# 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).

All employees should familiarize themselves with guidelines that follow this introduction. Questions about the proper classification of a specific piece of information should be addressed to your supervisor.

## 2.0 Scope

This document and the associated policies apply to students, and all college employees, including, but not limited to, faculty, staff, consultants, or other third party representative. The policies also apply to all individuals, whether authorized or not, who use the college's Information Systems from any location. Use of DSCTC information systems, even when carried out on a privately-owned computer that is not managed or maintained by DSCTC IT, is governed by these policies.

Drake State is the provider of information resources; use of such resources constitutes consent for DSCTC IT to monitor, inspect, audit, collect and remove any information without permission or further notice. Students and personnel shall be versed in what use is acceptable and what is prohibited. The college regards any violation of this policy as a serious offense. Violators of this policy are subject to disciplinary actions, including legal implications.

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 HIPPA 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 Family Educational Rights and Privacy Act (FERPA) affords eligible students certain rights with respect to their education records. (An "eligible student" under FERPA is a student who is 18 years of age or older or who attends a postsecondary institution.) These rights include:

- The right to inspect and review the student's education records within 45 days after the day Drake State receives a request for access. A student should submit to the registrar, dean, head of the academic department, or other appropriate official, a written request that identifies the record(s) the student wishes to inspect. The school official will make arrangements for access and notify the student of the time and place where the records may be inspected. If the records are not maintained by the school official to whom the request was submitted, that official shall advise the student of the correct official to whom the request should be addressed.
- The right to request the amendment of the student's education records that the student believes is inaccurate, misleading, or otherwise in violation of the student's privacy rights under FERPA.
- A student who wishes to ask Drake State Community and Technical College to amend a record should write the school official responsible for the record, clearly identify the part of the record the student wants changed, and specify why it should be changed. If Drake State Community and Technical College decides not to amend the record as requested, the school will notify the student in writing of the decision and the student's right to a hearing regarding the request for amendment. Additional information regarding the hearing procedures will be provided to the student when notified of the right to a hearing.
- The right to provide written consent before the university discloses personally identifiable information (PII) from the student's education records, except to the extent that FERPA authorizes disclosure without consent.

- 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 programs. Disclosures under this provision may be made, subject to the requirements of §99.35, in connection with an audit or evaluation of Federal- or State-supported education programs, or for the enforcement of or compliance with Federal legal requirements that relate to those programs. These entities may make further disclosures of PII to outside entities that are designated by them as their authorized representatives to conduct any audit, evaluation, or enforcement or compliance activity on their behalf. (§§99.31(a)(3) and 99.35)
- In connection with financial aid for which the student has applied or which the student has received, if the information is necessary to determine eligibility for the aid, determine the amount of the aid, determine the conditions of the aid, or enforce the terms and conditions of the aid. (§99.31(a)(4))
- To organizations conducting studies for, or on behalf of, the school, in order to: (a) develop, validate, or administer predictive tests; (b) administer student aid programs; or (c) improve instruction. (§99.31(a)(6))
- To accrediting organizations to carry out their accrediting functions. ((§99.31(a)(7))
- To parents of an eligible student if the student is a dependent for IRS tax purposes. (§99.31(a)(8))
- To comply with a judicial order or lawfully issued subpoena. (§99.31(a)(9))
- To appropriate officials in connection with a health or safety emergency, subject to §99.36. (§99.31(a)(10))
- Information the school has designated as "directory information" under §99.37. (§99.31(a)(11))
- To a victim of an alleged perpetrator of a crime of violence or a non-forcible sex offense, subject to the requirements of §99.39. The disclosure may only include the final results of the disciplinary proceeding with respect to that alleged crime or offense, regardless of the finding. (§99.31(a)(13))
- To the general public, the final results of a disciplinary proceeding, subject to the requirements of §99.39, if the school determines the student is an alleged perpetrator of a crime of violence or non-forcible sex offense and the student has committed a violation of the school's rules or policies with respect to the allegation made against him or her. (§99.31(a)(14))
- To parents of a student regarding the student's violation of any Federal, State, or local law, or of any rule or policy of the school, governing the use or possession of alcohol or a controlled substance if the school determines the student committed a disciplinary violation and the student is under the age of 21. (§99.31(a)(15))

**Payment Card Industry (PCI) Data Security Standards –** A framework of standards and compliance-requirements designed to protect consumer payment card data.

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.

Additional laws and regulations apply in the wake of unauthorized disclosure of individuals' data, requiring DSCTC IT to take specific actions if any protected data may have been disclosed either accidentally or maliciously to unauthorized parties. Individuals who handle protected data are encouraged to speak with their managers to better familiarize themselves with relevant laws and regulations.

**Gramm-Leach-Bliley Act** - The GLB Act, or GLBA, is also known as the Financial Modernization Act of 1999. It is a United States federal law that requires financial institutions to explain how they share and protect their customers' private information. To be GLBA compliant, financial institutions must communicate to their customers how they share the customers' sensitive data, inform customers of their right to opt-out if they prefer that their personal data not be shared with third parties, and apply specific protections to customers' private data in accordance with a written information security plan created by the institution.

The primary data protection implications of the GLBA are outlined in its Safeguards Rule, with additional privacy and security requirements issued by the FTC's Privacy of Consumer Financial Information Rule (Privacy Rule), created under the GLBA to drive implementation of GLBA requirements. The GLBA is enforced by the FTC, the federal banking agencies, and other federal regulatory authorities, as well as state insurance oversight agencies.

The following table lists the current system use policies and guidelines followed by Drake State Community and Technical College Information Technologies.

| POLICY | SUMMARY | WHO DOES IT APPLY TO? | ACTIONS NEEDED? |
|---|---|---|---|
| CHANCELLOR'S PROCEDURES FOR POLICY 223.01 Information Security (INFOSEC) | This policy establishes the formal ACCS information security policy, ensuring security and privacy requirements are integrated into the planning, budgeting, acquisition, and management of ACCS information, information resources, supporting infrastructures, personnel, equipment, and services | Anyone utilizing DSCTC provided technology resources and technology services. | Read the policy and follow the outlined standards and procedures. |
| Computer/Technology Usage Agreement or Acceptable Use Policy | To outline the acceptable use of and the agreement to comply with computer equipment and network technology at DSCTC | Anyone utilizing a device or technology service on the DSCTC network. | Read the policy, follow the outlined standards and procedures, and sign that you agree. All employees must sign the agreement upon initial employment. |
| Computer Network Policy | to establish conditions for use of, and requirements for appropriate security for Drake State computer and network resources | Anyone utilizing a device on the DSCTC network. | Read the policy and follow the outlined standards and procedures. |
| Email Policy and Procedures | to prevent tarnishing the public image of Drake State | Anyone utilizing a Drake State email resource. | Read the policy and follow the outlined standards and |

| | | | |
|---|---|---|---|
| | as well as promote security of the email system | | procedures. |
| Mobile Device Policy and Agreement | To set forth Drake's requirements regarding the responsibility and management of iPads and other mobile units purchased by the college for faculty and staff use. | Anyone utilizing mobile computers and communication devices owned or operated by Drake State including iPads, phones, or any other mobile device type. | Read the policy, follow the outlined standards and procedures, and sign that you agree. All employees must sign the agreement upon receiving a mobile device. |
| VPN Use Agreement | To allow the use of remote access to DSCTC application and network resources. | Anyone requesting remote access to a DSCTC application or network resource. | Read the policies referenced in the agreement and sign the agreement. DSCTC IT will install an approved VPN client on the DSCTC provided device. |
| Remote Access Policy | To define standards for connecting to the DSCTC network from any host. | Anyone requesting remote access to a DSCTC application or network resource. | Read the policy and follow the outlined standards and procedures. |
| Virtual Private Network Policy | To provide guidelines for Remote Access Network (VPN) connections to the DSCTC network. | Anyone requesting remote access to a DSCTC application or network resource. | Read the policy and follow the outlined standards and procedures. |
| Security Awareness Policy | To minimize the risk of cyber-attack by educating employees on the tactic and methods used to possibly comprise systems in use by DSCTC | All employees | Read the policy and participate in the monthly training topic. |

**4.0 Statement of Direction/Practicum**

Drake State Community and Technical College Information Technologies has taken and continues to take all reasonable measures to secure their IT infrastructure and data resident on that infrastructure. Although it is against Drake State policy to disclose specific manufacturer and model of in-place security solutions, Drake State does rely on Stateful Packet Inspection technology that can perform Network Address Translation for both ingress and egress. Likewise, Drake also relies on Inline Intrusion Detection and Prevention with Malware filtering and blacklist capabilities. Independent Security Audits supplement the IT security position of Drake by providing insight into other security risks. These audits provide prioritized security items, thereby giving Drake additional focus on areas of concern and solutions to those concerns.

All employees are required to take cybersecurity awareness training. These security awareness sessions are provided by NEOED. The cybersecurity course contains various topics related to information technologies and cybersecurity. The DSCTC IT Coordinator monitors the training and works with supervisors to ensure all employees' participation.

**4.1 Guiding Principles:**

Assignment of Responsibilities: The DSCTC IT Coordinator maintains a document that clearly identifies the individuals who provide security administration for each platform and application for the college

Consistency of Security Provisions: DSCTC IT will follow consistent access controls across platforms. Please see the following policies for specifics: CHANCELLOR'S PROCEDURES FOR POLICY 223.01 Information Security (INFOSEC), VPN Policy, and the Remote Access Policy.

Separation of Duties: Total separation of duties is not feasible for an institution and department of Drake's size and population. Limited specialized staff is an issue that will continue to be monitored and addressed by DSCTC IT. The separation of duties between application access, data and rules manipulation, and security setup will always be a primary objective of the college. DSCTC IT project managers and leads will include this practice when assigning duties to technical and administrative staff.

Audit ability: Standards are documented for specific types of access granted to each role, i.e. Admissions Staff, Registrar, Comptroller, etc.

All requests for logon ids, user ids, or access must be approved by the data owner or custodian, i.e. Student Data access must be approved by the Director of Admissions/Registrar. The same procedure is also followed for requesting: programming and setup changes, reports contain PII documentation, new data collection points, etc.

**4.2 Responsibilities**

**DSCTC IT** is responsible for:

1. Implementing campus-wide security policies to protect the college's data, computer, and network resources from intentional or inadvertent modification, disclosure or destruction.
2. Monitoring user adherence to these policies.
3. Authorizing security audits or security scans affecting computer and network resources.
4. Coordinating response to computer and network security incidents to include, but not be limited to, notification of incidents to campus security, internal auditors, and other college administrators as appropriate.
5. Require regular updates of all college computer and network resource software, especially those for which demonstrated security exposures are repaired.
6. Require strong encryption and secure authentication techniques throughout all college computer and network resources as stated in the CHANCELLOR'S PROCEDURES FOR POLICY 223.01 Information Security (INFOSEC).
7. Providing services (i.e., notifications, FAQs, patches, virus software updates, instruction, security alerts, etc.) to assist individuals to maintain security on their computer and network resources.
8. Developing additional security policies as needed as technology and infrastructure mature and change.

S**ystem users** are responsible for:

1. Understanding, agreeing to and complying with all security policies governing college computer and network resources and with all federal state and local laws, including laws applicable to the use of computer facilities, electronically encoded data and computer software.
2. Safeguarding passwords and/or other sensitive access control information related to their own accounts or network access. Such information must not be transmitted to, shared with, or divulged to others. Similarly, system users must recognize the sensitivity of all other passwords and computer or network access information in any form, and must not use, copy, transmit, share or divulge such information, nor convert the same from encrypted or enciphered form to unencrypted form or legible text. Any attempt to conduct such actions by a system user is a violation of this policy.
3. Taking reasonable precautions, including personal password maintenance and file protection measures, to prevent unauthorized use of their accounts, programs or data by others.

4. Ensuring accounts or computer and network access privileges are restricted to their own use only. System users must not share their accounts, nor grant accounts to others nor otherwise extend their own authorized computer and network access privileges to others.
5. Ensuring the secure configuration and operation of network services (e.g., World Wide Web, anonymous ftp, shared directories, files, and printers) they may establish on machines connected to college computer and network resources.
6. Conducting or attempting to conduct security experiments or security probes or scans involving or using college computer and network resources without the specific authorization of DSCTC IT is prohibited. The intentional or negligent deletion or alteration of information or data of others, intentional or negligent misuse of system resources, intentionally or negligently introducing or spreading computer viruses, and permitting misuse of system resources by others are prohibited.
7. Respecting the privacy of electronic communication. System users must not obtain nor attempt to obtain any electronic communication or information not intended for them. In particular, system users must not attempt to intercept or inspect information (e.g., packets) en route through college computer and network resources, nor use college computer and network resources to attempt to intercept or inspect information en route through networks elsewhere.
8. Respecting the physical hardware and network configuration of college-owned networks. System users must not extend the physical network on which their system resides (e.g., wiring, jacks, wireless connection) without proper authorization.
9. Abiding by all security measures implemented on college computer and network resources. System users must not attempt to defeat or subvert security measures. System users must not use any other network address (e.g., IP address) for a computer or network resource than has been properly assigned by an authorized system or network administrator.
10. Treating non-Drake computer and network resources in accordance with this policy. College computer and network resources must not be used to attempt to breach the security or security policy of other sites (either willfully or negligently). An action or attempted action affecting non-Drake computer and network resources that would violate this policy if performed on a Drake State Community and Technical College campus or utilizing computer and network resources is prohibited.

**5.0 Enforcement**

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment and legal action.