINs have been entered.
- If available, enable device encryption functionality to encrypt local storage.
- Turn off Bluetooth and Wi-Fi connectivity when not specifically in use.
- Limit the use of 3rd party device applications. Unsigned third-party applications pose a significant risk to information contained on the device.
- Store devices in a secure location or keep physical possession at all times
- Carry devices as hand luggage when traveling
- It is recommended that remote tracking capabilities are enable on devices
- Approved wireless transmission protocols and encryption must be used when transmitting *sensitive* information. *Sensitive* data traveling to and from the device must be encrypted during transmission. For browser based access, SSL encryption meets State standards.
- Approved remote access services and protocols must be used when connecting to State equipment. 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

- Data Disposal and re-use: Section 5 page 11.

- Asset Classification: Section 6.

8-102 Data Security Standard Policy

http://nitc.ne.gov/standards/security/Data_Security_Standard_20070918.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

FORM: Request to Link a Personal Portable Computing Device to the State Email System for Data Classified as "Confidential"

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 http://nitc.ne.gov/standards/security/so_guide.pdf). 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 (e.g. PHI, FTI). 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. PII, FISMA, NIST 800-53). All information must be protected to the standards required. Use this form.

INTERNAL USE ONLY is for non-sensitive information intended for use within your organization. The security is controlled, but not highly protected. Use Attachment A NITC Standard 5-204.

UNCLASSIFIED/ PUBLIC is for information that requires minimal security and can be handled in the public domain. Use Attachment A NITC Standard 5-204.

Standards:
All devices irrespective of device ownership that are syncing information with the State's email system must follow the standards listed in NITC Standard 5-204: http://nitc.ne.gov/standards/5-204.html

Recommendations:

- The Office of the CIO does not recommend using personal devices to process and store sensitive information.
- Federal and commercial privacy and security safeguards may not allow personal devices to contain certain types of information.
- Periodically delete unnecessary data and 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. *Confidential* 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.
- All State and Agency policies governing the use of confidential data are required to be followed.

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

- Data Disposal and re-use: Section 5 page 11.
- Asset Classification: Section 6.

8-102 Data Security Standard Policy

http://nitc.ne.gov/standards/security/Data_Security_Standard_20070918.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 CONFIDENTIAL USE ONLY and includes the following as supporting justification:

_____

_____

_____

My signature below identifies I have read and understand the policy requirements and agree to abide by policy to protect the data contained or accessed by the personal device. I acknowledge the risk and accept responsibility for safeguarding the State and the Agency information that is accessed and stored by the personal device.

_____ _____

Individual Date

Agency Director's initials required: _____

This is a high-risk activity not recommended by the State with potential civil and criminal liability and penalties. The State does not endorse the use of personal devices for the processing or storage of confidential information. Allowing this activity significantly increases the possibility of unwanted information disclosure. I acknowledge the risk and accept responsibility for safeguarding the State and the Agency information that is accessed and stored by the personal device.

The Agency Director's signature below identifies the acceptance of increased risk to the agency due to the use of the personal device while also acknowledging possible civil or criminal penalties against the agency or individual from confidential information disclosure.

_____ _____

Agency Director Date

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

_____ Approved _____ Denied

_____ _____

State Information Security Officer Date

_____ _____

State CIO Date