Handling of Printed Information

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 Sensitive information, then the document should be handled according to the Sensitive classification. Midwestern State University data users are urged to contact Information Technology for guidance in cases that present handling questions or security concerns. A handy reference for Personally Identifiable Information can be found here.

In all cases disposal of materials should follow the Midwestern State University records retention schedule.

Print Hardcopy of Information

This action covers printing documents from applications and databases. Once the data is reproduced in paper form, data users should follow the handling requirements for printed information.

Public: No special requirements
Sensitive: **Unattended printing** is allowed if access controls are in place to prevent unauthorized viewing of a printout.
Confidential: **Unattended printing** is allowed if access controls are in place to prevent unauthorized viewing of a printout. Printouts containing Confidential information should be picked up as soon as possible.

Storage of Printed Documents

Public: No special requirements
Sensitive: No special requirements
Confidential: Stored in a **secured location** when not in use.

Duplication and Distribution of Paper Documents

This action covers the duplication of printed documents only. Copies should only be made as specifically needed. Copies should not be distributed unless there is a business need to do so; and the recipient of a document should not further distribute it unless there is a business need to do so. It is also important for employees to understand how the distributed materials will be used and disposed of.

Public: No special requirements
Sensitive: No special requirements
Confidential: The receiver of the document containing Confidential information must not further distribute without permission of the data owner. Where necessary, the data owner should designate data which must not be further duplicated or distributed.

Mailing of Paper Documents via Campus Mail or External Carrier

This action includes mailing paper documents via Midwestern State University Campus Mail and via 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.

Public: No special requirements

Sensitive: 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.

Fax Paper Documents

This action covers sending and receiving faxed documents. When sending faxed documents, documents may either be sent directly from their electronic form, or more traditionally, by sending a paper document through a fax machine. This handling requirement applies to both types of fax transmission, but is primarily used to indicate sending faxes in the traditional, paper-based, manner. This handling requirement assumes a valid business need for sending or receiving a faxed document.

Public: No special requirements
Sensitive: Receiving faxes: **Unattended printing** is allowed if access controls are in place to prevent unauthorized viewing of a printout. Sending faxes: Prior to faxing, verify access controls or recipient presence at the time the fax is sent.
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. Sending faxes: Prior to faxing, verify access controls or recipient presence at the time the fax is sent.

When ***receiving*** faxed documents: Unattended faxing is allowed for Sensitive and Confidential data as long as controls are in place to prevent unauthorized viewing or pickup of the printouts. Follow the handling requirements for "**Print Hard Copy of Electronic Information.**"

When ***sending*** a fax containing Sensitive or Confidential data, the data users should contact the recipient to ensure that the fax machine receiving the data is secured using appropriate access controls, or that the recipient will promptly pick up the fax printout.

Labeling Paper Documents

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

Public: No special requirements
Sensitive: No special requirements
Confidential: Certain **documents** are to be labeled as "Confidential" regardless of internal or external use.

Disposal of Printed Documents

Public: No special requirements
Sensitive: Destroy the document
Confidential: Destroy the document

To destroy a document means to physically destroy it beyond any ability to recover the data on the document. Shredding a document is an appropriate destruction method.

Unattended Printing

Unattended printing is allowed for Sensitive and Confidential data as long as controls are in place to prevent unauthorized viewing or pick-up of the printouts. Printouts containing Confidential information should be picked up as soon as possible. “Access controls” for unattended printing or faxing include: utilization of a lock box for storage of unattended printouts and faxes; delayed output of printing and faxing until recipient initiates printout or fax.

For example, an acceptable practice is to send documents to a shared printer where a small group of people has access to the printer. A best practice would be to send documents to a shared printer with a separate bin where there is limited physical access to the printer (e.g., the printer is stored in a locked room).

Secured Location

"Secured location" includes placing data in locked office furniture, locked offices, and other locations specifically dedicated to secure storage of records and other information.

Sealed

“Sealed” means that an envelope is secured in such a way that tampering would be indicated upon receipt of the envelope, such as using tape across the envelope flap, sealing a self-adhesive envelope, placing a stamp or other sealing object across the envelope closure, etc. If you receive a Confidential document and it appears that the envelope has been tampered with, immediately notify the sender of the document.