

Information Security Plan

1.0 Purpose

Drake State Community and Technical College Information Technologies department security practices must comply with federal and state laws and standards. DSCTC IT adheres to strict policies to facilitate compliance with these laws. These laws and policies are generally designed to protect individuals and organizations against the unauthorized disclosure of information that could compromise their identity or privacy.

Protected data as defined by these laws and DSCTC IT cover a variety of information types including personally identifiable information, (SSNs), personal financial information, health information and other data deemed confidential.

The Information Security Plan is intended to help guide employees to determine what information can be disclosed to non-employees, as well as the relative sensitivity of information that should not be disclosed outside of Drake State Community and Technical College without proper authorization.

This document will serve to summarize and provide approved policies aimed at ensuring that the access, use and protection of the DSCTC information systems promotes the college's objectives. These policies will facilitate the following principles:

- Ensure that Users abide by state and federal laws, as well as the policies of DSCTC and the Alabama Community College System;
- ensure that all individuals accessing or using the information systems assume responsibility for protecting these resources from unauthorized access, modification, destruction or disclosure;
- ensure the integrity, reliability, and availability of the information systems;
- ensure that individuals do not abuse DSCTC information systems.

The information covered in these guidelines includes, but is not limited to, information that is either stored or shared via any means. This includes: electronic information, information on paper, and information shared orally or visually (such as telephone and video conferencing).

Drake State personnel are encouraged to use common sense judgment in securing Drake State Community and Technical College information to the proper extent. If an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact their manager.

3.0 Policy

Among the laws and regulations that mandate baseline privacy and information security controls, the most notable for DSCTC include the following:

Health Insurance Portability and Accountability Act (HIPAA) - Protective Health Information (PHI) may be used and disclosed for Treatment, Payment, and Healthcare Operations (TPO). The information that is disclosed must meet the “Minimum Necessary” standard. This means the least information required to accomplish the intended purpose.

DSCTC IT does not store or support the collection of healthcare information, however HIPAA may be indirectly associated with the DSCTC Health Sciences program in clinical studies. Students must adhere to the HIPAA guidelines. Students and employees are not authorized to store patient information on a Drake provided/supported device.

Family Educational Rights and Privacy Act (FERPA) - Protects the privacy of student education records and gives parents certain rights with respect to their children’s education records.

In addition to the Drake State Community and Technical College Catalog and Handbook, the following yearly FERPA notification is supported by DSCTC IT and is provided for all students. Additional student privacy information, may be found on the Family Policy Compliance Office website by following this link: <http://familypolicy.ed.gov/>

- The school discloses education records without a student's prior written consent under the FERPA exception for disclosure to school officials with legitimate educational interests. A school official is a person employed by Drake State in an administrative, supervisory, academic, research, or support staff position (including law enforcement unit personnel and health staff); a person serving on the board of trustees; or a student serving on an official committee, such as a disciplinary or grievance committee. A school official also may include a volunteer or contractor outside of Drake State who performs an institutional service of function for which the school would otherwise use its own employees and who is under the direct control of the school with respect to the use and maintenance of PII from education records, such as an attorney, auditor, or collection agent or a student volunteering to assist another school official in performing his or her tasks. A school official has a legitimate educational interest if the official needs to review an education record in order to fulfill his or her professional responsibilities for Drake State Community and Technical College.
- The right to file a complaint with the U.S. Department of Education concerning alleged failures by the school to comply with the requirements of FERPA. The name and address of the Office that administers FERPA is:
 Family Policy Compliance Office
 U.S. Department of Education
 400 Maryland Avenue, SW
 Washington, DC 20202

Drake State Community and Technical College considers the following to be directory information and may be released to individuals and/or agencies, institutions, etc., unless the student files a Do Not Release form in the Office of Admissions and Records.

Directory Information

Name
 Address
 Telephone listing
 E-mail address
 Date and place of birth
 Major field of study
 Dates of attendance
 Enrollment status
 Class standing
 Degrees, honors, and awards received
 Most recent educational agency or institution attended

FERPA permits the disclosure of PII from students' education records, without consent of the student, if the disclosure meets certain conditions found in §99.31 of the FERPA regulations. Except for disclosures to school officials, disclosures related to some judicial orders or lawfully issued subpoenas, disclosures of directory information, and disclosures to the student, §99.32 of FERPA regulations requires the institution to record the disclosure. Eligible students have a right to inspect and review the record of disclosures. A postsecondary institution may disclose PII from the education records without obtaining prior written consent of the student –

- To other school officials, including teachers, within Drake State Community and Technical College whom the school has determined to have legitimate educational interests. This includes contractors, consultants, volunteers, or other parties to whom the school has outsourced

institutional services or functions, provided that the conditions listed in §99.31(a)(1)(i)(B)(1) - (a)(1)(i)(B)(2) are met. (§99.31(a)(1))

- To officials of another school where the student seeks or intends to enroll, or where the student is already enrolled if the disclosure is for purposes related to the student's enrollment or transfer, subject to the requirements of §99.34. (§99.31(a)(2))
- To authorized representatives of the U. S. Comptroller General, the U. S. Attorney General, the U.S. Secretary of Education, or State and local educational authorities, such as a State postsecondary authority that is responsible for supervising the university's State-supported education prog.7 (e)3.9 (w 4.012 0 Td(-)Tp0.6.n -0.003 Tw 0.30 Td0 Tc 1.012 0 Td(-6.5 (p)6 (r)0.75 (i)1.192)1.7 B)4.3

Drake State Community and Technical College supported information systems do not store credit card data. The college utilizes Touchnet to interface with the Banner ERP/SiS for payments. The data is scanned and transmitted real-time and no data is stored in any college information system.

