2171 – Information Services Security Procedures

Barton County Community College has adopted the following Information Security Procedures as a measure to protect the confidentiality, integrity and availability of Institutional Data as well as any Information Systems that store, process, or transmit Institutional Data.

Scope
These Procedures applies to all faculty, staff, and third-party Agents of the College as well as any other College affiliate, including student workers, who are authorized to access or manage Institutional Data.

Maintenance
These Procedures will be reviewed by the College's Information Security Team every 3 years or as deemed appropriate based on changes in technology or regulatory requirements.

Enforcement
Violations of these Procedures may result in suspension or loss of the violator's use privileges, with respect to Institutional Data and College owned Information Systems. Additional administrative sanctions may apply up to and including termination of employment or contractor status with the College, Civil, criminal and equitable remedies may apply.

Exceptions
Exceptions to these Procedures must be approved by the Information Security Team and formally documented. Procedure exceptions will be reviewed on a periodic basis for appropriateness.

Definitions

Agent, for the purpose of these procedures, is defined as any third-party that has been contracted by the College to provide a set of services and who stores, processes, or transmits Institutional Data as part of those services.

Information System, is defined as any electronic system that stores, processes, or transmits information.

Institutional Data is defined as any data that is owned or licensed by the College.

1. Throughout its lifecycle, all Institutional Data shall be protected in a manner that is considered reasonable and appropriate, as defined in documentation approved and maintained by the Information Security Team, given the level of sensitivity, value and criticality that the Institutional Data has to the College.

2. Any Information System that stores, processes, or transmits Institutional Data shall be secured in a manner that is considered reasonable and appropriate, as defined in documentation approved and maintained by the Information Security Team, given the level of sensitivity, value and criticality that the Institutional Data has to the College.

3. Individuals who are authorized to access Institutional Data shall adhere to the appropriate Information Security Roles and Responsibilities and Computing Standards, as defined in documentation approved and maintained by the Information Security Team.

Contact(s): Chief Information Officer

Related Form(s): Information Security Roles and Responsibilities; Computing Standards

References:

Relevant Policy or Procedure(s): 1170-College Record Retention

Approved by: President
Date:
Revision(s):