MID-STATE TECHNICAL COLLEGE

ADMINISTRATIVE POLICY
Policy Section: ADMINISTRATION

Policy Title: DATA CLASSIFICATION, STORAGE, TRANSMISSION, RETENTION, ENCRYPTION, & MOBILE DEVICES

This policy covers all Mid-State data stored on Mid-State owned, Mid-State leased, and otherwise Mid-State provided systems and media, regardless of location as well as hardcopies of Mid-State data, such as printouts, faxes, notes, etc.

DATA CLASSIFICATION

Data residing on Mid-State systems should be continually evaluated and classified into the following categories:

- Personal: includes user's personal data, emails, documents, etc. This policy excludes personal information, so no further guidelines apply.
- Public: includes already-released marketing material, commonly known information, etc. There are no requirements for public information.
- Operational: includes data for basic business operations, communications with vendors, employees, etc. (non-confidential). The majority of data will fall into this category.
- Critical: any information deemed critical to business operations (often this data is operational or confidential as well). It is extremely important to identify critical data for security and backup purposes.
- Confidential: any information deemed proprietary to the business. Confidential data is typically the data that holds the most value to Mid-State. Often, confidential data is valuable to others as well, and thus can carry greater risk than general Mid-State data.

EXAMPLES OF CONFIDENTIAL DATA

The following list is not intended to be exhaustive, but provides guidelines on what type of information is typically considered confidential. Confidential data can include:

- Employee or customer social security numbers or personal information
- Medical and healthcare information
- Electronic Protected Health Information (EPHI)
- Customer data
- Network diagrams and security configurations
- Communications about legal matters
- Passwords
- Bank account information and routing numbers
- Payroll information

- Credit card information
- Vendor EIN
- Any confidential data held for a third party (be sure to adhere to any confidential data agreement covering such information)

DATA STORAGE

The following guidelines apply to storage of the different types of Mid-State data. Note: data needing to be backed up should be stored on Mid-State network drives. Data stored on local computer hard drives, OneDrive for Business, and Microsoft Teams is not backed up.

- Personal: there are no requirements for personal information.
- Public: there are no requirements for public information.
- Operational: operational data that needs to be backed up should be stored on a network drive (e.g., H, S, T, W drives). Data stored on local computer hard drives and data stored on OneDrive for Business is not backed up.
- Critical: critical data that needs to be backed up should be stored on a network drive (e.g., H, S, T, W drives). Data stored on local computer hard drives, OneDrive for Business, and Microsoft Teams is not backed up.
- Confidential: confidential information should be removed from desks, computer screens, and common areas unless it is currently in use. Confidential information should be stored under lock and key (or keycard/keypad), with the key, keycard, or code secured. Any confidential data needing to be backed up should be stored on a secured, authorized network drive (e.g., H, S, T, W drives). Data stored on local computer hard drives, OneDrive for Business, and Microsoft Teams is not backed up.

DATA TRANSMISSION

The following guidelines apply to transmission of the different types of Mid-State data.

- Personal: there are no requirements for personal information.
- Public: there are no requirements for public information.
- Operational: no specific requirements apply to transmission of Operational Data, however, as a general rule, the data should not be transmitted unless necessary for business purposes.
- Critical: there are no requirements on transmission of critical data, unless the data in question is also considered operational or confidential, in which case the applicable policy statements would apply.
- Confidential: confidential data should not be 1) transmitted outside Mid-State network without the use of strong encryption, 2) left on voicemail systems, either inside or outside Mid-State's network.

USE OF CONFIDENTIAL DATA

The following applies to how users should interact with confidential data:

- Users should be advised of any confidential data they have been granted access. Such data should be marked or otherwise designated "confidential."
- Users should only access confidential data to perform his/her job function.
- Users should not seek personal benefit, or assist others in seeking personal benefit, from the use of confidential information.
- Users should protect any confidential information to which they have been granted access and not reveal, release, share, email unencrypted, exhibit, display, distribute, or discuss the information unless necessary to do his or her job or the action is approved by his or her supervisor.
- Users should report any suspected misuse or unauthorized disclosure of confidential information immediately to his or her supervisor.
- If confidential information is shared with third parties, such as contractors or vendors, a confidential information or non-disclosure agreement should govern the third parties' use of confidential information.

SECURITY CONTROLS FOR CONFIDENTIAL DATA

Confidential data requires additional security controls in order to ensure its integrity. Mid-State recommends that the following guidelines are followed:

- Strong Encryption. Strong encryption should be used for confidential data transmitted external to Mid-State.
- Network Segmentation. Separating confidential data by network segmentation is strongly encouraged.
- Virtual Private Network (VPN). A VPN connection on a Mid-State only provided computer should be used by employees for connecting to Mid-State’s network or to PeopleSoft.
- Authentication. Strong passwords should be used for access to confidential data.
- Physical Security. Systems that contain confidential data should be reasonably secured.
- Printing. When printing confidential data the user should use best efforts to ensure that the information is not viewed by others. Printers that are used for confidential data should be located in secured areas.
- Faxing. When faxing confidential data, users should use cover sheets that inform the recipient that the information is confidential. Faxes should be set to print a confirmation page after a fax is sent; and the user should attach this page to the confidential data if it is to be stored. Fax machines that are regularly used for sending and/or receiving confidential data should be located in secured areas.

- Emailing. Confidential data should not be emailed outside Mid-State without the use of strong encryption.
- Mailing. If confidential information is sent outside Mid-State, the user should use a service that requires a signature for receipt of that information.
- Discussion. When confidential information is discussed it should be done in non-public places, and where the discussion cannot be overheard.
- Confidential data should be removed from documents unless its inclusion is absolutely necessary.
- Confidential data should never be stored on non-Mid-State provided machines (i.e., home computers).
- If confidential data is written on a whiteboard or other physical presentation tool, the data should be erased after the meeting is concluded.

DATA DESTRUCTION

The following guidelines apply to the destruction of the different types of Mid-State data.

- Personal: there are no requirements for personal information.
- Public: there are no requirements for public information.
- Operational: there are no requirements for the destruction of Operational Data, though shredding is encouraged.
- Critical: there are no requirements for the destruction of Critical Data, though shredding is encouraged.
- Confidential: confidential data should be destroyed in a manner that makes recovery of the information impossible. The following guidelines apply:
  - Paper documents: cross cut shredding is required.
  - Storage media (CD's, DVD's): physical destruction is required.
  - Computer Hard Drives/Systems/Mobile Storage Media/Printer Hard Drives/Fax Machine Hard Drives: at a minimum, data wiping should be used. Simply reformatting a drive does not make the data unrecoverable. If wiping is used, Mid-State should use the most secure commercially-available methods for data wiping. Alternatively, Mid-State has the option of physically destroying the storage media.

DATA RETENTION

The College strongly discourages the storage of a large number of messages on any system. Retention of messages consumes a large amount of space on the server(s) and can slow down system performance. In addition, because messages can contain the College’s confidential information, it is desirable to limit the number, distribution, and availability of such messages.

Electronic messages, whether sent or received, have the same legal status as hard copy documents and their retention is governed by the Wisconsin Records Retention Schedule. Accordingly, individuals are responsible for ensuring compliance with appropriate records retention requirements.

All relevant documents, including voicemail and email messages, must be preserved once a formal investigation or lawsuit has commenced.

Deletion By Users

As a general rule, if a message does not require a specific action or response, it should be deleted after it is read. If the content of the message needs to be saved according to the Wisconsin Records Retention Schedule, then the message should be placed in an email folder and saved for the necessary length of time. Employees should review their messages weekly and delete those that are not needed.

Deletion by System Administrator

The system administrator may enforce the following retention rules:

- The integrity and performance of the system(s) may require deletion of some messages.
- All messages may be deleted after 90 days if the user account is disabled.

DATA ENCRYPTION

The following information pertains to data encryption for Mid-State.

- Whole disk encryption – Mid-State provided laptops and mobile devices that connect to Mid-State's network should be encrypted. Mid-State owned desktop computers are not encrypted.
- Encryption of personal storage media/USB drives – Storing data on these types of devices is strongly discouraged. As such, there are no encryption requirements for personal storage media/USB drives.
- VPN tunnels – Mid-State utilizes a VPN tunnel for the transmission of data to and from the WILM data center, (e.g., PeopleSoft). Mid-State employees who have a need to access confidential information outside Mid-State should do so on a Mid-State provided device using a VPN connection into Mid-State's network.
- Email and email attachments – Mid-State strongly discourages sending confidential information via email or in email attachments; however, if the business need is present, then the use of strong encryption should be used for sending confidential data outside Mid-State.

DATA & MOBILE DEVICES

This section applies to Mid-State data as it relates to mobile devices that are capable of storing such data, including, but not limited to, laptops, notebooks, PDAs, smart phones, and USB drives. Since the policy covers the data itself, ownership of the mobile device is irrelevant. This policy covers any mobile device capable of coming into contact with Mid-State data.

Physical Security

By nature, a mobile device is more susceptible to loss or theft than a non-mobile system. Employees should carefully consider the physical security of their mobile devices and take appropriate protective measures, including the following:

- Laptop locks and cables can be used to secure laptops when in the office or other fixed locations.
- Mobile devices should be kept out of sight when not in use.
- Care should be given when using or transporting mobile devices in busy areas.
- As a general rule, mobile devices should not be stored in cars. If the situation leaves no other viable alternatives, the device should be stored in the trunk, with the interior trunk release locked; or in a lockable compartment such as a glove box.

Data Security
If a mobile device is lost or stolen, the data security controls that were implemented on the device are the last line of defense for protecting Mid-State data. The following sections specify Mid-State's requirements for data security as it relates to mobile devices.

- **Laptops** Whole disk encryption is required for Mid-State owned laptops that connect to Mid-State's network. Laptops should require a username and password or biometrics for login.
- **PDAs/Smart Phones** Use of encryption is not required on PDAs/smart phones but it is encouraged if data stored on the device is especially sensitive. Encryption of Mid-State provided smart phones is required.
- **Mobile Storage Media** This section covers any USB drive, flash drive, memory stick or other personal data storage media. Storage of Mid-State data on such devices is discouraged, but their use is permitted and encryption is not required.
- **Portable Media Players** No Mid-State data can be stored on personal media players.
- **Other Mobile Devices** Unless specifically addressed by this policy, storing Mid-State data on other mobile devices, or connecting such devices to Mid-State systems, is expressly prohibited. Questions or requests for clarification on what is and is not covered should be directed to the Vice President, Information Technology.

Connecting to Unsecured Networks
Users are permitted to connect Mid-State provided computers to public or unsecured networks, so long as accessing confidential data is not occurring. Examples of unsecured networks would typically, but not always, relate to Internet access, such as access provided from a home network, access provided by a hotel, an open or for-pay wireless hotspot, a convention network, or any other network not under direct control of Mid-State.

General Guidelines
The following guidelines apply to the use of mobile devices:

- Loss, theft, or other security incident related to a Mid-State provided mobile device should be reported promptly.
- Confidential data should not be stored on mobile devices.

- Data stored on mobile devices should be securely disposed of in accordance with the Data Destruction section of this policy.
- Users are not to store Mid-State data on non-Mid-State provided mobile equipment. This does not include simple contact information, such as phone numbers and email addresses, stored in an address book on a personal phone or PDA.

POLICY VIOLATIONS

Employees violating this policy are subject to revocation of electronic media privileges as well as discipline, up to and including termination to the extent permitted by state and federal law. Employees who break into unauthorized areas of the College's electronic media systems are also subject to civil liability and criminal prosecution.

Adopted:	*January 2016*
Last Reviewed:	*August 2020*
Last Revised:	*August 2020*