**Information Security Policy**

Central Community College safeguards the privacy of all visitors to our websites and applications. Central Community College describes our information security policy as it relates to the collection, protection, and disclosure of information resulting from the use of our computing systems, websites and apps; both information that is collected automatically and information that are provided voluntarily. Individuals who are authorized to access institutional data shall adhere to the appropriate roles and responsibilities, as defined in documentation approved and maintained by the information security team.

At a minimum the information security team will consist of the CISO, the Vice-President of Innovation and Instruction, and should include representatives who can provide institutional guidance on information security.

Central Community College complies with all applicable state and federal statutes, including, but not limited to, the Higher Education Opportunity Act (HEOA), Family Educational Rights and Privacy Act (FERPA), the Health Insurance Portability and Accountability Act (HIPAA), and the Nebraska Public Records Law. Central Community College will also comply with lawful subpoenas or court orders; the scope of these may include data gathered through websites and apps.

This Policy will be reviewed by the Board of Governors every 3 years or as deemed appropriate based on changes in technology or regulatory requirements.

Central Community College recognizes that from time-to-time exceptions to this policy must be granted. Exceptions made under this policy will only be made by the president of the college or the chief information security officer.

Central Community College appoints the vice-president of administrative services as the chief information security officer (CISO) with the following responsibilities.

1. Developing and implementing a College-wide information security program.
2. Documenting and disseminating information security policies and procedures.
3. Coordinating the development and implementation of a College-wide information security training and awareness program.
4. Coordinating a response to actual or suspected breaches in the confidentiality, integrity or availability of Institutional Data.