

## FORM: Request to Link a Personal Portable Computing Device to the State Email System for Data Classified as “Managed Access Public” or “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 Information Security Policy recognizes four basic levels of security classifications that are associated with varying degrees of known risks. See NITC 8-101: Information Security Policy (<http://nitc.nebraska.gov/standards/8-101.html>). 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 sensitive information that may include Personally Identifiable Information (PII) intended for use within your organization. This level requires a high level of security and would have a considerable impact in the event of an unauthorized data disclosure. **Do not use this form. Use Attachment B.**

**MANAGED ACCESS PUBLIC** is for non-sensitive information intended for use within your organization. The security is controlled, but not highly protected. **Use this form.**

**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 5-204 (<http://nitc.nebraska.gov/standards/5-204.html>).

### 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 3<sup>rd</sup> 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 NITC 8-303: Remote Access Standard (<http://nitc.nebraska.gov/standards/8-303.html>).

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

NITC 7-101: Acceptable Use Policy (<http://nitc.nebraska.gov/standards/7-101.html>)

NITC 8-101: Information Security Policy (<http://nitc.nebraska.gov/standards/8-101.html>)

NITC 8-102: Data Security Standard (<http://nitc.nebraska.gov/standards/8-102.html>)

**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.

**Please provide the following information:**

Agency	
Agency Number	
Work Phone Number	
Brand of Personal Device (ie: Apple, Motorola, Samsung)	
Type of Personal Device (ie: iPad, Droid, Galaxy)	
OS and Version of Personal Device	
Phone Number of Personal Device (if applicable)	

### 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 MANAGED ACCESS PUBLIC or PUBLIC and includes the following as supporting justification:

\_\_\_\_\_  
\_\_\_\_\_

I understand that in the event of litigation, or potential litigation, my personal device may be subject to discovery requirements up to and including impoundment of the device.

\_\_\_\_\_  
Printed Individual Name                      Individual Signature                      Date

\_\_\_\_\_  
Printed Agency Director Name                      Agency Director Signature                      Date

Send completed form to the State Information Security Officer at [siso@nebraska.gov](mailto:siso@nebraska.gov).

-----

\_\_\_\_\_ Approved      \_\_\_\_\_ Denied

\_\_\_\_\_  
Printed SISO Name                      SISO Signature                      Date