DENMARK TECHNICAL COLLEGE

ADMINISTRATIVE POLICY #03.30.07(2022) Information Security Policy

Policy Title: Information Security Policy

Policy Type: Administration

Policy Number: AC Policy #03.30.07 (2022)

Legal Authority: Section 59-53-51 of the 1976 Code of Laws of South Carolina, As Amended

State Board Policy: SBTCE Statement of Policy 4-4-105

Approval Date: September 5, 2022

Responsible Office: Department of Information Technology

Responsible Executive: Executive Vice President for Administration and Innovation/Chief Strategy Officer

Applies to: College Community

POLICY STATEMENT

This policy provides for the protection and enforcement of electronic data security in accordance with state policies and laws. It sets the minimum level of responsibility for employees, students, contractors, and third parties.

TABLE OF CONTENTS **PAGE NUMBER**

DEFINITIONS

There are no definitions associated with this policy.

CONTACT(S)

The Director of Information Technology officially interprets this policy. Additionally, the Director of Information Technology is responsible for obtaining approval for any revisions as required through the appropriate governance structures. Questions regarding this policy should be directed to the Department of Information Technology.

STAKEHOLDER(S)

College Community and service-area school districts, career centers, private institutions, and governing school associations.

POLICY CONTENT

Protection of Personal Information
Denmark Technical College protects the privacy of its employees, students, and alumni. All data with any personal information about an individual is processed and stored securely and confidentially.

The college uses the following data protection guidelines to protect each individual's personal information.

- Fair, lawful, and transparent processing
- Purpose limitation
- Data minimization
- Accuracy
- Data retention periods
- Data security
- Accountability

The College ensures both manual and digital records are secure. The level of security reflects the potential harm that could result from the loss or misuse of data. The College also has procedures in place to respond to any security breaches, including support from the South Carolina Technical College System (SCTCS).

The following security measures are used for data protection:

- Establishing password guidelines
- Installing enterprise firewalls and virtual private networks with multi-factor authentication
- Patching and staying current with system and application updates
- Deploying virus protection on all computers

- Encrypting any personal information held electronically
- Limiting electronic access – that is, only those who need to access the data off-campus are allowed

Information Security

In accordance with the South Carolina Department of Education's policies, the Information Technology Department of Denmark Technical College is responsible for initiating measures to assure and demonstrate compliance with the security requirements outlined in this policy.

- Implementing and maintaining an Information Security Program.
- Identifying a role (position/person/title) that is responsible for implementing and maintaining the college security program.
- Ensuring that security is part of the information planning and procurement process.
- Participating in annual information systems data security self-audits focusing on adherence to college policies, regulatory compliance, and risk mitigation strategies.
- Determining the feasibility of conducting regular external and internal vulnerability
- Assessments and penetration testing to verify that security controls are to identify weaknesses.
- Implementing a risk management process for the life cycle of each critical information system.
- Assuring the confidentiality, integrity, availability, and accountability of all college information while it is being processed, stored, and/or transmitted electronically.
- Assuming the lead role in resolving college data security and privacy incidents.
- Ensuring separation of duties and assigning appropriate system permissions and responsibilities for college system users.
- Identifying 'business owners' for any new system that is responsible for
    - classifying data,
    - approving access and permissions to the data,
    - ensuring methods are in place to prevent and monitor inappropriate access to
    - confidential data, and
    - determining when to retire or purge the data.

Denmark Technical College Employees, Contractors, and Third Parties

All Denmark Technical College employees, contractors, and third-party personnel are responsible for being aware of and complying with statewide and internal policies and their responsibilities for protecting versus using information resources only for intended purposes as defined by policies, laws, and regulations of the State or college, and being accountable for their actions relating to their use of all College information systems.

Data Disposal and Protection

- The Department of Information Technology sanitizes electronic and non-electronic media prior to disposal, release for reuse, and release outside of the Department of Information Technology based on applicable regulatory requirements.

- The Department of Information Technology employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.
- The Department of Information Technology implements controls to track media sanitization and disposal processes, wherever compliance requirements dictate, such actions must be followed, documented, and verified. Documentation must provide a record of the media sanitized, when, how media was sanitized, the person who performed the sanitization, and the final disposition of the media. The record of action taken must be maintained in a written or electronic format.
- The Department of Information Technology tests media sanitization equipment and procedures annually to ensure correct performance.
- The Department of Information Technology secures electronic media and devices and erases it prior to being reassigned or released for destruction.
- The Department of Information Technology defines and implements mechanisms for the disposal of digital media and data storage devices in equipment to be released outside the agency.
- The Department of Information Technology destroys hard copy media containing internal-use, confidential, or restricted information using approved methods prior to disposal.
- The Department of Information Technology employees follow the South Carolina Department of Education's acceptable use policies when transmitting data.
- The Department of Information Technology implements mechanisms to ensure the availability of information in the event of the loss of cryptographic keys by users.
- The Department of Information Technology implements mechanisms to ensure the confidentiality of private keys.
- The Department of Information Technology develops a mechanism to randomly select a key from the entire key space using hardware-based randomization.
- The Department of Information Technology implements appropriate controls to physically and logically safeguard the key-generating equipment from construction through receipt, installation, operation, and removal from service.
- For Restricted or data protected by federal or state laws or regulations: the Department of Information Technology uses Federal Information Processing Standards (FIPS)-140 validated (e.g., Advanced Encryption Standards (AES), Triple Data Encryption Algorithm (TDEA), Diffie-Hellman, RSA, Rivest Cipher 5 (RC5)) technology for encrypting confidential data.
- The Department of Information Technology ensures that sensitive data transmitted by email must be securely encrypted.
- The Department of Information Technology ensures that sensitive information transmitted through a public network must be encrypted prior to transmittal or be transmitted through an encrypted connection.
- The Department of Information Technology ensures that sensitive information transmitted wirelessly must be encrypted prior to transmittal or be transmitted through an encrypted connection.

TITLE: POLICY CONTENTS PUBLICATION

The policy will be widely distributed to the College community. To ensure timely publication and distribution thereof, the Director of Information Technology will make every effort to:

- Communicate the policy in writing, electronically, or otherwise to the College community, including current and prospective students within fourteen (14) days of approval.
- Submit this policy for inclusion in the Policy Library within fourteen (14) days of approval.
- Provide the policy to the Director of Public Information and Marketing to post on the College's webpage and all other related web pages, in the student handbook, and the College catalog, and
- Educate and train all stakeholders and appropriate audiences on the policy's content as necessary.

REVIEW SCHEDULE

- Next Scheduled Review: 9/5/2024
- Approval by, date: Executive Council, 09/5/2022
- Revision History: None
- Supersedes: None

RELATED DOCUMENTS

There are no related documents associated with this policy.

FORMS

There are no forms associated with this policy.