CHAPTER 5

STATE GOVERNMENT ENTERPRISE SYSTEMS

Article.

1. Enterprise Content Management System.
2. Email System.
3. Internet Fax System.
4. Active Directory.

--

ARTICLE 1

ENTERPRISE CONTENT MANAGEMENT SYSTEM

Section.

5-101. Enterprise content management system for state agencies.

(1) Purpose. The purpose of this section is to provide state agencies with a single technical solution for the following: capturing all types of content and storing content electronically; converting and minimizing the number of paper documents the state maintains; facilitating the search and retrieval of electronic documents; retaining and disposing of electronic documents based on retention policies; improving efficiency and accuracy of information exchanges; and unifying document management in a single system to take advantage of economies of scale.

(2) Content and Workflow Standard. State agencies managing content and creating workflow shall use the enterprise content management system that is provided by the Office of the CIO.

(3) Electronic Forms Guideline. State agencies, after consultation with the Office of the CIO, must consider using the e-forms software in the enterprise content management system for any new electronic forms applications.

(4) Exceptions. This section does not apply to: (a) higher education entities; or (b) systems in use by an agency at the time of the adoption of this section. Subsection (b) does not apply if an agency intends to purchase a significate amount of upgrades, new modules, or custom development.

(5) Definition. “Managing content and creating workflow” means the following: capturing paper documents through the use of scanners and storing them in an electronic form; capturing all type of content, including audio, video, e-faxes, emails, word processing documents, and spreadsheets, and storing them in an electronic form; electronic searching and retrieval of captured content; automating records retention and archiving; automating business processes through workflow; or, reducing or eliminating paper document storage.

--

History: Adopted on April 11, 2012. Amended on July 12, 2018.
URL: http://nitc.nebraska.gov/standards/5-101.pdf

5-102. [Repealed.]

--

History: Adopted on November 15, 2011. Repealed on November 8, 2018.
URL: http://nitc.nebraska.gov/standards/5-102.pdf

ARTICLE 2

EMAIL SYSTEM

Section.

5-201. Email standard for state agencies.

All state government agencies, except higher education entities, shall use the email service provided by the Office of the CIO for their workers.

--

History: Adopted on November 17, 1997 (by the Information Resources Cabinet). Amended on June 3, 2004; June 14, 2005; September 18, 2007; March 4, 2008; and July 12, 2018.

URL: http://nitc.nebraska.gov/standards/5-201.pdf

5-202. [Repealed.]

--

History: Adopted on November 13, 2003. Repealed on April 19, 2013.
URL: http://nitc.nebraska.gov/standards/5-202.pdf

5-203. [Repealed.]

--

History: Adopted on November 13, 2003. Repealed on April 19, 2013.
URL: http://nitc.nebraska.gov/standards/5-203.pdf

5-204. Email; linking a personal portable computing device to the state system.

(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) Procedures. Prior to connecting any personal PCD to the state's email system, a request must be submitted to the state information security officer for review. Attachment A is the request form to be used for data classified as MANAGED ACCESS PUBLIC or PUBLIC, and Attachment B is the request form to be used for data classified as CONFIDENTIAL. Completed forms should be emailed to the state information security officer at siso@nebraska.gov. The state information security officer will review each request. The state information security officer will either approve or deny a request and communicate the decision to the requesting agency within 14 days.

(3) Requirements. The following are the requirements for linking a personal portable computing device to the state email system:

(a) Active-sync. Only the native Microsoft Exchange active-sync method will be used as the syncing method for devices accessing the state email system;

(b) Password protection. The device must use a password for access to the device’s 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;

(c) Storage of CONFIDENTIAL information. Appropriate safeguards must be utilized when processing or storing sensitive information. At no time shall CONFIDENTIAL information be transferred or stored in a system not meeting required safeguards for information control and storage;

(d) 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;

(e) Theft or loss; 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 Office of the CIO Service Desk at 402-471-4636 or 800-982-2468;

(f) Theft or loss; 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;

(g) Disposal; removal of data; 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. 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);

(h) Support. Personal device use is not supported by the Office of the CIO. 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;

(i) 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;

(j) 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;

(k) Device modifications. No "jail broken" or devices modified beyond manufacturers expectations will be used to process or store sensitive information; and

(l) Legal requirements. All information must be protected to the extent required by applicable state and federal laws, regulations, and agency policies.

(4) Portable computing device, defined. Portable computing device means and includes the following devices: notebook computers; tablet PCs; handheld devices such as portable digital assistants (PDAs), Palm Pilots, Microsoft Pocket PCs, and RIM (Blackberry) devices; smart phones; and converged devices.

--

History: Adopted on March 1, 2011. Amended on June 30, 2011; February 14, 2012 (Technical Panel); December 10, 2013; February 11, 2014 (Technical Panel); and July 12, 2017.
URL: http://nitc.nebraska.gov/standards/5-204.pdf

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 email account will be used in conjunction with the access:

Exchange Account: _____

To the limits dictated by state 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. They can be summarized as follows:

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.pdf).

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 third-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; and
- 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.

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.

_____ Approved _____ Denied

_____	_____	_____
Printed SISO Name	SISO Signature	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 for the purpose of linking the device to the state's email system. The following state email account will be used in conjunction with the access:

Exchange Account: _____

To the limits dictated by state 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. They can be summarized as follows:

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. Use this form.

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

PUBLIC is for information that requires minimal security and can be handled in the public domain. Use Attachment A.

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.pdf).

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;
- 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; and
- All state and agency policies governing the use of CONFIDENTIAL data are required to be followed.

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 CONFIDENTIAL 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. 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

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.

_____	_____	_____
Printed Agency Director Name	Agency Director Signature	Date

Send completed form to the state information security officer at siso@nebraska.gov.

_____ Approved _____ Denied

_____	_____	_____
Printed SISO Name	SISO Signature	Date

_____	_____	_____
Printed CIO Name	CIO Signature	Date

ARTICLE 3

INTERNET FAX SYSTEM

Section.

5-301. Internet fax standard for state agencies.

All state government agencies, except higher education entities, shall use the OCIO Internet Fax System provided by the Office of the CIO for computer-based fax services, including desktop and application-based faxing.

This standard does not apply to the use of stand-alone fax machines connected directly to a telephone line.

--

History: Adopted on September 30, 2003. Amended on November 30, 2009 and July 12, 2018.
URL: http://nitc.nebraska.gov/standards/5-301.pdf

ARTICLE 4

ACTIVE DIRECTORY

Section.

5-401. Active Directory; user photographs.

(1) Purpose. Microsoft Active Directory has an attribute ("thumbnailPhoto") to store a thumbnail photograph of each user. Other applications, including Microsoft Outlook and the Exchange Global Address List, will display these photographs automatically in the context of providing information about the user. This policy provides guidance on the use of this feature in the state's shared Active Directory forest.

(2) Optional Use. Each agency has the option to use, or not use, the thumbnail photograph functionality in the state's shared Active Directory forest.

(3) Requirements. If an agency chooses to use the thumbnail photograph functionality, the following requirements will apply:

(a) Image file type: JPEG;

(b) Image file size: 10 KB or smaller;

(c) Image file name: Same as the user login ID plus the .jpg extension (for example, john.doe.jpg);

(d) Image size: 96x96 pixels is recommended;

(e) Image content: A recent head-and-shoulders photograph of the user (not an avatar, icon, drawing, etc.);

(f) The agency is responsible for obtaining photographs of their users;

(g) The agency must use the mechanism provided by the Office of the CIO for uploading agency image files; and

(h) The agency must not modify the Active Directory “thumbnailPhoto” attribute directly.

--

History: Adopted on December 10, 2013. Amended on July 12, 2018.
URL: http://nitc.nebraska.gov/standards/5-401.pdf