DRAKE STATE
COMMUNITY & TECHNICAL COLLEGE

Banner Access Security Policy

1.0 Purpose

The purpose of this policy is to establish conditions for use of, and requirements for security, confidentiality and appropriate use of all associated data which is processed, stored, maintained, or transmitted in conjunction with Drake State Community and Technical College's ERP/SIS Ellucian Banner. The policy also applies to all peripheral administrative systems that are related to the ERP/SIS including, but not limited to Blackboard or Canvas Learning Management Systems, TargetX or equivalent CRM solutions, Elevate, SPOL, etc.

2.0 Scope

The Banner Access Security Policy applies to all individuals who have access to campus computer systems and networks, including but not limited to all college employees and student workers, who may or may not have been granted access to sensitive data during the course of their employment with Drake State Community and Technical College. It applies not only to stored information, but also to the use of the various computer systems and programs used to generate or access data**,** the computers that run those programs including workstations to which the data has been downloaded, and the monitors and printed documents that display data.

Access will be limited to that necessary to perform assigned job functions. In addition to the information outlined here, the confidentiality, use and release of electronic data are further governed by established college policies and federal and state laws, including the following:

- Federal Education Rights and Privacy Act (FERPA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Gramm-Leach-Bliley Act (GLBA)
- Student Catalogs
- Employee Handbook
- Drake State Community and Technical College Information Technologies(DSCTC IT) Policies and Procedures

This policy addresses security and access associated with the Banner and all related peripheral administrative systems as defined within this document and does not supersede in any way the aforementioned policies and regulations.

Drake State Community and Technical College computer and network resources may be accessed or used only by individuals authorized by the college. Issuance of an account to a system user must be approved by an authorized college representative. Any question with regard to whether a specific use is authorized must be referred to DSCTC IT.

3.0 Policy

DSCTC IT grants user security roles for Ellucian Banner and peripheral administrative systems in cooperation with the Alabama Community College System IT department.

No user is granted access without written or emailed consent of the administrator or custodian of the data. Data Custodians are responsible for determining who should have access to data within their jurisdiction, and what those access privileges should be. Responsibilities for implementing security measures may be delegated, though accountability remains with the owner of the data. Additionally, Data Custodians oversee data management functions related to the capture, maintenance and dissemination of data for a particular operational area.

Access for instructional areas is granted upon notification from the Dean of the areas. Access is also granted for instructional areas upon request of the Vice President for Instruction. Deans may reserve the right for the division secretary to request access in their absence. Non-instructional functional areas access with be granted upon the request of the director or administrator of the area in question.

No Personal Identifiable Information(PII) data should be stored locally outside of the ERP/SiS. The ERP/SiS system is connectied and authenticated to via SSL/SSH connections only. If a users' role requires that they temporarily store any type of PII, special permissions must be requested by the Data Custodian of the area at the college in which the user resides and wishes to access. Upon approval, the user's DSCTC IT supported device will be encrypted by BitLocker.

Area of Responsibility	Data Custodian(s)
Student	Registrar, Director of Admissions & Records Director of Advising Director of Recruitment
Student Financial Aid	Director of Financial Aid
Finance	Vice President for Financial & Administrative Services Director of Purchasing and Accounts Payable
Human Resources	Director of Human Resources &Payroll

Student Accounts Receivables	Vice President for Financial & Administrative Services Director of Accounting
Instructional Areas (Credit-based)	Vice President for Instruction Deans Division Secretaries(per the Dean’s discretion)
Distance Learning	Director of Distance Learning
Non-Credit/Continuing Education	Director of Workforce Solutions
Institutional Research	Dean of Planning, Research and Grants

By law and college policy, certain data is confidential and may not be released without proper authorization. Users must adhere to any applicable federal and state laws as well as college policies and procedures concerning storage, retention, use, release, and destruction of data.

All ERP/SIS related data, whether maintained in the central database or captured by other data systems, including personal computers, remains the property of DSCTC and is covered by all DSCTC IT data policies. Access to and use of data should be approved only for DSCTC purposes.

All ERP/SIS related information must be treated as confidential. Public or “directory” information is subject to restriction on an individual basis. Any requests for disclosure of information, especially from outside the college, should be referred to the appropriate office.

3.1 Responsibilities

DSCTC IT is responsible for:

1. Administrating security access to the Ellucian Banner system in cooperation with ACCS IT.
2. Maintaining security classes and roles commiserate with the functional areas data and procedures in cooperation with ACCS IT.
3. Implementing campus-wide security policies to protect the college's computer and network resources from intentional or inadvertent modification, disclosure or destruction.
4. Monitoring user adherence to these policies.
5. Authorizing security audits or security scans affecting computer and network resources.
6. 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.
7. Require regular updates of all college computer and network resource software, especially those for which demonstrated security exposures are repaired.

8. Require strong encryption and secure authentication techniques throughout all college computer and network resources as stated in the Acceptable Encryption Policy as well as the Password Policy.
9. 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.
10. Developing additional security policies as needed as technology and infrastructure mature and change.

Administrators/Data Custodians are responsible for:

1. Requesting system access based on roles or area of function within the college via mail, email, or helpdesk ticket.
2. Ensuring individuals are adequately trained in the associated functional area in which they are requesting access.
3. Assuring that the level of access requested is consistent with each user's job responsibilities and sufficient for the user to effectively perform their duties.
4. Ensuring that if a users' role requires the temporay storage of any type of PII data, special permissions are be requested of DSCTC IT to encrypt the user's device.
5. Ensuring checks and balances are maintained within the functional area in regards to access given to the Banner system.
6. Notifying DSCTC IT immediately upon the separation of an employee with access/privileges to the ERP/SIS and peripheral administrative systems.

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. Ensuring that no Personal Identifiable Information(PII) data is stored locally outside of the ERP/SiS on their device. If a users' role requires that they temporarily store any type of PII data, special permissions must be requested by the Data Custodian of the area.
8. 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.
9. 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.
10. 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.
11. 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.

4.0 Enforcement

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