Zane State College

Information Security Policy & Plan

Last Modified: 12/2022

Table of Contents

Purpose

Zane State College an open access technical college located in Zanesville, Ohio is responsible for the collection and care of information related to students, faculty, staff, and internal business operations, as well as manages and maintains technical infrastructure required to house and maintain this information. Additionally, ZSC has contracts with Ohio Academic Resource Network (OARnet), and vendors of cloud and digital services and products to manage and maintain this information and infrastructure.

This policy will establish an information security program within the College. Zane State College's financial, student, and employee system or Enterprise Resource Planning (ERP) system is accessible through the campus network. This system is managed and cloud hosted by our vendor Jenzabar, Inc, however it is still vulnerable to security breaches that may compromise sensitive information resulting in data loss and other associated risks. Additionally, any sensitive information extracted from the ERP will also be included in any and all security procedures and included in this program. An information security program is necessary to ensure the following objectives are regularly reviewed and updated for best practice information security.

- Ensure the security and confidentiality of student, employee, and institutional information.
- Protect against threats or hazards to the security or integrity of student, employee, and institutional information.
- Protect against unauthorized access to or use of student, employee, and institutional information.
- Comply with federal and state statutes and regulations regarding the collection, maintenance, use, and security of information.
- Establish a college-wide approach to information security, including security awareness trainings, minimum education levels, and access to documentation.
- Establish and implement reasonable and effective practices for the protection and security of information.
- This policy establishes a program charged with ensuring Zane State College meets or exceeds all laws and ethical responsibilities for securing student, employee and institutional information.

Definitions

Accountability

Accountability refers to a system's capability to determine and track the actions and behaviors of a single individual within a system, and to identify that particular individual; accountability is also sometimes referred to as non-repudiation. Audit trails and system logs support accountability.

Active Directory

An electronic directory service developed by the Microsoft Corporation to centralize computer and user management.

Authentication

Authentication is the testing or reconciliation of evidence of users' identities. It establishes the user's identity and ensures that the user proves they are who they claim they are. The most common example of an authentication entity is a password. Single factor authentication (requiring a single challenge to validate identity) is commonly used for routine access control; multifactor authentication should be considered for sensitive or critical assets.

Authorization

Authorization is the granting of rights and permissions to an individual (or process) that enables access to an information resource. Once a user's identity and authentication are established, authorization levels determine the extent of system rights that a user can hold. Examples of authorization entities are access control lists and security groups.

Availability

Availability is the principle that means that information assets are available and usable by authorized users when and where they need them. Ensuring timely and reliable access to and use of information.

Confidentiality

Confidentiality is the principle that information and information systems are only available to authorized users, that they are only used for authorized purposes, and they are only accessed in an authorized manner. Confidentiality also determines information disclosure authority and conditions; unauthorized disclosure or use of confidential information is against college policy and could be illegal.

Enterprise Resource Planning (ERP)

Refers to a type of software the college uses to manage and operate daily business activities for the many departments. ERP systems tie together a multitude of business processes and enable the flow of data between

them. By collecting an organization's shared transactional data from multiple sources, ERP systems eliminate data duplication and provide data integrity with a single source.

Identification

Identification is the means by which a user claims their identity to a system—who is the user? The most common example is the UserID. This identification entity is commonly used for access control; identification is necessary for authentication and authorization.

Infrastructure

A set of information technology components that comprise the foundation of a technical service, typically a physical component, however can also be software or network components.

Integrity

Integrity is the principle that safeguards reliability, accuracy, and completeness of information assets. Integrity safeguards ensure modifications are not made by unauthorized users and that unauthorized modifications are not made by authorized users. Integrity controls also ensure information is current and has not been altered or damaged.

Network

A collection of hardware devices that enables two or more computers (or related equipment) to connect and communicate with each other.

Privacy

Privacy relates to the level of confidentiality and control granted to the user or individual subject of the information within a system. Privacy measures protect an individual's ability to determine what information is collected about them, who can access the information, how it may be used, and how it may be maintained. Loosely, privacy is to individual information (personal) what confidentiality is to corporate information.

Sensitive Information

Sensitive information includes data that requires protection because its loss, misuse, modification, or unauthorized access will negatively impact the welfare, privacy, assets, or security of an organization or individual.

Information Security Program Members

President's Staff Representative

Name: Joseph Keating, Executive Director of Operations	Email: jkeating@zanestate.edu
Work Phone: 740-588-1242	Mobile Phone: 740-418-7944

Program Officer

Name: Bryan Baker, Director of ITS Operations	Email: bbaker@zanestate.edu
Work Phone: 740-588-1204	Mobile Phone: 740-607-6000

Information Technology Services Department

Name: Ron Milner, Network Infrastructure Security Admin	Email: rmilner@zanestate.edu
Work Phone: 740-588-1356	Mobile Phone: 740-624-2147

Name: Shannon Vernon, Application Support Specialist	Email: svernon@zanestate.edu
Work Phone: 740-588-1265	Mobile Phone: 740-502-3056

Name: Christian Vicich, SQL/.NET Applications Developer	Email: cvicich@zanestate.edu
Work Phone: 740-588-4152	Mobile Phone: 740-630-8945

Additional Information Security Contacts

Communications

Name: Jennifer Folden, Director of Strategic Communications	Email: jfolden@zanestate.edu
Work Phone: 740-588-1225	Mobile Phone: 740-819-5035

Name: Keela Nelson, Digital Communications Specialist	Email: knelson1@zanestate.edu
Work Phone: 740-588-1318	Mobile Phone: 740-404-9838

Jenzabar (ERP) Consultant

Name: Joy Sourou, Senior Project Manage	Email: Joy.Sourou@jenzabar.com
Work Phone: 513-956-3315	

Network & Active Directory Security Consultants

Name: Will Bouharb, Sr. Executive CBTS	Email: will.bouharb@cbts.com
Work Phone: 614-440-9455	

Name: George Kohlhofer, Director RSM US LLP	Email: George.Kohlhofer@rsmus.com
Work Phone: 972-629-7914	

Ohio Academic Resource Network (OARnet)

Name: Toni Capocciama, Business Relations Manager	Email: toni@oar.net
Work Phone: 614-425-4524	

Policy Statement

Zane State College adheres to all applicable federal and state statutes and regulations to protect student, employee and institutional information. Best practices are observed to ensure industry standardized security measures are taken for all information systems.

As stated in our Computer and Lab Usage Policy, the college prohibits unauthorized access to, tampering with, acts of known or deliberate operations that cause damage or loss to information. Further, the college prohibits use of equipment or information to violate laws, commit breaches of confidentiality or privacy, compromise systems or networks, or otherwise sabotage college information or assets.

The college protects all student, employee and institutional information from threats and exploits guided by best practice security measures using reasonable and effective solutions. The level of security provided correlates with the type of information stored on the system. The college recognizes that it takes more than one office, policy, or procedure to create effective and strong security. As it is the responsibility of all college employees and other authorized users to share responsibility to minimize security risks and secure information within their control.

The college has established an information security program, led by the Director of IT Operations and guided by the Executive Director of Operations. Individuals within the program are encouraged to research and develop solutions, as well as make recommendations to policies, procedures, guidelines and other processes to support effective information security practices. This body stands different from the joint campus safety committee, as this program is solely focused on information security and Zane State College.

Campus-wide security awareness is critical to information security. Students and employees play a vital role in keeping the campus secure, and as such training and documentation will be provided regularly and easily found. The level of security training provided will depend on the level of access the person holds. All training will be documented to allow for state auditing, applicable laws, regulations and policy.

The college shall take appropriate action in response to misuse of information. Any violation of this policy may result in legal action and/or college disciplinary action under applicable college policies. This policy is available electronically on the web and upon request can be provided in paper format.

The Executive Director of Operations will review the Information Security Program quarterly with the Director of IT Operations. The Executive Director of Operations will provide updates at President’s Staff Meetings as needed.

Information Security Program

Information Security Program Overview

Zane State College recognizes that all information assets created, collected, used, and maintained by the college in the course of conducting our learning, research, and community/public service mission are subject to varying degrees of concern regarding security and privacy. Information assets include all data and all methods and devices used to create, store, and manage the data. All information assets and supporting infrastructure provided by the college are the property of Zane State College. Accordingly, the college reserves the right, and may be obligated by statutes, to manage and protect these assets.

To protect critical information and information systems, and to comply with applicable legislation, this policy serves as a charter and establishes a comprehensive Information Security Program. The primary function of the program is to establish a framework to assist in formalizing the implementation of the most current effective practices in the college information environment and institutional information security procedures. While these practices mostly affect the IT Department, some of them impact other areas of the college, and many third-party contractors.

Program Purpose and Objective

The purpose of the information security program is to ensure the confidentiality, integrity, and availability of student, employee and institutional information and the systems housing this information. The objective is to protect the college's information assets from threats and exploits, whether internal or external, deliberate or accidental.

The college maintains its information resources to fulfill its mission. The overall objectives of this program are to:

- Define, establish, and maintain an organizational structure for protecting information assets
- Implement a risk-based approach to protect information assets against threats, particularly to protect against loss of, unauthorized access to, or improper use of, information that could result in substantial harm or inconvenience to the college
- Provide the highest level of service while protecting information assets and integrating information security across all essential activities
- Identify issues that have resulted or may result in a breach of information assets, to respond to, mitigate damages resulting from, and prevent recurrence of information security issues
- Maintain all Federal, State, International, and industry-specific compliance obligations
- Develop and maintain processes used to ensure security of information

Program Sections

The program consists of four fundamental elements: Establishing information security organization, roles & responsibilities; Defining information security standards and principles; Specifying baseline security program safeguards and Continual evaluation and adjustment of the program.

Establishing Information Security Organization, Roles & Responsibilities

Operational responsibilities for the information security program to individual staff members will be assigned as deemed appropriate. The formally defined and delegated organizational roles and responsibilities include:

Deans, Directors, Chairs, Managers, and other Supervisors

Deans, Directors, Chairs, Managers, and other supervisors responsible for managing employees with access to information and information systems are responsible for specifying, implementing and enforcing the specific information security controls applicable to their respective areas. This includes ensuring all employees understand their individual responsibilities related to information security, particularly when accessing, processing, or transmitting sensitive or confidential information.

Supervisors are responsible for ensuring employees have the access required, and only the access required, to perform their jobs. Supervisors should periodically review their employees' access levels to ensure they are still appropriate, and take appropriate action to correct discrepancies/deficiencies. Supervisors must proactively notify Human Resources and the IT Department of any change in employment status that impacts access requirements. Supervisors are also responsible for reporting suspected misuse or other information security incidents to the IT Department.

Executive Director of Operations

Will provide oversight for the Information Security Program, the Program Officer responsible for the program and other security related regulations such as Gramm-Leach-Bliley. This person will review program related risk assessments, improvement strategies and completed objectives. The Executive Director of Operations will meet at least quarterly with the Program Officer and/or the program team to provide updates to the President's Cabinet.

Director of IT Operations

The Director of Information Technology Operations is designated as the Program Officer responsible for coordinating and overseeing the Information Security Program. The Program Officer must work closely with the various divisions and departments throughout the campus. The Program Officer also assists individuals who have the responsibility and authority for information owners with information security best practices relating to issues such as: establishing and disseminating enforceable rules regarding access to and acceptable use of information resources; conducting/coordinating information security risk assessment and analysis; establishing reasonable and effective security guidelines and measures to protect data and systems; assisting with monitoring and management of systems security vulnerabilities; conducting/coordinating information security audits; and assisting with investigations/resolution of problems and/or alleged violations of college policies. Questions/issues regarding the information security program or interpretation of this document should be initially directed to the IT Department.

Board of Trustees

It is the responsibility of this body to approve Zane State College policies into enactment. This Board having overall responsibility for the College, will receive periodical updates on the state of student, employee and institutional information, security assessments, and information security changes implemented as needed and at the direction of the President.

President's Cabinet

It is the responsibly of this body to review and perform final edits to all policy changes as a process toward enactment. This body represents all areas of the college and therefore is able to ensure all future policies are the best fit for the college as a whole. The Executive Director of Operations or the Director of IT Operations will provide at least annual updates on the state of student, employee and institutional information, security assessments, and information security changes implemented.

Team for Data Quality

The purpose of the Team for Data Quality (TDQ) is to:

- Develop a candid analysis of Zane State College's performance with respect to student outcomes and key initiatives.
- Examine quantitative and qualitative data and present findings in a clear and compelling way that shows where the College is doing well and where it needs to improve.
- Seek involvement of stakeholders to identify strengths and weaknesses of current policies, processes, structures, & services
- Aid College leadership in engaging stakeholders about the analysis of proposed goals and strategies
- Collaborate with Institutional Research, Information Technology, and other College departments to ensure that data needed for key initiatives can be appropriately collected and retrieved for analysis

Incident Response Team

The Cyber Security Incident Response Plan outlines the procedures the ZSC uses to detect and responds to unauthorized access or disclosure of sensitive information from systems utilized, housed, maintained or services by the ZSC. More specifically, this plan defines the roles and responsibilities of various institutional personnel with respect to the identification, isolation, and repair of data security breaches, outlines the timing, direction, and general content of communications among affected stakeholders and defines the different documents that will be required during various steps of the incident response.

In the event of a cyber security incident, Incident Response Team (IRT) staff have been trained to expeditiously address the incident. IRT personnel receive ongoing training to aid in recognizing anomalies in the campus systems that they regularly utilize and report any anomalies immediately the Incident Response Manager so the

IRT can be mobilized. Throughout the academic year, the Incident Response Manager, and members of the IRT are kept up to date on the latest security threats and educated how best to remediate incidents.

Information Technology Department

The IT Department is under the direction of the Executive Director of Operations, who is responsible for the college's information technology capabilities, including information security. The Executive Director of Operations is supported by the Director of Information Technology and the Information Technology staff.

The IT Department is primarily responsible for all technical information security controls. IT is primarily responsible for integration of technical information security tools, controls, and practices in the network environment, and is also often the end-users initial contact for reporting suspected information security failure or incidents. IT staff must follow information security best practices for managing infrastructure and services. IT is also primarily responsible for developing, practicing, integrating, and implementing security best practices for the college's applications such as the JenzabarOne system.

Employees with Access to Information

Employees (including Student employees) with access to information and information systems must abide by applicable college policies and procedures, as well as any additional practices or procedures established by their supervisors. Employees must use and safeguard information as governed by the regulations, duties and responsibilities of their position. This includes understanding the sensitivity of information used to perform their duties and securely accessing, processing, or transmitting sensitive or confidential information. Employee responsibility includes protection of their account password and any other protection the account has, as well as reporting suspected misuse or information security incidents to the IT Department.

Temporary Staff, Consultants and Service Providers

Temporary staff members are considered employees and have the same responsibilities as full or part-time employees with access to information and information systems.

Consultants, service providers, and other contracted third parties may be granted access to information on a 'need to know' basis. If a third party requires a network account, the IT Department must authorize the creation and access. The user is responsible for the security of his/her password(s) and accountable for any activity resulting from the use of his/her user ID(s) within reasonable scope of his/her control.

Third party network accounts will be active for a maximum of 90 days. If account access is no longer required before a year's time has elapsed, notify the IT Department to cancel the network account.

Third parties shall implement, maintain, and use appropriate administrative, technical, and physical security measures to preserve the confidentially, integrity, and availability of all electronically managed information. Upon termination of services, third parties will also return all information or certify destruction of information according to the agreement and/or specific terms of the contract.

Third party providers are also responsible for protection of account and password(s) and any other protection the account has, as well as reporting suspected misuse or information security incidents to the Zane State College IT Department. In the event of an information security incident caused by a third-party provider, the third party may be held liable for legal repercussions and expenses related to recovery/disclosure activities.

Students and Community Members

Students and community members are primarily responsible for the integrity of their own information and for reporting discrepancies to the appropriate office. All students and community members who are granted network accounts must comply with Zane State College's Acceptable Use of Information Technology Policy. This includes being responsible for all activity conducted via their college IT accounts within reasonable control, including protection of their passwords and any other protection the accounts have, as well as reporting suspected misuse or information security incidents.

Security Program Safeguards

Zane State College's Information Security Program includes safeguards designed to address the confidentiality, integrity, and availability of information assets. Where deemed necessary, the college has established operational policies and procedures to facilitate support of these controls. safeguards addressed by the security policy include, but are not limited to:

Access Control

Zane State College controls information asset access to authorized users, to processes acting on behalf of authorized users, or to authorized devices for systems that hold information.

Zane State College controls information asset access to transactions and functions that authorized users are permitted to execute in accordance with their role supporting the college.

Awareness and Training

Zane State College ensures that managers, systems administrators, and users of organizational information assets are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of organizational information assets.

Security Awareness Training is provided to all employees to ensure they are adequately trained to carry out their assigned information asset protection related duties and responsibilities.

Audit and Accountability

Zane State College creates, protects, and retains information system audit records to the extent needed to support monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information asset activity.

Zane State College takes reasonable effort to ensure the actions of individual information system users can be uniquely traced to those users, and administrative and technical policy is used to ensure they can be held accountable for their actions.

Configuration Management

Configuration documentation and inventories are established and maintained for information assets (including hardware, software and firmware) throughout the respective system development lifecycles.

Zane State College establishes and enforces security configuration settings for information technology products deployed in organizational information systems.

Identification and Authentication

All accounts must use complex passwords, including processes acting on behalf of users, or local device accounts.

Zane State College authenticates (or verifies) the identities of those users, processes, or devices as a prerequisite to allowing access to information assets. Multi-Factor Authentication is also required for all student, employee and privileged user accounts. This second factor could be phone call, text or Microsoft Authenticator App.

Incident Response

A cybersecurity incident plan has been developed and implemented for information assets that house or access Zane State College controlled information. The incident response capability includes a defined plan that addresses incident response:

- Detection
- Reporting & Analysis
- Containment
- Eradication
- Recovery
- Post-Incident Activity

Incidents will be tracked, documented, and reported to appropriate personnel and/or authorities both internal and external to the College's policies and compliance requirements.

Maintenance

Zane State College routinely maintains its information assets using effective industry-wide standards based on the nature of the information system or asset.

All tools, techniques, and mechanisms used to conduct information system maintenance are current or latest editions and practices. Controls are in place and enforced for all systems involving information.

Media Protection

All sensitive information is required to be protected by appropriate media protection mechanisms (i.e. encryption) to ensure the highest levels of security when stored anywhere except our cloud hosted ERP Jenzabar system.

Sensitive information is required to be protected to ensure the highest levels of confidentiality, integrity and availability in all media formats.

Zane State College policy restricts access to sensitive information on any media to authorized users.

Information system media containing sensitive information is required to be sanitized or destroyed before disposal or release for reuse.

Personnel Security

Almost all Zane State College employees require access to college information assets to support the college mission. The college has implemented multiple personnel security controls.

Prior to employment all candidates for employment undergo background checks in accordance with college policy. Contractual agreements with employees and contractors outline responsibilities of the individual/contractor to information security.

During employment management is responsible for ensuring all employees and contractors adhere to applicable information policies and procedures within the college. All employees must undergo awareness training based on their roles, as well as review of policies and procedures applicable to their jobs. There is a formal, communicated process to follow should employees or contractors fail to comply with security requirements.

Employee off-boarding processes ensure that appropriate access changes to information assets are addressed during and after personnel changes. Human Resources off-boarding process includes exit interviews and appropriate handling of college property in possession of exiting employees. Human Resources will advise the IT Department as to when access to sensitive information is removed from the exiting employees account and when that account is disabled or removed.

Physical Protection

As a public institution, Zane State College employs a layered and flexible approach to protection and monitoring of the physical facility and support infrastructure for information assets.

The college limits physical access to information systems, equipment, and the respective operating environments to authorized individuals based on role of the individual and classification. The IT Department has established access control and credentialing processes for sensitive locations to authorized individuals and that system maintains a list of personnel with authorized access to facility areas where sensitive information systems (such as server rooms, network closets) are physically located. Audit logs of physical access are be maintained and reviewed as appropriate.

The college requires an escort of visitors and monitoring of visitor activity in physically sensitive areas unless the area is under surveillance by our network camera system. Surveillance recordings are saved for 90 days.

The college has developed a Disaster Recovery and Business Continuity Plan to address protection against natural disasters or other malicious attacks, as well as accidental incidents. This plan involves triple redundancy including a primary, secondary and cold storage array. This solution is firewall protected and isolated from all networks. This solution is reviewed every six months for effectiveness and patched accordingly.

The Facilities department has implemented standards and processes addressing security measures for offices, conference rooms, classrooms, etc., including considerations for temperature, protection against water damage, and emergency lighting. Updated HVAC controls and filters have either been installed or is scheduled.

All college assets are required to be appropriately maintained and inventoried in accordance with the Business Office. Physical removal of assets requires appropriate authorization and follows established procedures.

Risk Management

Zane State College will periodically assess the risk to operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the college's information assets and the associated processing, storage, or transmission of information.

Risk assessments shall be performed upon initial acquisition of college-owned information asset and prior to establishment of service agreements with third parties. The risk assessment shall be reviewed and updated as appropriate, either at a specified time interval or when significant change is made to the information asset. Prior to engaging a third-party information services provider, a risk assessment must be conducted to ensure best practice information security. Where appropriate, third parties must provide documentation around their own risk management procedures, staffing requirements, recordkeeping, and security processes.

Routine vulnerability scans of information assets should be conducted prior to implementation and periodically detected vulnerabilities should be mitigated based on risk level and classification of the asset.

The IT Department will determine what needs to be monitored and measured to demonstrate effectiveness of security and overall risk management processes in accordance with all state and federal laws and guidelines (e.g. incident reporting, and decrease in overall incidents).

Security Assessment

The college periodically assess the security controls in information systems to determine if the controls are effective in their application.

Security and vulnerability assessments are routinely performed by the IT Department. Assessments are performed by a third-party provider at periodic intervals to ensure appropriate levels of coverage and oversight. The college will partner with OARnet and Tenable to provide this service. The college will develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in information systems.

Information system security assessments and controls with be monitored on an ongoing basis to ensure the continued effectiveness of the controls. The college will have real time portal access to all security assessments and set controls.

System and Communications Protection

Zane State College will monitor, control, and protect communications (i.e. information transmitted or received by JenzabarOne and other information holding systems) at the external boundaries and key internal boundaries of the information systems.

Information transfers to and from the JenzabarOne system will be carefully monitored and all access must be approved by the IT Department. Remote access to JenzabarOne is limited to a Microsoft Azure Remote Desktop virtualization solution in the cloud. Personal devices are not permitted to have JenzabarOne software installed or sensitive information downloaded to them.

JenzabarOne is a Jenzabar cloud hosted ERP solution that requires a secure point-to-point tunnel to reach. Access to these tunnels is restricted by Multi-Factor Authentication and Active Directory security groups. All users not deemed privileged employees are provided limited public access to JenzabarOne and in website form.

Network communications traffic will be denied by default and network communications traffic will be allowed by exception through use of hardware firewalls (i.e. deny all, permit by exception).

External parties must agree to securely transfer data and use strong encryption for certificates and passwords. Cryptographic mechanisms are implemented to prevent unauthorized disclosure of information during transmission unless otherwise protected by alternative physical safeguards. All encryption keys will be protected throughout their entire lifecycle. Encryption is used to protect the confidentiality of sensitive/non-public information in all systems that support cryptography.

System and Information Integrity

Zane State College will identify, report, and correct JenzabarOne information system flaws in a timely manner. Information system security alerts and advisories will be monitored and appropriate actions will be taken in response.

The JenzabarOne system is monitored and security provided by Jenzabar. Jenzabar will ensure the security and safety of hardware, attacks from the outside public and within from their own company network. Zane State College will protect user access by forcing Multi-Factor Authentication for all privileged user accounts, network segmentation and group-based account security.

Continual Evaluation and Adjustment

The Executive Director of Operations with support of the Director of Information Technology Operations will evaluate and adjust the Information Security Program in light of the results of risk identification and assessment activities undertaken pursuant to the Program, testing and monitoring, as well as any material changes to operations or business arrangements, and any other circumstances which may reasonably have an impact on the Information Security Program.

The Director of Information Technology Operations will prepare an annual report on the status of the Information Security Program and provide that to the Executive Director of Operations. The Director of Information Technology Operations may prepare more frequent reports as necessary or requested.