Office of Technology and Information Services

State of South Carolina Information Security and Privacy Data Handling Guidelines

V.1.0 (01.04.2018)

admin

THE SOUTH CAROLINA
DEPARTMENT *of* ADMINISTRATION

Contents

Revision History

Update this table every time a new edition of the document is published.

Date	Author	Title	Version	Notes
01.04.2018	Enterprise Privacy Office		1.0	Posted

Purpose

These guidelines define the recommendations for handling data by state of South Carolina (State) agencies. These guidelines are compliant with the SCDIS Information Security Program Master Policy and with the controls established in SCDIS-200 Information Security and Privacy Standards. This information can be found by visiting http://www.admin.sc.gov/technology/information-security/policies-and-procedures .

Definitions

Within the scope of this document, the following terms are used as defined below.

- **Agency** – Refers to state agencies, including institutions, departments, divisions, boards, commissions and authorities.

Roles

- **Agency Privacy Liaison** – The individual or their designee who is responsible for ensuring agency compliance with the state privacy policies.
- **Agency Security Liaison** – The individual or their designee who is responsible for addressing information security issues.
- **Data Custodian** – Individual that manages the application/system that contains the business process data (e.g., IT system administrator).
- **Division of Information Security (DIS)** – An operating unit under the South Carolina Department of Administration (Admin), responsible for a variety of statewide policies, standards, programs and services relating to cybersecurity and information systems.
- **Division of Technology Operations (DTO) Service Desk** – An operating unit under Admin's DTO serving as a single point of contact for Admin's customers who need assistance with IT services. The DTO Service Desk will assist with the tracking and management of incidents.
- **Enterprise Privacy Office (EPO)** – An operating unit under Admin, responsible for advising state agencies on the management of personal information as well as establishing, assessing and enhancing privacy protection policy, training and compliance measures.

Data Classification

The Information Security and Privacy Policy – Data Protection and Privacy v1.0, effective October 30, 2013, requires that all state of South Carolina agencies and institutions classify their information assets into specified categories according to the Data Classification Schema and Guidelines, regardless of form whether electronic, hard copy or intellectual property. This information can be found by visiting http://admin.sc.gov/technology/enterprise-privacy/policy-and-guidance. Agency information shall be classified into one of the following categories:

- **Public** – Information intended or required to be shared with the public.
- **Internal Use** – Non-sensitive information used in the daily operations of an agency.

- **Confidential** – Sensitive information used or held by an agency. Considerable loss or harm could occur because of unauthorized access, use or disclosure of this information.
- **Restricted** – Highly sensitive information used or held by an agency. Statutory or regulatory penalties, notification provisions, or other mandates could result if the information is accessed, used or disclosed in an unauthorized manner.

Security Requirements for Handling Information

"Handling" information includes storing, viewing, using, updating, deleting, transferring or destroying data. Based upon how data are classified (public, internal use, confidential or restricted) and its form, that data may have certain safeguards that need to be applied when handled.

These handling requirements are intended for the use and storage of agency data located on state-owned resources, and represent the minimum requirements for handling of data in any form by state workforce. In some cases, more stringent data handling procedures may be required due to regulatory, contractual or policy obligations. Agency workforce is urged to contact their security or privacy liaisons for guidance in cases that present handling questions or security concerns.

These data handling requirements are divided into three categories.

1. Printed Information (paper, microfiche and/or microfilm).
2. Electronically stored (digital) Information.
3. Electronically transmitted Information.

These handling requirements are reviewed periodically, and whenever technological capabilities evolve, by the Division of Information Security, Division of Technology Operations, and the Enterprise Privacy Office.

Handling of Printed Information (paper, microfiche, microfilm)

How printed information should be handled is based upon the category of data that is contained in the document. Printed information should be handled according to the highest classification level of data contained in the document. For example, if a document contains both public and restricted information, then the document should be handled according to the requirements for protecting restricted information. Agency staff are urged to contact their security or privacy liaison for guidance in situations that present handling questions or security concerns.

Actions (press Ctrl key and click on title below, to jump to section)

- Printing Hard Copy Information
- Storing Printed Documents
- Duplicating and Distributing Paper Documents
- Mailing Paper Documents via Interagency Mail Service or External Carrier
- Internal Transfer of Paper Documents Within a Building
- Faxing Paper Documents

- Faxing Using Machines with Data Connections
- Labeling Paper Documents
- Disposing of Printed Documents

Printing Hard Copy Information

This action covers printing documents from applications, databases or other file stores. Once the data are reproduced in paper form, agency staff should follow the following handling requirements for printed information.

Classification	Requirements
Public	• No special requirements.
Internal Use	• Unattended printing is allowed if physical access controls are in place to prevent unauthorized viewing of a printout.
Confidential	• Unattended printing is allowed if physical access controls are in place to prevent unauthorized viewing of a printout. • Printouts containing confidential information should be picked up immediately upon print.
Restricted	• Unattended printing is allowed if physical access controls are in place to prevent unauthorized viewing of a printout. • Printouts containing restricted information should be picked up immediately upon print.

Storing Printed Documents

Classification	Requirements
Public	• No special requirements.
Internal Use	• Store in a secured location when not in use.
Confidential	• Store in a secured location when not in use. Storage cabinets should be locked when not in use, or when personnel are not present, and behind two locks (e.g., office, cabinet). • Access to documents with confidential data should be limited to only those individuals with a legal right to access the information. • Key inventories and access to locations storing confidential data should be monitored closely and keys/access granted only to individuals with a legitimate need to access the documents in the storage location.
Restricted	• Store in a secured location when not in use. Storage cabinets should be locked when not in use, or when personnel are not present, and behind two locks (e.g., office, cabinet).

	• Access to documents with restricted data should be limited to only those individuals with a legal right to access the information. • Key inventories and access to locations storing restricted data should be monitored closely and keys/access granted only to individuals with a legitimate need to access the documents in the storage location.

Duplicating and Distributing Paper Documents

This action covers the duplication and distribution of printed documents only. Copies should only be made when needed for a specific purpose. Copies should not be distributed or forwarded unless there is a business need to do so. It is also important for staff to understand how the distributed materials will be used and disposed of.

Classification	Requirements
Public	• No special requirements.
Internal Use	• No special requirements.
Confidential	• Documents should not be left unattended on the copier. • The receiver of the document containing confidential information must not distribute further without permission of the information owner. • Where necessary, the information owner should designate data that must not be further duplicated or distributed.
Restricted	• Documents should not be left unattended on the copier. • The receiver of the document containing restricted information must not distribute without permission of the information owner. • Where necessary, the information owner should designate data that must not be further duplicated or distributed.

Mailing Paper Documents via Interagency Mail Service or External Carrier

This action includes mailing paper documents via the Interagency Mail Service or an external carrier such as the United States Postal Service or FedEx. This handling requirement assumes a valid business need for the mailing of paper-based documents.

Classification	Requirements
Public	• No special requirements.
Internal Use	• No special requirements.
Confidential	• No classification marking on external envelope. Envelope is to be sealed in such a way that tampering would be indicated upon receipt.

	• Delivery service must include receipt acknowledgement sent back to sender.
Restricted	• No classification marking on external envelope. Envelope is to be sealed in such a way that tampering would be indicated upon receipt. • Delivery service must include receipt acknowledgement sent back to sender.

Internal Transfer of Paper Documents within a Building

This action includes transferring of paper documents between staff located within a common location, such as within the same building. This handling requirement assumes a valid business need for the sharing of paper-based documents.

Classification	Requirements
Public	• No special requirements.
Internal Use	• No special requirements.
Confidential	• Documents containing confidential information should be placed inside of a folder and the Sensitive Contents Cover Sheet (Appendix A) should be attached to the outside of the folder.
Restricted	• Documents containing restricted information should be placed inside of a folder and the Sensitive Contents Cover Sheet (Appendix A) should be attached to the outside of the folder.

Faxing Paper Documents

When sending faxed documents, documents may be sent either directly from their electronic form, or more traditionally, by sending a paper document through a fax machine. This handling requirement applies to sending faxes in the traditional, paper-based, manner. This handling requirement assumes a valid business need for sending or receiving a faxed document.

Classification	Requirements
Public	• If a document is received in error, notify the sender. • If a document is faxed to the wrong person, notify the recipient.
Internal Use	• If a document is received in error, notify the sender. • If a document is faxed to the wrong person, contact the recipient and request that the any paper document be shredded, and any electronic copy be securely deleted.
Confidential	• Receiving faxes: Unattended printing is allowed if access controls are in place to prevent unauthorized viewing of a printout. Printouts are to be picked up as soon as possible and responsibility for monitoring

	the fax machine is assigned to ensure prompt removal and delivery of documents to recipients. • If a document containing confidential information is received in error, immediately notify the sender. • Sending faxes: Before faxing, verify the recipient's fax number. Use a cover sheet that includes a confidentiality notice, prominently displayed, example below. • If a document containing confidential information is faxed to the wrong person, immediately report according to your agency's incident response procedures.
Restricted	• Receiving faxes: Unattended printing is allowed if access controls are in place to prevent unauthorized viewing of a printout. Printouts are to be picked up as soon as possible and responsibility for monitoring the fax machine is assigned to ensure prompt removal and delivery of documents to recipients. • If a document containing confidential information is received in error, immediately notify the sender. • Sending faxes: Before faxing, verify the recipient's fax number. Use a cover sheet that includes a confidentiality notice, prominently displayed, example below. • If a document containing restricted information is faxed to the wrong person, immediately report according to your agency's incident response procedures.

Sample Confidentiality Notice

WARNING: CONFIDENTIALITY NOTICE

This cover sheet and all materials enclosed with this transmission are the private, confidential property of the sender. This message is intended solely for the individual or entity to which it was addressed, and may contain information that is privileged, confidential and exempt from disclosure under applicable law. If you are not the intended recipient, or the employee or agent responsible for delivering the message to the intended recipient, you are hereby notified that any disclosure, dissemination, copying or the taking of any other action relevant to the contents of this transmission are strictly prohibited. If you have received this transmission in error, please secure the materials and notify us immediately at (xxx) xxx-xxxx or xxxx@xxxxx.sc.gov. If you cannot reach us, please securely shred or erase all information received. Thank you.

Faxing Using Machines with Data Connections

This handling requirement applies to faxed documents sent electronically from or to a fax and transmitted through a server. It assumes a valid business need for sending or receiving a faxed document.

Classification	Requirements
Public	• If a document is received in error, notify the sender. • If a document is faxed to the wrong person, notify the recipient.
Internal Use	• If a document is received in error, notify the sender. • If a document is faxed to the wrong person, contact the recipient and request that the electronic copy be securely deleted.
Confidential	• Receiving faxes: If a document containing confidential information is received in error, immediately notify the sender and your privacy liaison. • Sending faxes: Before faxing, verify the recipient's fax number. Use a cover sheet that includes a confidentiality notice, example below. • If a document containing confidential information is faxed to the wrong person, immediately report according to your agency's incident response procedures. • Transmission/File Storage: Transmission between the fax and server should be encrypted. Access should be controlled to any shared file folders to personnel with a business need to access the documents and access-level auditing enabled. The fax should be located in a secure zone, with no access from open networks.
Restricted	• Receiving faxes: If a document containing restricted information is received in error, immediately notify the sender and your privacy liaison. • Sending faxes: Before faxing, verify the recipient's fax number. Use a cover sheet that includes a confidentiality notice, example below. • If a document containing restricted information is faxed to the wrong person, immediately report according to your agency's incident response procedures. • Transmission/File Storage: Transmission between the fax and server should be encrypted. Access should be controlled to any shared file folders to personnel with a business need to access the documents and access-level auditing enabled. The fax should be located in a secure zone, with no access from open networks.

Sample Confidentiality Notice

WARNING: CONFIDENTIALITY NOTICE

This cover sheet and all materials enclosed with this transmission are the private, confidential property of the sender. This message is intended solely for the individual or entity to which it was addressed, and may contain information that is privileged, confidential and exempt from disclosure under applicable law. If you are not the intended recipient, or the employee or agent responsible for delivering the message to the intended recipient, you are hereby notified that any disclosure, dissemination, copying, or the taking of any other action relevant to the contents of this transmission are strictly prohibited. If you have received this transmission in error, please secure the materials and notify us immediately at (xxx) xxx-xxxx or xxxx@xxxxx.sc.gov. If you cannot reach us, please securely shred or erase all information received. Thank you.

Labeling Paper Documents

This action covers labeling of paper documents. Some areas may choose to label their documents in order to ensure appropriate handling within the agency.

Classification	Requirements
Public	• No special requirements.
Internal Use	• No special requirements.
Confidential	• Certain documents are to be labeled as "Confidential" regardless of internal or external use.
Restricted	• Certain documents are to be labeled as "Confidential" regardless of internal or external use.

Disposing of Printed Documents

A document can only be considered as public if all information present is intended or required to be shared with the public. Unless you are certain all of the information is public, treat it as non-public.

Classification	Requirements
Public	• No special requirements.
Internal Use	• The document should be destroyed beyond any ability to recover, in compliance with SCDIS-501 Information Media Disposal Procedure (https://admin.sc.gov/files/SCDIS-501-Information-Media-Disposal-Procedure.pdf).
Confidential	• The document should be destroyed beyond any ability to recover, in compliance with SCDIS-501 Information Media Disposal Procedure (https://admin.sc.gov/files/SCDIS-501-Information-Media-Disposal-Procedure.pdf).

Restricted	• The document should be destroyed beyond any ability to recover, in compliance with SCDIS-501 Information Media Disposal Procedure (https://admin.sc.gov/files/SCDIS-501-Information-Media-Disposal-Procedure.pdf).

To destroy a document means to physically destroy it beyond any ability to recover the data on the document. Shredding a paper document is an appropriate destruction method. The use of a contracted vendor for confidential document destruction is acceptable for disposal of all classifications of paper-based information unless there are additional requirements specific to that information (e.g., the retention schedule, terms of an executed Non-Disclosure Agreement, or any other contract with disposition requirements). The possessor of the information should consider all such requirements before destroying documentation.

Electronically-stored (digital) Information

How electronic information should be handled is based upon the category of data that is contained in the electronic file. Electronic information must be handled according to the highest classification level of data contained in the file. For example, if a file contains both public and restricted information, then the file should be handled according to the restricted classification. Agency staff are urged to contact their security liaison for guidance in cases that present handling questions or security concerns.

Actions (press Ctrl key and click on title below, to jump to section)

- Storage on Servers, Authentication Required
- Storage on Servers, No Authentication Required
- Storage on Electronic Media
- Disposal of Physical Electronic Media
- Voicemail
- Access to Data in Applications and Databases

Storage on Servers, Authentication Required

This category includes file storage servers or other storage spaces where access is protected via authentication credentials. This category can also include storage on vendor solutions where the agency has determined that there is a business need for the vendor's solution and has entered into a contract with the vendor. Authentication credentials are used to access the vendor's solution.

As a result, this category includes the following storage scenarios:

- Data stored on servers that can be accessed on an agency workstation as part of a user's workstation profile.
- Data stored on servers that can be accessed remotely via a File Transfer Protocol where authentication credentials must be provided before a user can access the files. Data stored on

servers that can be accessed remotely via the use of a tool through the internet where authentication credentials must be provided before a user can access the files.
- Web spaces with information intended for agency dissemination only, and where authentication credentials must be provided before a user can access data.
- Data stored on third-party hosted-servers where the agency has determined that there is a business need for the vendor's solution, the agency has entered into a contract with the vendor, and authentication credentials are used to access the vendor's solution.

DTO-provided central and departmental servers are among the most secure places to store agency restricted data. Some restricted data types (e.g., protected health information, banking information or credit card information) may be subject to laws that require the data to be stored in an encrypted form or require the data to be restricted to specific authorized users only. Some common laws that may require additional security precautions include HIPAA (for protected health information), FERPA (for student information), GLBA (for financial account information), and PCI (for credit card information). Contact your security liaison if you have questions about how these laws may apply to the data you are using.

Classification	Requirements
Public	• No special requirements.
Internal Use	• Access controls should restrict access to only individuals with a legitimate business need to access the data.
Confidential	• Access controls should restrict access to only individuals with a legitimate business need to access the data. • Additional requirements applied, as determined by the agency, in accordance with state policy.
Restricted	• Access controls should restrict access to only individuals with a legal right and business need to access the data. • Additional requirements applied subject to any applicable laws, as discussed above.

Storage on Servers, No Authentication Required

This category includes file storage servers where the data stored on those servers can be accessed via internet, and where that access does not require the use of authentication credentials to access the files. Therefore, this category includes the following storage scenarios:

- Agency webpages with information intended for public dissemination.
- Files on servers that can be accessed remotely via the use of a tool through the internet where authentication credentials are not required before access.

Data custodians are urged to exercise caution when providing access to agency data without appropriate authentication. For instance, when allowing non-agency users to access agency data, a data custodian must make sure that there are adequate protections (e.g., password protection, encryption and secure communication channels) in place to protect certain categories of data.

Classification	Requirements
Public	• No special requirements.
Internal Use	• Not allowed.
Confidential	• Not allowed.
Restricted	• Not allowed.

Storage on Electronic Media and Portable Devices

This category includes all media on which electronic data can be stored, including, but not limited to: internal and external hard drives, laptops, tablet computers, smartphones, magnetic tapes, diskettes, CDs, DVDs and USB storage devices.

Data custodians are reminded that DTO-supported central and departmental servers, where authentication is required, are the best place to store all categories of agency data, particularly restricted data. Data custodians are encouraged to consult their security liaison if confidential or restricted data must be stored on electronic media (other than on agency servers).

Data custodians should exercise caution and common sense when storing agency data on personally owned computing devices (e.g., home computers), including electronic media. In almost all instances, agency internal use, confidential or restricted data should never be stored on agency staff's personally owned computing devices.

Classification	Requirements
Public	• No special requirements.
Internal Use	• Physical security should be employed for storage of removable media when not in use (e.g., locked cabinet).
Confidential	• Storage on removable devices is not recommended. • If necessary to store data on removable devices for limited purposes, electronic media must be properly secured from loss, theft, and unauthorized access according to the SCDIS-200 Information Security and Privacy Standards, sections 7.100, 7.200 and 7.300 (https://admin.sc.gov/files/SCDIS-200-InformationSecurityandPrivacyStandards.xlsx).
Restricted	• Storage on removable devices is not recommended. • If necessary to store data on removable devices for limited purposes, electronic media must be properly secured from loss, theft, and unauthorized access according to the SCDIS-200 Information Security and Privacy Standards, sections 7.100, 7.200 and 7.300

	(https://admin.sc.gov/files/SCDIS-200-InformationSecurityandPrivacyStandards.xlsx).

Disposal of Physical Electronic Media

This category applies to any electronic media, purchased or leased, that is ready for transfer either for an alternate use within the agency, for return to a lessor, or for disposal as surplus.

The scope of this category is intended to apply to any electronic media on which data can be stored. Storage media may be a component of multifunction devices, scanners, printers and fax machines whether leased or owned by the agency. It may include devices such as, computers, magnetic hard drives, solid-state hard drives, flash memory cards and drives, printers, optical storage devices, cellular phones and handheld computing devices. Departments leasing equipment with data storage capabilities are encouraged to make sure all lease agreements include provisions about securely deleting or replacing device hard drives once the device is no longer in use at the agency (and before the device leaves the agency's property). Departments can contact their security liaison for assistance, if needed.

Classification	Requirements
Public	• Erase the media according to SCDIS-501 Information Media Disposal Procedure (https:/admin.sc.gov/files/SCDIS-501-Information-Media-Disposal-Procedure.pdf), or destroy the storage media beyond the ability to recover.
Internal Use	• Erase the media according to SCDIS-501 Information Media Disposal Procedure (https:/admin.sc.gov/files/SCDIS-501-Information-Media-Disposal-Procedure.pdf), or destroy the storage media beyond the ability to recover.
Confidential	• Erase the media according to SCDIS-501 Information Media Disposal Procedure (https://admin.sc.gov/files/SCDIS-501-Information-Media-Disposal-Procedure.pdf), or destroy the storage media beyond the ability to recover.
Restricted	• Erase the media according to SCDIS-501 Information Media Disposal Procedure (https://admin.sc.gov/files/SCDIS-501-Information-Media-Disposal-Procedure.pdf), or destroy the storage media beyond the ability to recover.

Voicemail

Many agencies use a computerized messaging system for voicemail services. The messaging system allows you to manage your voicemail messages via telephone and/or computer through web access. Voicemail messages can also be forwarded to an e-mail address (e.g., wav or proprietary .vbk attachment.)

Agency workforce must exercise care in using the messaging system and in forwarding voicemail messages to e-mail as an attachment. In some instances, this "forward to e-mail" service must be disabled for an entire area in order to prevent the transmission of restricted information via e-mail. This is particularly important with respect to the e-mail forwarding function in areas that might be covered by HIPAA. Agency workforce is urged to contact the agency privacy liaison for guidance in these cases.

Classification	Requirements
Public	• No special requirements.
Internal Use	• No special requirements.
Confidential	• Agency workforce who anticipate the receipt of confidential information in voicemails should not utilize the e-mail-forwarding feature. • If confidential information is included in a received voicemail message, delete the message and associated e-mail messages immediately upon receipt.
Restricted	• Agency workforce who anticipate the receipt of restricted information in voicemails should not utilize the e-mail-forwarding feature. • If restricted information is included in a received voicemail message, delete the message and associated e-mail messages immediately upon receipt.

Access to Data in Applications and Databases

This category includes access to data in agency applications and databases for business operations purposes. In most cases, access to information and the ability to use, manipulate, or delete that information is based on roles defined by business areas. Users are urged to contact the business process owner or privacy liaison for guidance in situations that present data handling questions.

Electronically-transmitted Information

How information should be transmitted is based upon the category of data that is contained in the electronic file. Agency staff are encouraged to use the most secure means possible to transmit agency data. It is expected that agencies will move toward encrypted transmission options over time, and encourage their vendors and exchange agencies to move in this same direction. Contact your IT Support Services representative for the approved encryption methods for your agency.

Information should be transmitted in the manner applicable to the highest classification level of data contained in a file or document. For example, if a file contains both Public and Restricted information, then the file should be transmitted according to the restricted classification. Agency workforce is urged to contact their security liaison for guidance in cases that present handling questions or security concerns.

Actions

- Electronic Communications

Electronic Communications

This category includes almost all electronic communications. It includes communication mechanisms such as e-mail, instant messaging, FTP, connections to administrative applications, and wireless or cellular technologies.

Classification	Requirements
Public	• No special requirements. • Note that for electronic communications requiring password-protected login, the password is considered confidential information. Consequently, login actions must be conducted through an encrypted connection.
Internal Use	• Encryption suggested. • Note that for electronic communications requiring password-protected login, the password is considered confidential information. Consequently, login actions must be conducted through an encrypted connection.
Confidential	• Encryption required. Include a confidentiality notice in the e-mail, example below.
Restricted	• Encryption required. Include a confidentiality notice in the e-mail, example below.

An agency's Confidential and Restricted data should never be transmitted over any unencrypted network, nor stored on any unencrypted removable storage media. It must be transmitted and/or stored using approved encrypted protocols (i.e. HTTPS, SecureFTP, Secure Email, etc.) with approved encryption algorithms (i.e. AES256).

For agencies using email services provided by the Division of Technology Operations, email can be sent securely by following the procedures outlined in Appendix B – Secure E-mail.

Due to the complexities of approved services, protocols and algorithms, agency workforce must use only approved data handling solutions and should consult with their security liaison about questions related to properly protecting electronic communications.

For e-mail transmissions that include Confidential or Restricted data, a confidentiality notice should be included, sample below.

Sample Confidentiality Notice

This communication, including any attachments, is for the sole use of the intended recipient(s) and may contain confidential information, legally privileged information, and/or information that is protected from disclosure by federal and/or state law. If you are not the intended recipient(s), please contact the sender at (803) xxx-xxxx and destroy all copies of the original message beyond the ability to recover. Any unauthorized review, use, disclosure or distribution is prohibited.

Guidance

The Division of Information Security and Enterprise Privacy Office shall provide guidelines, document templates, tutorials or other forms of assistance for the use of agencies by distribution means appropriate to the nature and sensitivity of the content, upon request.

DIS Policies, Procedures and Guidelines (http://admin.sc.gov/technology/information-security/policies-and-procedures).

EPO Policy and Guidance (http://admin.sc.gov/technology/enterprise-privacy/policy-and-guidance).

Appendix A - Sensitive Contents Cover Sheet

This Sensitive Contents Cover Sheet should be attached to the first page of a folder holding documents that include sensitive information, for use in transferring documents to workforce within the same physical location, e.g., the same building.

admin
THE SOUTH CAROLINA
DEPARTMENT *of* ADMINISTRATION

CONFIDENTIAL OR RESTRICTED CONTENTS DATA COVER SHEET

TO BE USED WITH ALL DOCUMENTS CONTAINING PERSONAL INFORMATION

Contents shall not be disclosed, discussed or shared with individuals unless they have a direct need-to-know in the performance of their official duties. Deliver this/these document(s) directly to the intended recipient.
DO NOT leave with a third party.

The enclosed document(s) may contain personal or privileged information. Unauthorized disclosure of this information may result in disciplinary action up to an including termination. If you are not the intended recipient or believe that you have received this document(s) in error, do not copy, disseminate or otherwise use the information and contact the owner/creator or your privacy liaison regarding the document(s).

SENSITIVE CONTENTS DATA COVER SHEET

Appendix B - Secure E-mail

Sending a Secure E-mail

The State’s DTO-supported e-mail system can be used to send sensitive information either inside the State network or to external parties. The following procedure should be used to ensure that appropriate encryption is applied to the transmission.

1. Send the sensitive e-mail to recipient(s) with [secure] in the header. Note that his must include the brackets [ ].
2. The system will automatically send separate message(s) to recipient(s) with the instructions.

Receiving a Secure E-mail from an Account Outside of the State E-mail System

1. If this is your first time getting a message in the Secure Mail system, you should have received a second e-mail that would instruct you to activate your account. Click on Activate your personal account. You will be asked to enter preferred sign in credentials and reset questions in case you need to reset your password at a later date. The activation e-mail looks like this:

From: <donotreply@sc.gov>
Date: November 28, 2017 at 16:00:27 EST
To: <>
Subject: Secure Web Mail: WELCOME

State of South Carolina Secure E-mail

Secure Web Mail: WELCOME

You have been assigned a Secure Web Mail account on secureemail.sc.gov.

This means that you can now securely read messages which have been deemed to be of a sensitive nature.

Activate your personal account

When you first activate your account, you will be asked to define your sign in credentials.

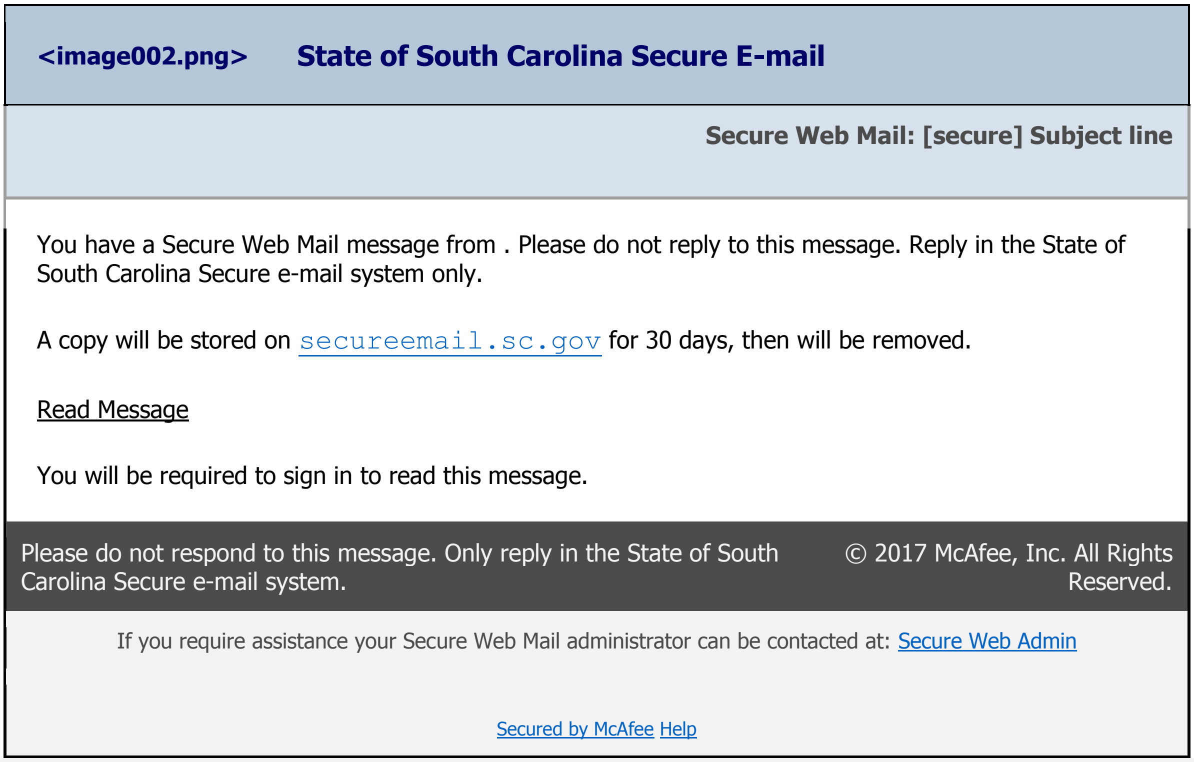
Please do not respond to this message. Only reply in the State of South Carolina Secure e-mail system.

If you require assistance your Secure Web Mail administrator can be contacted at: Secure Web Admin

Secured by McAfee Help

2. If you did not receive that e-mail, or do not recall your password, click the "Read Message" link in the e-mail you received. Then, click "Forgotten your password?" There will be questions for you to answer to reset your password. If that does not work, please reach out to the Secure Web Admin for help.

3. Once your account has been activated, you will receive a message similar to the sample, below, directing you to access the message on the secure e-mail site. Click Read Message to access the message contents. You will be able to Reply, Delete, or Print the message.



<image002.png> State of South Carolina Secure E-mail

Secure Web Mail: [secure] Subject line

You have a Secure Web Mail message from . Please do not reply to this message. Reply in the State of South Carolina Secure e-mail system only.

A copy will be stored on secureemail.sc.gov for 30 days, then will be removed.

Read Message

You will be required to sign in to read this message.

Please do not respond to this message. Only reply in the State of South Carolina Secure e-mail system.

© 2017 McAfee, Inc. All Rights Reserved.

If you require assistance your Secure Web Mail administrator can be contacted at: Secure Web Admin

Secured by McAfee Help