Policy Title: INFORMATION SECURITY PROGRAM

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.

SCOPE & OBJECTIVES

The objectives of this comprehensive written Information Security Program (ISP) include defining, documenting, and supporting the implementation and maintenance of the administrative, technical, and physical safeguards Mid-State Technical College has selected to protect the personal information it collects, receives, uses, and maintains. All employees, staff, contractors, vendors, officers, directors, and guests are required to comply with this ISP.

Mid-State Technical College will protect employee and student information by adopting and implementing, at a minimum, the security standards, policies, and procedures outlined in this ISP. This ISP outlines the minimum standards for the protection of personal information and has been developed in accordance with the requirements of all applicable state and federal laws and takes precedence over any legal obligation or other Mid-State Technical College policy or procedure.

The purpose of this ISP is to:

1. Ensure the security, confidentiality, integrity, and availability of personal information Mid-State Technical College collects, receives, uses, and maintains.
2. Protect against any anticipated threats or hazards to the security, confidentiality, integrity, or availability of such information.
3. Protect against unauthorized access to or use of Mid-State Technical College-maintained personal information that could result in substantial harm or inconvenience to any employee or student. Fulfill Mid-State Technical College’s obligation to comply with all state and federal regulations, policies, and standards associated with safeguarding employee and student information.
4. Define an information security program that is appropriate to Mid-State Technical College's size, scope, and business, its available resources, and the amount of personal information that Mid-State Technical College owns or maintains on behalf of others, while recognizing the need to protect both employee and student information.

This ISP applies to all employees, staff, contractors, vendors, officers, directors, and guests of Mid-State Technical College. It applies to any records that contain personal information in any format and on any media, whether in electronic or paper form.

For purposes of this ISP, "personal information" means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular employee or student. Personal information includes, but is not limited to, the following if it

identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular employee or student:

- Identifiers such as a real name, alias, postal address, online identifiers such as Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers.
- Employee and student records, including but not limited to, digital and electronic signatures, telephone numbers, insurance policy numbers, credit and debit card numbers, financial and credit-related information, physical characteristics and descriptions (e.g., government identification), bank account numbers, and medical and health insurance information (in the context of employment).
- Characteristics of protected classifications under state or federal law.
- Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.
- Biometric information.
- Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding employee or student's interaction with an Internet Web site, application, or advertisement.
- Geolocation data.
- Audio, electronic, visual, thermal, olfactory, or similar information.
- Professional or employment-related information.
- Education information, defined as information that is not publicly available personally identifiable information.
- Inferences drawn from any of the information identified in this subdivision to create a profile about an employee or student reflecting the employee or student's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.
- Persistent identifiers that can be used to recognize an employee or student, or a device that is linked to a consumer, over time and across different services, including, but not limited to, a device identifier; an Internet Protocol address; cookies, beacons, pixel tags, mobile ad identifiers, or similar technology; employee or student number, unique pseudonym, or user alias; telephone numbers, or other forms of persistent or probabilistic identifiers that can be used to identify a particular employee or student, or device.

"Personal information" does not include publicly available information, aggregate employee or student information, or employee or student information that is deidentified. For purposes of this paragraph, "publicly available" means information that is lawfully made available from federal, state, or local government records.

VICE PRESIDENT OF INFORMATION TECHNOLOGY

This ISP and the safeguards it contemplates are implemented and maintained by a single qualified employee designated by Mid-State Technical College. The Vice President of Information Technology (VP of IT) is responsible for the design, implementation, and maintenance of information safeguards and other

responsibilities as outlined in this ISP. The VP of IT may delegate or outsource the performance of any function under the ISP as they deem necessary from time to time. Mid-State Technical College has designated the following individual as the VP of IT: Bradley Russell, Vice President, Information Technology.

The VP of IT will be responsible for the following:

- Implementation and maintenance of this ISP, including, but not limited to:
    - Assessing internal and external risks to personal information and maintaining related documentation, including risk assessment reports and remediation steps.
    - Coordinating the development, distribution, and maintenance of information security policies and procedures.
    - Coordinating the design of reasonable and appropriate administrative, technical, and physical safeguards to protect personal information.
    - Ensuring that the safeguards are implemented and maintained to protect personal information throughout Mid-State Technical College, where applicable.
    - Overseeing service providers, processors, and third parties that access or maintain personal information on behalf of Mid-State Technical College.
    - Monitoring and testing the ISP's implementation and effectiveness on an ongoing basis through documented risk assessments and other mechanisms.
    - Defining and managing incident response procedures.
    - Establishing and managing enforcement policies and procedures for this ISP, in collaboration with Mid-State Technical College's legal counsel, Human Resources department, and upper management.
- Employee, staff, and contractor information security training, including:
    - Providing periodic security awareness and related training regarding this ISP, Mid-State Technical College's safeguards, and relevant information security policies and procedures for all employees, staff, and contractors.
    - Ensuring that those employees, staff, and contractors who have been enrolled in training courses have completed and passed the course in a timely manner.
    - Retaining training completion records.
- Reviewing this ISP at least annually, or whenever there is a material change in Mid-State Technical College's business practices that may reasonably implicate the security, confidentiality, integrity, or availability of records containing personal information.
- Periodically reporting to Mid-State Technical College management and Board of Directors (BOD) regarding the status of the information security program and Mid-State Technical College's safeguards to protect personal information.

IMPLEMENTATION CYCLE

Mid-State Technical College utilizes a methodology that establishes information security policies based on periodic and updated risk assessments. Once initial risks are identified and assessed, mitigation controls are documented by the VP of IT or their designees. Employees are then trained and made aware of their responsibilities for following the proper information safeguards outlined in this document. Mid-State Technical College will then be monitored and tested for its effectiveness at complying with the safeguards

by performing updated risk assessments, performed at least annually. The process continues as periodic audits and risk assessments are conducted to identify and evaluate residual risk.

RISK ASSESSMENTS

As a part of developing and implementing this ISP, Mid-State Technical College will conduct and document periodic risk assessments, at least annually, or whenever there is a material change in Mid-State Technical College's business practices that may implicate the security, confidentiality, integrity, or availability of records containing personal information.

The risk assessment will evaluate:

1. Reasonably foreseeable internal and external risks to the security, confidentiality, integrity, or availability of any electronic, paper, or other records containing personal information.
2. The likelihood and potential damage that could result from such risks, taking into consideration the sensitivity of the personal information.
3. The sufficiency of relevant policies, procedures, systems, and safeguards in place to control such risks, in areas that include, but may not be limited to:
    a. Employee, staff, and contractor training and management.
    b. Employee, staff, contractor, service provider, process, and third-party compliance with this ISP and related policies and procedures.
    c. Information systems, including network, computer, and software acquisition, design, implementation, operations, and maintenance, as well as data processing, storage, transmission, retention, and disposal.
    d. Mid-State Technical College's ability to prevent, detect, and respond to attacks, intrusions, and other security incidents or system failures.

Following each risk assessment, Mid-State Technical College will:

1. Design, implement, and maintain reasonable and appropriate safeguards to minimize identified risks.
2. Make available the results of the risk assessment to upper management for review.
3. Reasonably and appropriately mitigate any identified risks or violations of this ISP and document such mitigation in the risk assessment.
4. Regularly monitor the effectiveness of Mid-State Technical College's safeguards, as specified in this ISP.

SAFEGUARD PRINCIPALS

Mid-State Technical College will develop, implement, and maintain reasonable administrative, electronic, technical, and physical safeguards in accordance with applicable laws and standards to protect the security, confidentiality, integrity, and availability of personal information that Mid-State Technical College owns, accesses, or maintains on behalf of others. In doing so, Mid-State Technical College will adhere to the following principles:

1. Safeguards will be appropriate to Mid-State Technical College's size, scope, and business, its available resources, and the amount of personal information that Mid-State Technical College

owns or maintains on behalf of others, while recognizing the need to protect both employee and student personal information.

2. Mid-State Technical College will document its administrative, electronic, technical, and physical safeguards (see next section of this ISP).
3. Mid-State Technical College's administrative safeguards will include, at a minimum:
    a. Designating one or more employees to coordinate the information security program (see VP of IT section of this ISP).
    b. Identifying reasonably foreseeable internal and external risks and assessing whether existing safeguards adequately control the identified risks (see two previous sections of this ISP).
    c. Training employees in security program practices and procedures (with management oversight).
    d. Selecting service providers that are capable of maintaining appropriate safeguards and requiring service providers to maintain safeguards by contract (see service provider section of this ISP).
    e. Adjusting the information security program in light of business changes or new circumstances.
4. Mid-State Technical College's electronic and technical safeguards will include maintenance of a security system covering its network (including wireless capabilities) and computers that, at a minimum, and to the extent technically feasible, support:
    a. Secure user authentication protocols, including:
        i. Controlling user identification and authentication with a reasonably secure method of assigning and selecting passwords (ensuring that passwords are kept in a location or format that does not compromise security) or by using other technologies, such as biometrics or token devices.
        ii. Restricting access to active users and active user accounts only and preventing terminated employees or contractors from accessing systems or records.
        iii. Blocking a particular user identifier's access after multiple unsuccessful attempts to gain access or placing limitations on access for the particular system.
    b. Secure access control measures, including:
        i. Restricting access to records and files containing personal information to those with a need-to-know to perform their duties.
        ii. Assigning each individual with computer or network access unique identifiers and passwords (or other authentication means, but not vendor-supplied default passwords) that are reasonably designed to maintain security.
    c. Encryption of all personal information traveling wirelessly or across public networks.
    d. Encryption of all personal information stored on laptops or other portable or mobile devices, and to the extent technically feasible, personal information stored on any other device or media (data-at-rest).

e. Reasonable system monitoring for preventing, detecting, and responding to unauthorized use of or access to personal information or other attacks or system failures.
f. Reasonably current firewall protection and software patches for systems that contain (or may provide access to systems that contain) personal information.
g. Current system security software (or a version that can still be supported with reasonably current patches and malicious software ("malware") definitions) that (1) includes malware protection with reasonably current patches and malware definitions, and (2) is configured to receive updates on a regular basis.

5. Mid-State Technical College's physical safeguards will, at a minimum, provide for:
   a. Defining and implementing reasonable physical security measures to protect areas where personal information may be accessed, including reasonably restricting physical access and storing records containing personal information in locked facilities, areas, or containers.
   b. Preventing, detecting, and responding to intrusions or unauthorized access to personal information, including during or after data collection, transportation, or disposal.
   c. Secure disposal or destruction of personal information, whether in paper or electronic form, when it is no longer to be retained in accordance with applicable laws or accepted standards.

INFORMATION SECURITY POLICIES, PROCEDURES & SAFEGUARDS

The following policies, procedures, and safeguards reflect Mid-State Technical College's objectives for managing operations and controlling activities related to information security. Additionally, the policies and procedures within this document represent Mid-State Technical College's ongoing efforts in achieving and maintaining internal control over employee and student information security as well as compliance with state and federal requirements. This section of the ISP outlines minimum requirements and is not meant to be a comprehensive or all-inclusive list. The VP of IT will implement, test, monitor, and enforce all of the policies and procedures covered below:

General Organization Safeguards

- Documents with personal information will not be left unattended on the desk or workspace of any employee. At a minimum, employees will place any documents containing employee or student information in a drawer or enclosed container.
- Student personal information that is no longer part of the admission process should generally not be retained unless required by law or Mid-State Technical College policy, or unless it is securely stored, such as in a locked drawer or file cabinet.
- When away from their office, desk, or workspace, employees, staff, and contractors will either (1) lock their office doors, or (2) utilize lockable storage for any employee or student personal information. If keys and/or locks are not available, then the workspace will be cleared of all employee or student personal information, with no personal information left visibly unattended.

- Files and documents containing personal information that do not need to be retained by state, federal, or internal Mid-State Technical College rules will be securely destroyed and never placed into a regular trash or recycling bin. This includes mistakenly printed documents (including duplicates), as well as handwritten notes with employee or student personal information such as names, addresses, emails, and telephone numbers.
- Printers, fax machines, copiers, and other office equipment will be located in secure areas that are well monitored. At a minimum, documents should be immediately retrieved when faxed or printed from a remotely located machine. Under no circumstances should a document be left unattended at an unsecured machine location. Trash bins near copiers, printers, and other office equipment should be inspected for documents containing personal information.
- Personal information should never be placed in a manner that exposes employee or student information to unintended individuals. When with an employee or student, only that employee or student's personal information should be visible near the employee's desk or workspace.
- Admission interviews, as well as any other verbally communicated information involving the collection or disclosure of personal information, will be conducted in areas secure from eavesdropping. Employees will not use speakerphones in open areas susceptible to eavesdropping.
- All new employees should be trained in the basics of employee and student information security policies, procedures and safeguards outlined in this ISP. This should be conducted during, and incorporated into, the new employee onboarding process. Training will recur, at a minimum, annually for each employee.
- All employees will be granted access to employee or student information (both physical and electronic) on a need-to-know and least-access basis.
- Mid-State Technical College will conduct an inventory of all categories of personal information collected, map to which departments it is shared, the business purposes for which it is shared or disclosed, the categories of third parties and service providers to whom it is shared or disclosed, and the categories of sources from whom it is collected.

Physical & Administrative Safeguards

- Mid-State Technical College recognizes that best practices relating to information security are constantly evolving and therefore adopts many of the physical and administrative safeguards outlined in guidance and enforcement actions from the Federal Trade Commission. Accordingly, Mid-State Technical College will do each of the following:
    - Limit Access to Employee and Student Files to Individuals with a Need-to-Know
    - Protect File Storage Areas with Locking or Continuous Monitoring
    - Ensure Copiers and Office Equipment Are Kept Clear of Personal Information
    - Protect File Storage Areas from Destruction and Damage
    - Ensure Unattended Computers Are Not Left Unlocked
    - Ensure Proper Disposal of Employee and Student Information
    - Provide Mechanisms for Secure Disposal of Personal Information

- Ensure Unattended Workspaces Are Kept Clear of Personal Information & Security Credentials
- Keep Safety Standards in Place when Data is in-transit
- Require locking unattended offices and cabinets containing employee or student information

Electronic & Technical Safeguards

- Mid-State Technical College recognizes that best practices relating to information security are constantly evolving and therefore adopts many of the technical safeguards outlined in guidance and enforcement actions from the Federal Trade Commission. Accordingly, Mid-State Technical College will do each of the following:
    - Hold On to Information Only as Long as You Have a Legitimate Business Need
    - Use Only Fake or Test Data for Training and Testing Purposes
    - Restrict Electronic Access to Sensitive Data to Individuals with a Business Need
    - Limit Administrative Access to select Information Technology personnel
    - Require Complex and Unique Passwords
    - Ensure User Credentials Are Not Stored in Vulnerable Formats
    - Require MFA for All Systems Containing Non-public Personal Information
    - Disable User Accounts After Multiple Unsuccessful Login Attempts
    - Encrypt Data at Rest and in Transit
    - Use Firewalls to Segment Networks
    - Use or Enable Intrusion Detection and Monitoring Tools
    - Require Remote Network Access Be Done Through VPN and MFA
    - Place Limits on Third-Party Access to Networks and Applications
    - Update and Patch Third-Party Software
    - Encrypt Data Sent Over Point-of-Sale Devices
    - Restrict Downloading of Unauthorized Software
    - Encrypt Information Sent Over Wireless Networks
    - Ensure Digital Copiers Have Encryption or Overwriting Enabled
    - Add Auto-Wiping, Encryption, or Centralized Computing to Mobile Devices

Adoption of Safeguards

- Mid-State Technical College also adopts physical, administrative, and technical safeguards. Accordingly, Mid-State Technical College will do each of the following:
- Establish and Maintain Detailed Enterprise Asset Inventory
- Address Unauthorized Assets
- Establish and Maintain a Software Inventory
- Ensure Authorized Software is Currently Supported
- Address Unauthorized Software
- Establish and Maintain a Data Management Process

- Establish and Maintain a Data Inventory
- Configure Data Access Control Lists
- Enforce Data Retention
- Securely Dispose of Data
- Encrypt Data on End-User Devices
- Establish and Maintain a Secure Configuration Process
- Establish and Maintain a Secure Configuration Process for Network Infrastructure
- Configure Automatic Session Locking on Enterprise Assets
- Implement and Manage a Firewall on Servers
- Implement and Manage a Firewall on End-User Devices
- Securely Manage Enterprise Assets and Software
- Manage Default Accounts on Enterprise Assets and Software
- Uninstall or Disable Unnecessary Services on Enterprise Assets and Software
- Establish and Maintain an Inventory of Accounts
- Use Unique Passwords
- Disable Dormant Accounts
- Restrict Administrator Privileges to Dedicated Administrator Accounts
- Establish an Access Granting Process
- Establish an Access Revoking Process
- Require MFA for Externally Exposed Applications
- Require MFA for Remote Network Access
- Require MFA for Administrative Access
- Establish and Maintain a Vulnerability Management Process
- Establish and Maintain a Remediation Process
- Perform Automated Operating System Patch Management
- Perform Automated Application Patch Management
- Establish and Maintain an Audit Log Management Process
- Collect Audit Logs
- Ensure Adequate Audit Log Storage
- Ensure Use of Only Fully Supported Browsers and Email Clients
- Use DNS Filtering Services
- Deploy and Maintain Anti-Malware Software
- Configure Automatic Anti-Malware Signature Updates
- Disable Autorun and Autoplay for Removable Media
- Establish and Maintain a Data Recovery Process
- Perform Automated Backups
- Protect Recovery Data
- Establish and Maintain an Isolated Instance of Recovery Data
- Ensure Network Infrastructure is Up to Date
- Establish and Maintain a Security Awareness Training Program

- Train Employees to Recognize Social Engineering Attacks
- Train Employees on Authentication Best Practices
- Train Employees Data Handling Best Practices
- Train Employees on Causes of Unintentional Data Exposure
- Train Employees on Recognizing and Reporting Security Incidents
- Train Employees on How to Identify and Report if Their Enterprise Assets are Missing Security Updates
- Train Employees on the Dangers of Connecting to and Transmitting Enterprise Data Over Insecure Networks
- Establish and Maintain an Inventory of Service Providers
- Designate Personnel to Manage Incident Handling
- Establish and Maintain Contact Information for Reporting Security Incidents

Record Request & Information Disclosure Policies

- Only authorized employees will disclose, share, send, or provide employee or student personal information to third parties.
- In general, employee and student records containing personal information should not be mailed, emailed, texted, faxed, or otherwise transmitted electronically. Whenever possible, employees authorized to provide employee and student records containing personal information will require the employee or student to pick up the records in-person after being required to present a valid government-issued photo identification. If the person cannot reasonably be expected to visit the college physical locations, the person's identity must be verified using both of the following methods:
    - Requesting they fax a copy of a valid government-issued photo identification:
        1. In the event an employee or student prefers to email or text their license, employees have an obligation to inform the employee or student that Mid-State Technical College does not endorse, recommend, or request sensitive information be sent via email. Furthermore, employees are prohibited from accepting such information in the form of a text, whether on a company or personal phone. An employee or student who insists on sending information via email should be informed of the risks of sending information over an unencrypted network and that faxing or providing in-person are safer alternatives.
        2. Requesting the person's full name and at least two other identifiers such as date of birth, address, phone number, last four digits of Social Security Number, or email address.
- Mid-State Technical College personnel handling record requests have an obligation to securely destroy, and shred employee or student information obtained in the process of verifying an employee or student's identity (e.g. shredding a faxed government-issued photo ID).

- In no event may documents containing sensitive employee or student information (e.g., financial information, Social Security Number, credit information, and identification cards) be mailed or electronically transmitted without proper authorization and through approved and secure communication channels.
- To the extent possible and reasonable under the circumstances, sensitive information should be redacted from files prior to them being released to the employee or student.
- In general, employee and student records containing personal information should not be provided to unaffiliated third parties (e.g., vendors, manufacturers, and financial institutions) unless doing so is (1) required by law, (2) required to process a transaction initiated or requested by the employee or student, or (3) pursuant to a valid subpoena.
- Special rules under state and federal laws govern the disclosure of information related to victims or potential victims of identity theft. Employees should contact the VP of IT regarding requests related to identity theft.

SERVICE PROVIDER OVERSIGHT

Mid-State Technical College will oversee each of its service providers and processors that may have access to or otherwise create, collect, use, or maintain personal information on its behalf by:

1. Evaluating the service provider's or processor's ability to implement and maintain appropriate security measures, consistent with this ISP and all applicable laws and Mid-State Technical College's obligations. This may include having the service provider or processor complete a vendor risk assessment questionnaire.
2. Requiring the service provider or processor by contract to implement and maintain reasonable security measures, consistent with this ISP and all applicable laws and Mid-State Technical College's obligations. This may include having the service provider or processor complete and sign an applicable Data Processor Agreement.
3. Monitoring and auditing the service provider's or processor's performance to verify compliance with this ISP and all applicable laws and Mid-State Technical College's obligations.

IT CHANGE MANAGEMENT POLICY

Changes to Mid-State Technical College's IT infrastructure introduces a heightened risk of cybersecurity incidents. Accordingly, this section governs the addition, removal, or modification of the elements of Mid-State Technical College's IT infrastructure as follows:

- Adding and removing end-user devices. The VP of IT or designated IT personnel must be involved in adding end-user devices. Adding end-user devices, such as desktops, laptops, phones, or tablets requires that the devices be securely configured in accordance with the technical and electronic safeguards outlined in this policy. This includes, but is not limited to, automatic session locking after a defined period of inactivity, strong password requirements, and device lockouts after a specified number of failed authentication attempts. If possible, portable devices should

be set up to support remote wiping of all company data upon suspected theft, loss, or employee termination.

- Adding third-party software & applications. Prior to adding any third-party software or applications (whether hosted on premises or cloud-based), the vendor must be assessed for the adequacy of their technical and physical information safeguards. This includes, at a minimum, completing an electronic vendor risk assessment questionnaire for the service provider.
- Additions or modifications to web browsers. Cybercriminals can exploit web browsers in multiple ways. If they have access to exploits of vulnerable browsers, they can craft malicious webpages that can exploit those vulnerabilities when browsed with an insecure, or unpatched, browser. Alternatively, they can try to target any number of common web browser third-party plugins that may allow them to hook into the browser or even directly into the operating system or application. Accordingly, before allowing any browser to execute on the network, the following must be ensured:
    - Browser plugins are limited to trusted sources or otherwise disabled. Many plugins come from untrusted sources, and some are even written to be malicious. Therefore, it is best to prevent users from intentionally or unintentionally installing untrusted plugins that might contain malware or critical security vulnerabilities.
    - Automatic updates and patches for the browser and plugins have been properly configured.
    - Content filters for phishing and malware sites have been enabled.
    - Pop-up blockers have been enabled. Pop-ups can host embedded malware directly or lure users into clicking links using social engineering tricks.
- Major additions or modifications to servers, operating systems, or network elements. Any major modification, addition, or removal of servers, operating systems, or network elements (e.g., routers, switches, and firewalls) must be accompanied by the following:
    - A full internal penetration test.
    - A full internal and external vulnerability assessment.
- Conduct a technical risk assessment that is designed to assess the safeguards outlined in this ISP, as appropriate based on the changes made.

DATA RETENTION PLAN

The information of Mid-State Technical College is important to how it conducts business, protects employee and student data, and manages employees. Federal and state law require Mid-State Technical College to retain certain employee or student records, usually for a specific amount of time. Mid-State Technical College must retain certain records because they contain information that (1) serves as Mid-State Technical College's corporate memory, (2) have enduring business value, or (3) must be kept to satisfy legal, accounting, or regulatory requirements. The accidental or intentional destruction of these records during their specified retention periods could result in the following consequences for Mid-State Technical College and/or its employees:

- Fines and penalties imposed by state and federal agencies.

- Loss of rights.
- Obstruction of justice charges.
- Inference of spoliation of evidence and spoliation tort claims.
- Contempt of court charges.
- Serious disadvantages in litigation.

This policy is part of a company-wide system for the review, retention, and destruction of records that Mid-State Technical College creates or receives in connection with the business it conducts. Any type of information created, received, or transmitted in the transaction of Mid-State Technical College's business, regardless of physical format (collectively “record” or “records” hereinafter) are covered by this policy. Examples of where the various types of information are located include:

- Appointment books and calendars.
- Audio and video recordings.
- Computer programs and online applications.
- Contracts.
- Admission files.
- Electronic files.
- Emails.
- Handwritten notes.
- Hard drives.
- Invoices.
- Letters and other correspondence.
- Memory in cell phones and mobile devices.
- Online postings, such as on Facebook, Twitter, Instagram, Snapchat, Slack, Reddit, and other social media platforms and websites.
- Repair files.
- Voicemails.

Therefore, any paper records and electronic files, which are part of any of the categories listed in the Record Retention Schedule contained in this policy, must be retained for the amount of time indicated in the Record Retention Schedule. A record must not be retained beyond the period indicated in the Record Retention Schedule unless a valid business reason (or a litigation hold or other special situation) calls for its continued retention. If you are unsure whether to retain a certain record, contact the VP of IT.

Mid-State Technical College prohibits the inappropriate destruction of any records, files, documents, samples, and other forms of information. Disposable information consists of data that may be discarded or deleted at the discretion of the user once it has served its temporary useful purpose and/or data that may be safely destroyed because it is not a record as defined by this policy. Examples may include:

- Duplicates of originals that have not been annotated.
- Preliminary drafts of letters, memoranda, reports, worksheets, and informal notes that do not represent significant steps or decisions in the preparation of an official record.

- Books, periodicals, manuals, training binders, and other printed materials obtained from sources outside of Mid-State Technical College and retained primarily for reference purposes.
- Spam and junk mail.

How and When to Destroy Records

Mid-State Technical College's VP of IT is responsible for the continuing process of identifying the records that have met their required retention period and supervising their destruction. Regarding employee and student information, if no record retention period is specified, the secure disposal of employee or student information in any format must occur no later than two years after the last date the information is used in connection with the provision of a product or service to the employee or student to which it relates, unless such information is necessary for business operations or for other legitimate business purposes. The destruction of confidential, financial, employee, student, and personnel-related records must be conducted by shredding. The destruction of electronic records must be coordinated with the VP of IT. The destruction of records must stop immediately upon notification from legal counsel that a litigation hold is to begin because Mid-State Technical College may be involved in a lawsuit or an official investigation (see below). Destruction may begin again once legal counsel lifts the relevant litigation hold.

Litigation Holds and Other Special Situations

Mid-State Technical College requires all employees to comply fully with its published record retention schedule and procedures as provided in this policy. All employees should note the following general exception to any stated destruction schedule: If you believe, or legal counsel informs you, that Mid-State Technical College records are relevant to current litigation, potential litigation (that is, a dispute that could result in litigation), government investigation, audit, or other event, you must preserve and not delete, dispose, destroy, or change those records, including emails, until legal counsel determines those records are no longer needed. This exception is referred to as a litigation hold or legal hold and replaces any previously or subsequently established destruction schedule for those records. If you believe this exception may apply, or have any questions regarding whether it may apply, please contact the VP of IT. In addition, you may be asked to suspend any routine document disposal procedures in connection with certain other types of events, such as the merger of Mid-State Technical College with another organization or the replacement of Mid-State Technical College's information technology systems.

Periodic Review & Other Responsibilities

The VP of IT will periodically review this policy and its procedures with legal counsel and/or Mid-State Technical College's certified public accountant to ensure Mid-State Technical College is minimizing the unnecessary retention of data to the extent possible and is in full compliance with relevant new or amended regulations. The VP of IT (or a more qualified individual as determined by the VP of IT) is responsible for identifying the documents that Mid-State Technical College must or should retain, and determining, in collaboration with legal counsel, the proper period of retention. The VP of IT also arranges for the proper storage and retrieval of records, coordinating with outside vendors where appropriate. Additionally, the VP of IT is responsible for the destruction of records whose retention period has expired.

Records Retention Schedules

Mid-State Technical College follows the State of Wisconsin's Public Records Board Statewide General Records Schedules located here: Public Records Board Statewide General Records Schedules. This establishes retention or destruction schedules or procedures for specific categories of records. This is done to ensure legal compliance and accomplish other objectives, such as protecting intellectual property and controlling costs. Employees should give special consideration to the categories of documents listed in the records retention schedules per the URL above. Avoid retaining a record if there is no business reason for doing so and consult with the VP of IT or legal counsel if unsure.

ENFORCEMENT

Violations of this ISP may result in disciplinary action, up to and including termination, in accordance with Mid-State Technical College's human resources policies.

PROGRAM REVIEW

Mid-State Technical College will review this ISP and the security measures defined herein at least annually, or whenever there is a material change in Mid-State Technical College's business practices that may reasonably implicate the security, confidentiality, integrity, or availability of records containing personal information. Mid-State Technical College will retain documentation regarding any such program review, including risk assessment, mitigation steps, disciplinary actions, and remedial actions.

Adopted: *January 2024*
Last Reviewed: *May 2024*
Last Revised: *January 2024*