

**ADMINISTRATIVE REGULATIONS
TABLE OF CONTENTS**

8000 INFORMATION TECHNOLOGY

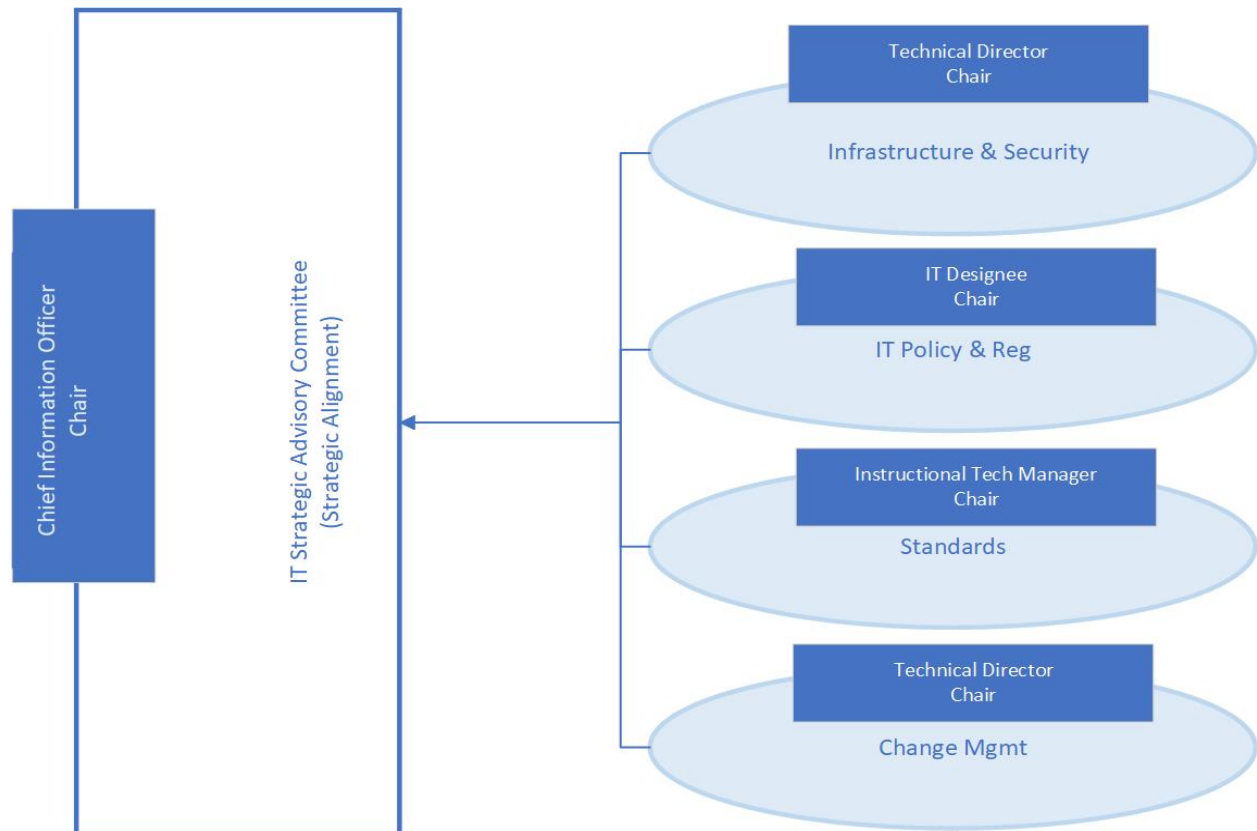
R 8100	Introduction and Governance
R 8200	Appropriate Use
R 8210	Access to Accounts and Information
R 8300	Access
R 8310	Authentication
R 8320	Identification
R 8330	Authorization
R 8400	Data Security
R 8500	Hardware and Software Support
R 8450	Gramm-Leach-Bliley Act
R 8700	Electronic Communication
R 8750	Mobile Communications
R 8910	Privacy Notification

Introduction and Governance

The Board of Trustees authorizes the use of information technology to support an effective and efficient environment for high-quality instruction and information and to Enhance communication, access, and the College's ability to meet the needs of students and other stakeholders.

The Information Technology Strategic Advisory Committee (ITSAC) provides institutional strategic alignment by establishing priorities and recommend policies and regulations, and is accountable and transparent to the college community. The ITSAC, including subcommittees, advises the Chief Information Officer. The Chief Information Officer submits recommendations to the President, the Executive Leadership Team, or College Council as appropriate.

IT Governance is comprised of the main governing body (ITSAC) and subcommittees. The actions of the subcommittees are recommendations to the ITSAC. This committee shall meet monthly to review all recommendations of the subcommittees. The structure is as follows:



1. Information Technology Strategic Advisory Committee
2. Infrastructure and Security
3. IT Policy and Regulations
4. Standards
5. Change Management

Additional adhoc task forces may be formed for special purposes.

The IT governance structure and responsibility:

1. Information Technology Strategic Advisory Committee (ITSAC)
 - a. Meeting frequency: monthly.
 - b. Chairperson: Chief Information Officer
 - c. Agenda: Developed by chairperson, distributed two days prior to scheduled meeting.
 - d. Document and review IT Service Catalog.
 - e. Overseeing the development and prioritization of a two-year technical roadmap.
 - f. Routinely measuring and monitoring the Return on Investment (ROI) of new and ongoing technology service or solution initiatives.
 - g. Review and approval of recommendations of subcommittees for alignment with IT tactical and strategic plans, as well as institutional strategic plan and initiatives.
 - h. Document and submit committee recommendations to the president, Executive Leadership Team (ELT), or College Council as appropriate.
2. Infrastructure and Security (ITSAC-I)
 - a. Meeting frequency: monthly or as needed.
 - b. Chairperson: IT Technical Director
 - c. Agenda: Developed by chairperson, distributed two days prior to scheduled meeting.
 - d. Develops, recommends and evaluates technologies for the development, support, management, and maintenance of the college IT infrastructure.
 - e. Creates task forces to investigate and to develop recommendations for college-wide IT infrastructure initiatives, when appropriate or necessary.
 - f. Identifies and assesses college cyber security, privacy and compliance needs and assist with their development and implementation.
3. IT Policy and Regulations (ITSAC-P)
 - a. Meeting frequency: quarterly, or as needed.
 - b. Chairperson: IT Designee
 - c. Agenda: Developed by chairperson, distributed two days prior to scheduled meeting.
 - d. Evaluates, authors, reviews, and recommends to ITSAC information security regulations that address risk and align with applicable federal and state regulations, as well as college policy, insurance and compliance requirements.

- e. Evaluates, authors, reviews, and recommends to ITSAC technology use regulations that address risk and align with applicable federal and state regulations, as well as college policy, insurance and compliance requirements.
 - f. Evaluates, authors, reviews, and recommends to ITSAC enterprise applications use regulations that address risk and align with applicable federal and state regulations, as well as college policy, insurance and compliance requirements.
 - g. Evaluates, authors, reviews, and recommends to ITSAC instructional and academic technology regulations that address risk and align with applicable federal and state regulations, as well as college policy, insurance and compliance requirements.
 - h. Create task forces to investigate and develop recommendations for policy and regulation on new or emerging technologies, when appropriate or necessary.
4. Standards (ITSAC-S)
- a. Meeting frequency: quarterly, or as needed.
 - b. Chairperson: Instructional Technology Manager
 - c. Agenda: Developed by chairperson, distributed two days prior to scheduled meeting.
 - d. Supports the development and maintenance of standards that enable a college-wide technology deployment that can be efficiently and strategically managed.
 - e. Establishes standards that formally guide the acquisition, maintenance and operations of information technology systems and infrastructure to make sure they are available, secure, cost effective and interoperable (as appropriate to business and academic requirements).
 - f. Create task forces to investigate and develop recommendations for college-wide IT hardware, software, and infrastructure initiatives, when appropriate or necessary.
5. Change Management (ITSAC-C)
- a. Meeting frequency: Monthly, or as needed.
 - b. Chairperson: IT Technical Director
 - c. Agenda: Developed by chairperson, distributed two days prior to scheduled meeting.
 - d. Ensures that standardized methods and procedures are used for technical changes.
 - e. Minimizes the impact of change-related incidents upon service quality, and consequently improves the day-to-day operations of the organization.
 - f.

IT Governance Values

The IT governance committees will use the RACI responsibility model.

- **R – Responsible:** Governance structure must focus on decision-making and results more so than implementation and project management.
- **A – Accountable:** Committees and task forces must be held accountable for delivering on their responsibilities. Clear escalation paths for issue resolution must be defined and outlined in charter documentation.

- C – Consulted: Governance committees work with and in all areas of the college with the purpose of understanding expectations.
- I – Informed: Communication must occur into, out of, and across the committees and with campus.

Additional values include:

- Transparency: Governance structure and process must be clear. How decisions are made and how users communicate with ITSAC must be readily apparent to campus.
- Appropriate Representation: Constituency groups across campus must be represented.

The ITSAC membership includes the following members:

- The Chief Information Officer, chair
 - Designee appointed by the Vice President for Finance and Administration
 - Faculty designee appointed by the Vice President for Educational Services
 - Technical dean or department chair designee appointed by the Vice President for Educational Services
 - Institutional Research Director or designee appointed by the Vice President for Educational Services
 - Professional staff designee appointed by the Dean for Student Services
 - Classified staff designee appointed by the Dean for Student Services
 - Designee appointed by the President
 - The ITS Technical Director, non-voting, ex-officio
 - The ITS Manager of Instructional Technology Services, non-voting, ex-officio
- Members will serve a two-year term, with half the members replaced each year.

(Revised 3/2019 – MH)

Appropriate Use

State Fair Community College (SFCC) shall provide technological resources to the campus community of students, faculty, staff, and the public to support its educational mission. SFCC technology can provide access to resources on and off campus, as well as the ability to communicate with other users worldwide. This access is a privilege and requires that individual users act responsibly. Users shall respect the rights of other users, respect the integrity of the systems and related physical resources, and observe all relevant laws, regulations, and contractual obligations. SFCC technological resources shall always be used in compliance with all international, federal, state, and local laws.

This regulation applies to all users of SFCC technological resources including faculty, staff, students, guests, external individuals or organizations and individuals accessing external network services, such as the internet via college facilities. Preserving the access to information resources is a community effort that requires each member to act responsibly and guard against abuses. Therefore, both the community as a whole and each individual user have an obligation to abide by the following standards of acceptable and ethical use:

- Use only those technological resources for which you have authorization.
- Use technological resources only for their intended purpose.
- Protect the access and integrity of technological resources.
- Abide by the applicable laws and college policies and respect copyrights and intellectual property rights of others, including the legal use of copyrighted software.
- Respect the privacy and personal rights of others.

Failure to comply with the appropriate use of these resources threatens the atmosphere for the sharing of information, the free exchange of ideas and the secure environment for creating and maintaining information property and subjects one to discipline. Any member of the college community found using technological resources for unethical and unacceptable practices has violated this policy and is subject to disciplinary proceedings including the suspension of system privileges, expulsion from school, termination of employment, and/or legal action as may be appropriate.

SFCC reserves the right to limit or restrict the use of its technological resources based on institutional priorities and financial consideration, as well as when it is presented with evidence of a violation of college policies, contractual agreements, or state and federal laws.

Although members of the community have an expectation of privacy, if a user is suspected of violating this policy, their right to privacy may be superseded by the college's requirements to protect the integrity of technological resources, the rights of all users and the property of the college. The college, thus, reserves the right to examine material stored on or transmitted through its facilities if there is cause to believe that the standards for acceptable and ethical use are being violated by a member of the college community. See Regulation 8210 Access to Accounts and Information.

User Responsibilities

Use of college technological resources is granted based on acceptance of the following specific responsibilities:

- Use only those technological resources for which you have authorization.
For example: it is a violation
 - to use technological resources you have not been specifically authorized to use.
 - to use someone else's account and password or share your account and password with someone else to access files, data or processes without authorization.
 - to purposely look for or exploit security flaws to gain system or data access.
- Use technological resources only for their intended purpose.
For example: it is a violation
 - to send forged electronic messages including but not limited to e-mail or instant messaging.
 - to hide their identity, or to interfere with other systems or users.
 - to use electronic resources for harassment or stalking other individuals.
 - to send bomb threats or "hoax messages."
 - to send SPAM or Phishing messages to intercept or monitor any network communications not intended for you.
 - to use technological resources for advertising or other commercial purposes.
 - to attempt to circumvent security mechanisms.
 - to use privileged access for other than official duties.
 - to use former privileges after graduation, transfer or termination.
- Protect the access and integrity of technological resources.
For example: it is a violation
 - to distribute a virus, ransomware, malicious script, malicious program or worm that damages, harms or compromises a system or network.
 - to prevent others from accessing an authorized service.
 - to attempt to deliberately degrade performance or deny service.
 - to corrupt or misuse information.
 - to alter or destroy information without authorization.
- Abide by applicable laws and college policies and respect the copyrights and protected intellectual property rights of others.
For example: it is a violation
 - to make more copies of licensed software than the license allows.
 - to download, use or distribute without permission copyrighted software.
 - to operate or participate in pyramid schemes.
 - to distribute pornography or to upload, download, distribute or possess pornography in public spaces.
 - to distribute, download or possess illegal content including but not limited to images, video, audio, files or software.
 - to not abide by all licensing agreements or terms of use applicable to technological resources.

- Respect the privacy and personal rights of others.
For example: it is a violation
 - to tap a phone line or run a network sniffer without authorization.
 - to access or attempt to access another individual's account or data without explicit authorization.
 - to intercept or possess another individual's authentication factor including but not limited to passwords and tokens.
 - to access or copy another user's electronic messages, data, programs, or other files without permission.
- Report suspicious or unlawful activity, system defects/bugs, or policy and regulation violations to Information Technology Services (ITS).
- Users are expected to cooperate with any investigation of policy or regulation abuse.
- Handle college data in accordance with Policy and Regulation 8400.

System Administrator Responsibilities

System administrators and providers of college computing and information technology resources have the additional responsibility of ensuring the integrity, confidentiality, and availability of the resources they are managing. Persons in these positions are granted significant trust to use their privileges appropriately for their intended purpose and only when required to maintain the system. Any private information seen in carrying out these duties must be treated in the strictest confidence, unless it relates to a violation or the security of the system.

Security Caveat

Be aware that although technological resource providers are charged with preserving the integrity and security of resources, security sometimes can be breached through actions beyond their control. Users are therefore urged to take appropriate precautions such as safeguarding their account and password, taking full advantage of file security mechanisms, backing up critical data using approved tools and promptly reporting any misuse or violations of the policy.

Violations

Every member of the college community has an obligation to report suspected violations of the above guidelines or of the Information Technology Policies - 8000. Reports should be directed to the unit, department, school, or administrative area responsible for the system involved.

If a suspected violation involves a student, a judicial referral may be made to the Dean of Student Services. Incidents reported to the Dean will be handled through the college's Student Code of Conduct.

If a suspected violation involves a staff or faculty member a referral will be made to the individual's supervisor and the Human Resources Department.

Access to Accounts and Information

State Fair Community College (SFCC) offers electronic services and the use of its electronic equipment and systems, including but not limited to servers, computers, mobile devices, telephone systems, and cloud-hosted storage (collectively, “technological resources”), to students, faculty and staff for educational, research and administrative purposes in furtherance of its mission.

SFCC has the legal right to access, preserve, and review all information stored on or transmitted through its technological resources. SFCC endeavors to afford reasonable privacy for Users (as defined in Policy and Regulation 8200) and does not access information created and/or stored by Users on its technological resources except when it determines that it has a legitimate operational need to do so. Examples of legitimate operational needs include, but are not limited to, the “reasons for access” articulated in Reasons for Access.

If SFCC determines, in its sole judgment, that it requires access to the account, device, or information of an individual user without prior notice to the user, SFCC may access the account, device, or information as provided in this Access to Accounts and Information Regulation 8210 and document the transaction for compliance purposes.

Who Is Affected by This Policy

This Regulation applies to all students, faculty and staff. It also applies to all other individuals and entities granted use of SFCC’s technological resources, including, but not limited to, contractors, temporary employees, volunteers, and the public (collectively, “Users”).

Reasons for Access

SFCC may access User accounts and information when, in SFCC’s sole judgment, doing so is reasonably necessary to achieve a legitimate operational need. Examples of such needs include, but are not limited to:

- evaluating or responding to health or safety risks
- ensuring continuity of operations during the unavailability of a user unexpectedly or for a prolonged period, or after the departure or death of a User
- when necessary to identify, diagnose or correct technological resources security vulnerabilities and problems, or otherwise preserve the integrity of technological resources
- investigating a possible violation of law or SFCC policy and regulations
- complying with federal, state, or local law or rules
- complying with validly issued subpoenas, governmental information requests, warrants, court orders, and discovery obligations in a pending or reasonably anticipated legal proceeding. In securing such access, SFCC officials will follow the request and approval procedures described in Procedures for Access.

Procedures for Access

The following procedure will be implemented when the college needs to access, preserve or review a User’s electronic account or information.

For business continuity needs

Whenever access to information or resources stored in an SFCC IT system is temporarily unavailable due to the absence of a User, and immediate access is necessary to accomplish an institutional objective or program, an administrative leader for the affected department (department chair, director, or equivalent) submits an Access Request and includes the following information:

- the name of the account holder whose existing information is to be exported, accessed or shared
- the reason why the access and data is needed
- the precise description of the information needed, including a date range

Information Technology Services (ITS) receives the request and confers with the requestor as needed and seeks approval as follows:

- for employees, an email is sent to the Executive Director of Human Resources or designee for review and approval.
- for students, an email is sent to the Dean of Student Services, FERPA Officer, or designee for review and approval.

ITS will use a ticket request for documentation purposes. ITS staff will promptly and confidentially access the account or information to provide the department leader a copy of the requested information. Depending on the circumstances and when necessary for business continuity needs, ITS may provide access to an account (for example, if the requester requires access to an Outlook calendar) and/or arrange for the temporary forwarding of emails to another email account.

For requests other than business continuity needs

Requests should flow to ITS (via email at networkservices@sfccmo.edu) through an authorized college official, as follows:

- for employees, an email is sent to the Executive Director of Human Resources or designee for review and approval, who then provides the official request to ITS.
- for students, an email is sent to the Dean of Student Services, FERPA Officer, or designee for review and approval, who then provides the official request to ITS.
- for legal issues, an email is sent to the President's Office or designee for review and approval, who then provides the official request to ITS.
- for safety or security requests, an email is sent to the President's Office or designee, who then provides the official request to ITS.

The Access to Accounts and Information Form should be used to provide the official request to ITS.

Before the requested information is provided, Human Resources must evaluate the request of the respective Dean or Vice President or their designee and concur that it is consistent with applicable laws and college policies. Once the Chief Information Officer (CIO) or designee has received the approved request and verified authorization from the appropriate authorized college official, the CIO or designee will work with the appropriate technical personnel to implement the request.

The CIO will follow instructions from the appropriate authorized college official regarding the preservation and archiving of requested data, and will document the request, disclosure details, the name and title of the requestor, and the reason for the request.

*No restricted or confidential information is ever to be documented in the ticketing system. Requests must be reviewed and, if necessary, modified to ensure confidentiality.

Requesting “Out of Office” Messages for an Unavailable Employee

When an employee is unexpectedly unavailable to receive and respond to email, and legitimate operational needs require continuity of communication, an administrative leader from the employee’s department (department chair, director, or equivalent) or Office of Human Resources Manager has the authority to request ITS to enable an "Out of Office" message from the employee's email account by submitting an “Out of Office” request to the Help Desk.

ITS receives the request and confers with the requestor as needed. ITS will use the ticket request for documentation purposes. ITS staff will confidentially access the email account for the sole purpose of creating and enabling the “Out of Office” message. The technical staff notifies the CIO and the original requestor, schedules the removal of the “Out of Office” message per the agreed upon date, and then closes the ticket.

Definitions

Phishing - The fraudulent practice of sending emails or other messages purporting to be from reputable companies or individuals in order to induce individuals to reveal personal information, such as passwords, bank accounts or credit card numbers.

Private space - Personal residence rooms in the Residence Halls.

Public space - All spaces not considered private space.

SPAM - Unsolicited usually commercial messages such as emails, text messages, or Internet postings.

Technological resources- SFCC offers electronic services and the use of its electronic equipment, systems and applications, including but not limited to servers, computers, mobile devices, wired and wireless networks, telephone systems, and cloud applications and services

(Approved 6/29/23)

Access

Computing and networking resources shall be provided for the educational, academic, and administrative purposes of the college. Some computer labs, networks, systems, and other resources shall be restricted to students who are enrolled in specific courses or programs or employees who have specific work assignments. Computer users shall learn and follow the access regulations for each resource used and shall use the resources appropriately and consistently with access regulations.

The use of these computers/networks/applications is a privilege granted to members of the college community. When using this account, you are agreeing to:

1. Take no actions which violate the Information Technology Appropriate Use Regulation 8200, Employee Handbook, or other applicable policy or law.
2. Use these resources only for purposes consistent with the college's mission and applicable policy or law. Inappropriate use includes, but is not limited to:
 - a. sending harassing messages or in any way harassing other computer users
 - b. gaining OR attempting to gain access to accounts or files without permission on any computer or network system
 - c. making unauthorized copies of any copyright protected software, or other copyrighted or trademarked material, regardless of source
 - d. taking actions which threaten the security or capacity of computer or network systems, or which destroy, damage or overload these resources
 - e. violating any applicable law or policy

Failure to abide by these policies will result in revocation of your privileges to use computing and network resources. Although we have backup procedures in place, use of these facilities is at your own risk since recoverability and security of data cannot be guaranteed. Files, data and disks may be considered SFCC property and are therefore subject to access by the college. Certain data may also be subject to access pursuant to Missouri Public Records statutes, via subpoena, or consistent with other state or federal law including but not limited to FERPA and GLBA.

(Revised 2/2023 – RR)

Authentication

Authentication is the process by which users or service accounts provide proof of who they claim to be. State Fair Community College (SFCC) shall maintain authentication services that securely identify users and service accounts to minimize the chance of improper authentication.

Authentication Level

Authentication levels used are dependent upon data and system classification within Regulation 8400. Authentication levels must be implemented whenever technically possible. All exceptions to the regulation must be documented as part of a risk assessment. Authentication levels must be considered during the procurement of new systems and upgrades of existing systems.

Strong Authentication

Strong authentication is the requirement to use multiple factors to verify the identity of a user accessing networks and/or applications, as opposed to the traditional method which requires only one factor of authentication (username and password solely).

Standard Authentication

Standard authentication is the requirement to use a single factor to verify the identity of a user accessing networks and/or applications typically requiring username and password solely.

No Authentication

No authentication does not have the requirement to use factors to verify identity of a user for accessing public information.

Authentication time out and Re-authentication

Authentication time-out and re-authentication are necessary to prevent unauthorized use through stealing open sessions both physically (leaving a computer unlocked) or virtually (session hijacking). Confidential and internal data must use strong authentication.

	No Authentication	Standard Authentication	Strong Authentication
Idle Time Out	None	75 Minutes	75 Minutes
Re-Authentication	None	12 Hours	2 Hours

Encryption

All authentications must be configured with encryption using industry standards and best practices.

Authenticators

When feasible authenticators must use the listed authentication methods against the SFCC Active Directory through Single-Sign-On (SSO).

Preferred authentication methods (in preferential order):

- Single-Sign-On (SSO)
 - SAML2.0
 - Shibboleth
 - Office 365/Azure
- RADIUS

Acceptable but less desirable:

- Lightweight Directory Authentication Protocol Secure (LDAPS)

MFA (Multi-Factor-Authentication)

Strong authentication counters the weaknesses inherent in traditional, one-factor authentication methods because they are:

- Harder to duplicate
- Cannot be re-generated
- Cannot be easily guessed
- Cannot be re-used
- Physically stored independently from the other factor of authentication, thereby deterring simultaneous use by an unauthorized user

Accepted MFA methods:

- Hardware OTP (one-time passphrase)
- Software OTP
- SMS (text messaging)
- Voice Call
- U2F AuthN
- Biometric

Lost or stolen MFA hardware including hardware tokens, cell phones and SIM chips must be reported immediately to Information Technology Services (ITS) for deactivation or revocation.

When using a cell phone for MFA a security lock screen should be set.

Password policy

Passwords are made up of various alpha numeric characters, which can be broken down into four-character groups. These are uppercase alphabetic, lowercase alphabetic, numeric, and special characters. Increasing the length and complexity of passwords increases the time necessary to crack passwords exponentially.

Passwords must:

- Contain:
 - English Uppercase Alphabetic (A - Z)
 - English Lowercase Alphabetic (a - z)
 - Numeric digits (0 – 9)
 - Special characters (e.g., exclamation point [!], dollar sign [\$], pound sign [#], percent sign [%], asterisk [*], etc.)
- Be longer than 12 characters

Good password ideas:

- Long unique phrases
- Multiple random words
- Random passwords generated by an approved password manager

Bad/prohibited passwords:

- Directory information such as your name, address, date of birth, username, nickname, or any term that could be easily guessed.
- Related to the job or personal life, e.g., not a license plate number, spouse's name, telephone number, etc.
- Commonly used passwords (e.g., p@ssw0rd, etc.).
- Proper names or places.
- Characters that are fixed combined with characters that predictably change. For example, users may not choose passwords like "boxtop01" and "boxtop02" or "x345JAN" and "x345FEB", etc., or identical or similar passwords the user previously chose.
- Keyboard paths or patterns such as "12345678" or "qwerty."

Password Lifetime Requirements

The purpose for requiring password lifetime restrictions is to prevent users from using their favorite password until it expires and changing their password more times than the system remembers, and cycling back to their favorite password, thus circumventing the system.

Password Expirations

- Accounts using standard authentication must reset their password on a regular basis according to industry best practices.
- Accounts protected with strong authentication are exempted from password expiration.

Password Length

All passwords shall be at least 12 characters in length, except within legacy systems that cannot support 12-character passwords.

Password Ownership Requirements

Passwords for all systems are subject to the following password ownership rules:

- Users shall not disclose their password to anyone. ITS employees will never ask for a user's password.
- If passwords must be sent electronically, the corresponding username must be sent over a different electronic communication to avoid interception.
- User-initiated password reset shall be supported by systems.
- Systems must be configured to log all password resets by users and administrators.
- Password reset requires identity verification.
- Only authorized individuals shall be granted rights to reset other users' account passwords.

Password Storage Requirements

- Systems are to store passwords using industry encryption best practices.
- Passwords must not to be stored in clear text.

Password Managers

A password manager is a program that encrypts and stores usernames and passwords for multiple applications and systems under a single username and password. Contact ITS for a list of approved password managers.

Login Failure Limits

Systems must be configured to limit the number of login failures resulting in account lockout. Login failure limits prevent “brute force” attacks.

(Added 2/2023 – RR)

Table of Contents

Identification

Securely and uniquely identifying individuals who make use of SFCC resources helps ensure that access to information and resources can be limited to those individuals who have a legitimate reason. All users will be assigned a unique identity to securely authenticate to SFCC information technology resources to which they have been authorized.

The SFCC unique identity is a Microsoft Active Directory username. Usernames are created by Banner and fed to Active Directory and other systems through automation. Alternative unique identifiers may be used by systems if they are linked backed to the Active Directory username.

System and/or application administrators may be issued additional unique identities for the separation of administrative job functions, roles and rights from their “standard” SFCC unique identity. The purpose of this is to limit security risk from compromised systems and accounts.

A system or service account is an account used by an application to interact with the operating system. System/service accounts may be used under these conditions:

- Documentation for the account must include usage, purpose, lifecycle and ITS owner
- Password changed regularly
- Monitored through auditing/logging
- Single use
- Annually reviewed
- Decommissioned at end of the lifecycle

(Added 2/2023 – RR)

Authorization

The SFCC unique identity shall be issued after the request is authorized appropriately and documented adequately. SFCC unique identities shall be deactivated, disabled and/or deleted as soon as reasonably possible after authorized notification of termination of contract, employment, or relationship with the college. Access to information in information technology system resources will be granted on a “need to know” or “minimum necessary” basis and must be authorized by the immediate information owner.

User Authorization should be based on “least privilege”

User authorization access control procedures should require:

- Documented procedures which facilitate the implementation of the access control policy and associated access controls
- Access to the information system based on:
 - A valid need-to-know that is determined by assigned duties
 - Intended system usage
 - Data owner approval
 - Manager's approval

Account Life Cycle

SFCC unique usernames are generated by Banner through an automated process triggered upon student admittance, completion of the employee hiring process, or registration as contractors or associated staff. Usernames are disabled/deleted pursuant to table 1.

Guest access usernames are created with information provided at the time of the registration and are disabled and deleted within the guidelines below. Guest access usernames are considered temporary identification and provide limited access to unclassified data or services pursuant to Policy and Regulation 8400.

Table 1: Account Disable/Deletion Conditions

Account Type	Creation	Disabled	Delete
Student	Condition: Admitted as a Student Processing period: 24 hours	Condition: Not enrolled in courses. Registered but dropped all classes Death Time period: 12 months	Condition: Disabled and not enrolled in courses. Time period: 6 months
Pre-student /Fin Aid Appl	Condition: Financial Aid Application Processing period: 1 hour	Condition: No completed school application Time period: 12 months	Condition: Disabled Time period: 6 months
Access Only Students	Condition: Apply as access only for specific courses Processing period: 24 hours	Condition: End of course Time period: 1 term	Condition: No reenrollment for a term Time period: 1 term
Employee	Condition: Completion of Hiring process Time period: 1 hour	Condition: Administrative or medical leave Time period: Immediate per leave Termination/retirement dates	Condition: Termination/retirement Time period: 6 Months
Affiliated Staff	Condition: Completion of HR paperwork Time period: 1 hour	Condition: Disassociation Time Period: Immediate per disassociation date	Condition: Disabled Time Period: 6 months
Service	Condition: Application/service setup Time period: 1 hour	Condition: Termination of application/service Time Period: Immediate	Time Period: Quarterly review of disabled service accounts
Guest	Condition: Completion of online request Time period: Immediate	Time Period: up to 48 hours	Time Period: 48 hours
Public	n/a	n/a	n/a

Definitions

Authenticator - The means used to confirm the identity of a user, processor, or device (e.g., user password or token).

Authentication - Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

Authentication Factor – A security credential such as a password, PIN or token that is used to prove the identity of a user. Factors may include something you know, something you have or something you are.

Authorization - The official management decision given by an organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations based on the implementation of an agreed-upon set of security controls.

Data Owner – See Regulation 8400.

Data Steward – See Regulation 8400.

Data Custodian – See Regulation 8400.

FERPA - Family Educational Rights and Privacy Act of 1974 otherwise known as the Buckley Amendment.

GLBA - Gramm-Leach-Bliley Act.

Identification – The method of uniquely identifying a user of a system or application.

Microsoft Active Directory – Microsoft’s centralized identity-based identity-services system. Active Directory uses multiple protocols to authenticate and manage user and computer accounts, services, and resources.

Multi-Factor Authentication (MFA) - Authentication using two or more distinct factors to achieve authentication. Factors include: (i) something you know (e.g., password/PIN); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric).

One Time passphrase (OTP) – May include various methods to electronically verify possession of a physical device or identity. Examples of which are cryptographically synchronized numbers (PINs) or tokens that are provided via SMS, voice or mobile applications.

Password Manager – Is an application that stores in an encrypted format multiple usernames and passwords. The user unlocks the repository of usernames and passwords using a single or MFA set of authentication credentials.

Standard Authentication – is the requirement to use a single factor to verify the identity of a user accessing networks and/or applications typically requiring username and password solely.

Strong Authentication - is the requirement to use multiple factors to verify the identity of a user accessing networks and/or applications, as opposed to standard authentication.

System or Service Account – An account used for single purposes such as running programs in a scheduled or automated manner.

U2F AuthN – Universal 2nd Factor Authentication standard.

(Added 2/2023 – RR)

Data Security and Retention

Data is necessary to conduct the business of State Fair Community College (SFCC). The life cycle of data includes collection, classification, responsibilities and access, storage and transmission, retention, and destruction of data. This regulation establishes the process, procedure and definition for each portion of the data lifecycle for the security and privacy of the constituents/community of the institution. All members of the SFCC community are responsible for protecting data in the lifecycle from unauthorized change, destruction, or disclosure. SFCC complies with all applicable laws and regulations regarding the dissemination and protection of data that is confidential including, but not limited to the Family Educational Rights and Privacy Act (FERPA) of 1974 and Gramm-Leach-Bliley Act (GLBA).

Violations of any part of this regulation may result in disciplinary action as prescribed by SFCC policies and regulations.

Prior to purchasing systems, resources, transmitting applications, or cloud services to be used for the purpose of storing or transmitting data, the tool must be vetted by ITS to verify it meets the technical requirements defined within Policy and Regulation 8400.

Data Lifecycle

Figure 1: Data Lifecycle

Collection

- All data ingested by the college must move through the data life cycle process.
- Data is evaluated and assigned to an appropriate existing business process. If no business process exists a new process must be created as defined in this regulation.
- Upon collection all appropriate care must be taken to securely receive and store the data if the data potentially will be classified as Internal Use or Confidential. Follow the appropriate Storage/Transmission requirements outlined in this regulation.

Classification

Maintaining and identifying the following information classifications for all college data:

Public

- Information or documents which are available to the public.
- For example, information hosted on the public website (www.sfccmo.edu), directory information (as defined per FERPA), press releases, policies and regulations, academic calendar, sports statistics, social media information...
- Collecting:
 - Security – no requirements
 - Assign Data Owner
- No security storage requirements

Internal Use Only

- Information or documents restricted for use within the college which relates to the institution's business. Computer generated reports listing students, employee and financial data are primarily for internal use only. Documents and data of this kind need not be kept under lock and key although reasonable care should be taken to keep it from public view. Precautions must be taken when these data are transferred to another individual or destroyed.
- This data may be available to the public per MO Sunshine Law.
- For example, but not limited to: work schedules, faculty roster, vendor information, business and operations information, electronic surveillance, salary information
- Any information that is reasonably not public
- Collecting:
 - Should be securely stored and transmitted
 - Assign Data Owner
 - Set retention policy
- Should be securely stored and transmitted during the entire life cycle

Confidential

- Personally Identifiable Information (PII) is data that would breach reasonable privacy expectations or data that could be detrimental to all members of the SFCC community if improperly disclosed. Regulated by law.
- These data are made available only to those individuals whose job responsibilities require such data. This kind of data, when printed on paper, must be kept under lock and key and carefully safeguarded. Precautions must be taken when these data are transferred to another individual or destroyed.

- Examples of PII, include but not limited to:
 - Student – FERPA, student data, criminal data, foster care, homelessness, applications and appeals
 - Financial PCI DSS – Credit Card data, bank account information, tax documentation and payroll
 - Health – Health data, HIPAA and ADA
 - HR (Human Resources) – criminal background checks and personnel records
- Collecting:
 - Must be securely stored and transmitted
 - Assign Data Owner
 - Set retention policy
- Must be securely stored and transmitted during the entire life cycle

Responsibilities and Access

- Staff who maintain data and handle computer-generated documents must:
 - Comply with all FERPA, HIPAA, GLBA, local, state, federal, and international laws
 - Use data and data access only as required in the performance of their jobs
 - Disclose Confidential and Internal Use Only data to other staff on a need-to-know basis
 - Exercise due care to protect data from unauthorized use, disclosure, alteration, and destruction
 - Utilize disk encryption software for all SFCC laptops, and for office PC and portable storage for Banner users (for example Bitlocker)
 - Follow established data processing practices, policies and regulations when using SFCC information systems including, but not limited to, the following:
 - Workstations are not to be left unattended after logging-in
 - Log off all public/lab workstations after use
 - Record passwords only in SFCC authorized password managers per Regulation 8310
 - Disclosing login account and password to anyone, including ITS personnel, is prohibited per Regulation 8310
 - Encrypt confidential and Internal use only data when transmitting data.
 - Will not use 3rd party unapproved systems
- Selling or transferring e-mail addresses, mailing labels, or other serial data to outside agencies or vendors is prohibited unless approved by the President's Office.
- Institutional Research (IR) is responsible for sending external reporting data to off-campus entities. Data reported externally should be validated with the Data Owner and/or IR prior to release.
- Public data is to be released/published in accordance with Marketing and Communications (MarComm) Policy and Regulation 9000.
- Institution-wide statistical data must be validated by IR including but not limited to:
 - Survey date definitions
 - Source for "official" federal, state, IPEDS (Integrated Postsecondary Education Data System), accreditation comes from each department, but IR coordinates gathering the data between multiple departments.
 - Read only access to data.
 - Extracts data – Data Analyzer – analysis/reporting

- Data custodianship defined by State, Federal, and international regulations and laws supersede roles defined within this regulation.

Roles

- **Data User** – Employees who have access to internal use only and confidential data in order to conduct college business and operations. Data Users encompass Data Executives, owners, stewards, analyzers, and custodians; Data Users also include faculty or staff who access internal use only and confidential data.

Typical responsibilities include:

- Understanding and complying with college policies and regulations for the access, use, disclosure, and protection of institutional data.
- Alerting Data Owners to data discrepancies, inaccuracies or data validation concerns.
- Alerting Data Owners and custodians immediately to any security incidents.
- **Data Executive** – Employees who are the highest-ranking individuals accountable for what happens with and to college data. Data Executives are usually administrative-level positions, including but not limited to, the president of the college or other designated employee(s).

Typical responsibilities include:

- Providing authority for setting policies and regulations related to data use and oversight.
- Addressing data-related issues that escalate to the highest level.
- Authorizing the release of confidential and internal use data, per applicable regulatory and legal requirements, to outside entities.
- The legal custodian of the information remains responsible for ensuring that data constituting a college record is handled appropriately.
- **Data Owner** – Employees who have planning and high-level responsibility for the management of data within their functional areas. Data Owners are usually vice presidents, deans or directors.

Typical responsibilities include:

- Authorizing access to Data Stewards.
- Ensuring the data collected are accurate, reliable and properly captured.
- Addressing data discrepancies, inaccuracies or other data validation concerns.
- Establishing processes for data collection and accountability.
- Ensuring compliance with regulatory or other legal requirements.
- Reviewing annual data access summaries and removing access from anyone who is no longer authorized.
- **Data Steward** – Employees who use data as part of their assigned duties within the college. Data Stewards are usually subject matter experts on specific sets of data within their functional areas.

Typical responsibilities include:

- Entering, maintaining and manipulating data.
- Ensuring the data collected are accurate, reliable and properly captured.
- Alerting Data Owners to data discrepancies, inaccuracies, or other data validation concerns.
- **Data Analyzer** – Employees who are granted access to data for analysis and reporting purposes. Data Analyzers are usually, but not limited to, employees within the IR department.

Typical responsibilities include:

- Practicing due diligence in ensuring data reported are accurate, reliable, and in compliance with regulatory or other legal requirements.
- Alerting Data Owners to data discrepancies, inaccuracies, other data validation concerns, and new reporting requirements.
- Working with Data Owners to meet “official” data definition requirements for the purpose of reporting/surveying.
- Assisting Data Owners in defining data collection processes as related to outcome reporting and analysis.
- **Data Custodian** – Employees who are responsible for the maintenance and operation of systems that serve as repositories of institutional data. Data Custodians are usually, but not limited to, employees of the Information Technology Services department.

Typical responsibilities include:

- Providing a secure infrastructure in support of data management including, but not limited to, backup and recovery processes and secure transmission of data.
- Granting access privileges to users as authorized by Data Owners.
- Controlling levels of access to ensure individuals have access only to information for which they have been authorized, and that access is removed when no longer needed.
- Installing, configuring, patching, and upgrading hardware and software used for data management.
- Alerting Data Owners to data discrepancies, inaccuracies, and data validation or security concerns.
- Building data systems to meet the classifications of data as well as Data Owner specifications.
- Advising Data Owners regarding the data collection process, including but not limited to, assessing existing and future data structures, organization, systems and storage constraints.
- Providing annual access summaries to Data Owners.
- Note: It is not the responsibility of Data Custodians to disseminate data to anyone on or off campus. Data dissemination is the responsibility of Data Executives, owners, stewards, and analyzers within the constraints of their respective roles.

Storage and Transmission

Data is in one of two states:

- **At-rest** - stored physically or saved electronically somewhere.
- **In-motion** - being transmitted or moved between multiple places or electronic storage.

At-rest: storage

- Store information in repositories that cannot be accessed by unauthorized individuals.
- Physical media should be stored in locked drawers and cabinets when not in use.
- Encryption of all digital information is encouraged.
- Limit the number of copies of data to the minimum possible and do not retain longer than needed.
- Confidential data has specific requirements:
 - Data must be encrypted with the decryption key stored separately
 - Departments and Data Owners are responsible to comply with all applicable laws and regulations regarding the dissemination and protection of data that is confidential including, but not limited to the Family Educational Rights and Privacy Act (FERPA) of 1974 and GLBA.
 - An inventory of physical media containing confidential information must be maintained by the department in accordance with all applicable laws and regulations. The inventory must include the description, Data Owner, current location of the media, date of destruction (length of retention), the classification of data and the purpose for keeping the data.
- Secure data storage meets these requirements
 - Physical data (such as paper documents or removable media) must be kept under lock and key.
 - Electronic data must be encrypted using industry best practices when at rest.
 - Mobile devices storing secure data must be encrypted using industry best practices including but not limited to BitLocker.
- As Data Custodians ITS maintains backups of data on site, remotely and offline for DR.

In-motion: Physical Media Transmission

- Avoid printing confidential data unless necessary.
- Use care when printing to ensure the paper copies are not left unattended, for example on printers or desks.
- Shred printed copies when they are no longer needed.
- Ensure mailings are addressed carefully and sent in sealed envelopes.
- Do not save confidential or internal use data to unencrypted removable or unapproved physical media such as:
 - USB thumb drives
 - CD-ROM discs
 - External hard drives

In-motion: Electronic Transmission

- Encryption should be used during transmission.
- Confidential data must be encrypted during transmission.
- Use secure e-mail encryption systems when e-mailing confidential data.
- Avoid faxing confidential data.

- Use care to ensure paper copies are not left unattended when using fax machines and are promptly secured or shredded when no longer needed.
- Avoid saving or making extra copies of data outside of approved backup systems.
- Compensating controls must be formally documented and the reason for the exception.
- Maintain a network and computer system that provides safeguards against unauthorized access of these data.
- Maintain software and hardware encryption software for the enterprise.

Data Classifications

- **Public Data**
 - Data Security is not required.
- **Internal Use Data**
 - Should not save to “personal devices” such as thumb drive or personal phone.
 - Should be encrypted in-motion when transmitted over the Internal network.
 - Should be encrypted at-rest.
 - Must not be saved to non SFCC approved cloud or 3rd party systems.
 - Must be encrypted in-motion over the Internet.
 - Must be encrypted at-rest on mobile devices.
- **Confidential Data**
 - Should be encrypted in motion when transmitted over the Internal network.
 - Must not save to personal devices.
 - Must not be saved to non SFCC approved cloud or 3rd party systems.
 - Must be encrypted in-motion over the Internet.
 - Must be encrypted at-rest on mobile devices.
 - Must be encrypted at-rest on internal systems.

Retention

- Data should be retained for as long as is required to achieve the purpose for which data were collected and processed pursuant to GDPR (General Data Protection Regulation) Article 5.
- All data must have a retention definition.
- Data Owner must be aware of all legal requirements for retaining and documenting data.

Data Backups

- Information Technology Services maintains documentation on the back-up and retention procedures and ensures that those policies and procedures are followed consistently. The retention policy specifies the amount of time that a particular item of data can be recovered after it has been deleted but in no case shall it exceed 120 days for data, or 18 months for e-mail.
- Responsibilities
 - **Data Custodian**
 - The central IT organization at the college and at each college location will establish and publish retention schedules for any back-up and deleted data managed by those groups. This will include, but is not limited to, systems such as the central email servers and Banner.
 - **Data Executive and Owner**
 - The legal custodian of the information remains responsible for ensuring that data that constitutes a college record is handled appropriately.

- **Data Owners**

- Administrative, academic and other divisions or departments that provide or manage central storage service for their users must document their back-up and retention policies or procedures.

Table 1: Data Backup and Archive retention periods

Type of Record	Description	Official Repository	Duration
communications	Employee E-Mail	Information Technology Services	18 Months
communications	Student E-Mail	Information Technology Services	0 Days
data	File Server	Information Technology Services	120 days
data	Log files	Information Technology Services	120 days
data	User files and databases stored on campus servers	Information Technology Services	120 days
communications	Phone call detail logs	Information Technology Services	120 days
communications	Voicemail	Information Technology Services	0 Days
communications	Instant Messaging	Information Technology Services	7 days

Data Archive

- All email sent to and received from employee SFCC email accounts are automatically archived for 18 months (sliding window). This is within the requirements for archiving of electronic communications in the regulation set forth by the Missouri Secretary of State, Section 109, RSMo.

Cloud Systems

- All cloud systems retention processes must be documented.
- Cloud systems should be configured to meet SFCC retention requirements.

Destruction

Once data and/or data systems have reached the end of their data life cycle, they will be destroyed per the following guidelines.

Follow all Missouri state and Federal laws, guidelines, and recommendation for destruction of physical media.

- Electronic files
 - When electronic records have reached the end of their data life cycle the record should be deleted.
- Physical Electronic Media Destruction
 - Follow all State laws, guidelines, and recommendation for destruction of physical electronic media.
 - Departments must ensure that tapes or other forms of media scheduled for destruction are disposed of properly. - non its managed systems.
 - Examples include but are not limited to:
 - Removable media such as usb thumb drives
 - Mobile device, computer and server hard drives

- Non-electronic Physical media
 - Departments are responsible for all physical paper destruction per all State and federal laws, guidelines, and recommendations for destruction of physical media.
 - Destroy paper media using a cross-cut shredder or similar appropriate technology and then recycle or discard.
 - Including but not limited to:
 - paper
 - microfiche records
- Data Archive
 - Configured to automatically delete based upon a sliding window.
- Data stored with a Cloud vendor
 - Document proof of destruction.

Definitions

3rd party systems - A vendor or entity not of SFCC.

All members of the community - Employees, students, alumni, donors, board members and volunteers.

Archive - Longer term storage of data after its active life.

At-rest - Electronic Information which is saved or stored physically in any electronic form (e.g., databases, data warehouses, spreadsheets, archives, tapes, off-site backups and mobile devices).

Authorization – See Regulation 8330. The official management decision given by an organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations based on the implementation of an agreed-upon set of security controls.

Authentication – See Regulation 8310. Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

Backup - (1) The process of making duplicate copies of electronic data, typically for security reasons. Different from the process of archiving a record. Backups of electronic information are made in case of equipment failure, etc. to ensure the availability of active records for ongoing administrative purposes. (2) A substitute or alternative. May refer to a disk or tape that contains a copy of data, or to a person authorized to act in the absence of another person.

Cloud - System or provider that stores SFCC data somewhere other than physically on an SFCC owned system.

Compensating controls - Alternative mechanisms that are put in place to satisfy the requirement for a security measure that is determined to be impractical to implement at the present time.

Data collection - Identifying and defining the process and framework for entering and accumulating data.

Data entry - Inputting & entering data into systems per defined collection process.

Disaster recovery (DR) - An organization's method of regaining access and functionality to its IT infrastructure after events like a natural disaster, cyber-attack, or even business disruptions related to the COVID-19 pandemic. A variety of disaster recovery (DR) methods can be part of a disaster recovery plan. DR is one aspect of business continuity.

Disk encryption software - Computer security software that protects the confidentiality of data stored on computer media (e.g., a hard disk, floppy disk, or USB device).

Encryption - Any procedure used in cryptography to convert plain text into cipher text to prevent anyone but the intended recipient or owner from reading that data.

FERPA - Family Educational Rights and Privacy Act of 1974 otherwise known as the Buckley Amendment.

GLBA - Gramm-Leach-Bliley Act.

GDPR - General Data Protection Regulation.

Hardware - Physical Server data storage, CPU, Memory, Network devices.

In motion - When data is transmitted between two systems either by a user or through automation.

Internal (local) - SFCC internal network main campus and remote campuses.

Internal systems - Systems and devices physically connected to the SFCC network.

IR – Institutional Research Department.

Log files - Computer-generated data files that contain information about usage patterns, activities, and operations within an operating system, application, server or another device.

Maintenance - Any act that either prevents the failure or malfunction of equipment or restores its operating capability.

Personal devices - Devices not directly owned by SFCC.

Personally Identifiable Information (PII) - information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means.

PCI DSS – Payment Card Industry Data Security Standard.

Retention – The act of keeping or storing information/data for a particular time period.

Sliding window – The concept in archiving data where the storage system is configured to automatically delete data past a certain time period such as 18 months from current date.

(Revised 2/2023 – RR)

Data Security – Gramm-Leach-Bliley Act Safeguards Rule

The intent of this document is to describe how the various components of the college's information security program are in accord with, and support compliance with, the [Gramm-Leach-Bliley Act Safeguards Rule \(GLBA\)](#), and to provide references to additional materials and to applicable policies and guidelines.

GLBA Objectives and Requirements

In compliance with the Gramm-Leach-Bliley Safeguards Rule and regulations issued by the Federal Trade Commission pursuant to that Rule, the college has established this Information Security Plan to:

- Ensure the security and confidentiality of customer information.
- Protect against anticipated threats to the security or integrity of customer information.
- Guard against unauthorized access to or use of customer information that could result in harm or inconvenience to any customer.
- Comply with applicable Gramm-Leach-Bliley rules as published by the Federal Trade Commission.

Consistent with its efforts to meet these objectives, the college will:

- Designate one or more staff members to oversee and coordinate the Information Security Plan.
- Conduct risk assessments to identify foreseeable internal and external risks that could lead to unauthorized disclosure or misuse of confidential information.
- Implement plans to control the risks.
- Contractually require third-party service providers to implement and maintain confidentiality safeguards.
- Periodically evaluate and adjust the Information Security Plan to ensure ongoing protection of confidential information.

Coordination of the GLBA Information Security Plan

The following staff play a role in coordinating the various aspects of the information security plan:

- The Technical Director coordinates the college-wide Information Technology security program and assists units in their security implementation, in accordance with SFCC regulations 8300 and 8400.
- The Information Technology Services Advisory Committee (ITSAC), chaired by the Chief Information Officer, oversees the subcommittees IT Policy and Regulations (ITSAC-P) and Standards (ITSAC-S). The subcommittees evaluate specific GLBA-required standards to ensure they are incorporated into the plan. Any recommendations are made to the GLBA compliance Officer, the Director of Financial Aid.
- The Director of Financial Aid oversees compliance with the GLBA and receives and reviews all recommendations for change. (Approved 10/2022)

Hardware and Software Support

The College shall maintain a list of supported computer hardware and software. Purchases of products on the College's list will be supported by Educational Technology Services in terms of compatibility, installation, training, maintenance, troubleshooting, and upgrades. Educational Technology Services may decline to provide support for products not on the list. Faculty and staff who wish to purchase products for institutional use that are not on the College list may submit those products to the appropriate Educational Technology Services advisory committee for review and possible recommendation to the President, who shall review recommendations during the annual budgeting process.

The Vice President of Technology Services will approve all purchases of hardware and software. Educational Technology Services may decline to provide support for products not on the standards list. Faculty and staff who wish to purchase products for institutional use that are not on the College's standard list may submit justification for the non-standard product to the Educational Technology Services Advisory Committee for review and possible approval. Appeals to the ETS Advisory Committee decision may be appealed to the Executive Leadership Team.

Please go to the Standards web page for the up to date hardware standards.

Electronic Communications

The College provides e-mail services for faculty and staff for use when engaging in activities related to College business. Incidental personal use that does not interfere with College operations generate incremental identifiable costs, saturate the data networks of the College, or negatively impact the individual's job performance is permitted. E-mail may not be used for commercial purposes or for personal financial gain. In addition, users shall accept and comply with the individual responsibilities relating to computer and information technology set forth in the SFCC Appropriate Use Policy and Regulation 8200.

This e-mail policy covers all uses of the College e-mail facilities. Any user of College email facilities consents to all provisions of this regulation and agrees to comply with all of the terms and conditions set forth herein, all other applicable College policies, regulations, and procedures, and with applicable local, state, and federal laws and regulations.

Users of College E-mail Facilities whose actions violate this policy or any other College policy or regulation may be subject to revocation or limitation of e-mail privileges as well as other disciplinary actions or may be referred to appropriate external authorities.

Access to E-mail:

SFCC provides College E-mail Facilities for legitimate College-related activities to faculty, students, staff, and other individuals and entities granted e-mail privileges at SFCC, as well as connections between on-campus electronic mail systems and external data networks. The use of College E-mail Facilities -- like the use of any other Collegeprovided resource and like any other College-related activity -- is subject to the normal requirements of legal and ethical behavior within the College community. Thus, legitimate use of College E-mail Facilities does not extend to whatever is technically possible.

SFCC E-mail Account:

Staff members with access to a College-owned computer on campus and faculty are required to activate their Official SFCC E-mail Account. Users are expected to read, and shall be presumed to have received and read, all official SFCC e-mail messages sent to their SFCC E-mail Accounts.

Individual academic and administrative units may choose to operate their own e-mail facilities as an alternative to the centrally available resources, but the use of any such facilities shall also be subject to this policy.

Acceptable Use:

State Fair Community College provides College E-mail Facilities for activities and associated administrative functions supporting its mission of learning, discovery, and engagement. Although modest personal use of College E-mail Facilities is allowed, College E-mail Facilities should be used for College-related educational and administrative purposes. Any use of College E-mail Facilities that interferes with College activities and functions or does not respect the image and reputation of SFCC is improper.

Policies and regulations that apply to other forms of communications at the College also apply to electronic mail (Reference Regulation 8200 - Appropriate Use). In addition, the following specific actions and uses of College E-mail Facilities are improper:

1. Concealment or misrepresentation of names or affiliations in e-mail messages.
2. Alteration of source or destination address of e-mail.
3. Use of e-mail for commercial or private business purposes that have not been approved.
4. Use of e-mail for organized political activity or political solicitation.
5. Use of e-mail to harass or threaten other individuals.
6. Use of e-mail that degrades or demeans other individuals.

Public Record and Privacy:

Any e-mail sent from users at State Fair Community College or residing on SFCC E-mail Facilities may be a public record and may be subject to disclosure.

SFCC does not monitor the content of electronic mail as a routine procedure. The College reserves the right to inspect, copy, store, or disclose the contents of electronic mail messages, but will do so only when it believes these actions are appropriate to: prevent or correct improper use of College E-Mail Facilities; ensure compliance with College policies, procedures, or regulations; satisfy a legal obligation; or ensure the proper operations of College E-mail facilities or the SFCC Data Network. Any SFCC administrator who believes such actions are necessary must first obtain the written approval of an appropriate administrative authority: a dean in the case of an academic unit, or a director in the case of an administrative unit.

Use of E-mail for SFCC Business:

The official SFCC e-mail account shall be considered an official means for communicating College business, and may in some cases be the sole means of communication. Users are expected to read, and shall be presumed to have received and read, all official SFCC e-mail messages sent to their official SFCC e-mail accounts. Because the contents of such e-mail are subject to laws governing public records, users will need to exercise judgment in sending content that may be deemed confidential. Furthermore, e-mail transmissions may not be secure, and contents that are expected to remain confidential should not be communicated via e-mail. Common examples of confidential contents include: student grades, personnel records, individual donor gift records, and data subject to the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Family Educational Rights and Privacy Act (FERPA) regulations, and the Gramm Leach Bliley Act (GLBA).

Deans, vice presidents, and their appointees may send broad-based messages relating to College business without any prior approval. The author of any business messages, however, assumes responsibility for assuring that messages do not violate any College policies, regulations, or procedures. Disclaimers of confidentiality included in e-mail messages do not protect the sender if confidential information is shared or disclosed inappropriately.

Mobile Communications

Cellular telephones and cellular-based wireless communications devices can be an effective resource for campus employees in the performance of their job duties. For employees who spend considerable time outside of their assigned office area, or who must be accessible outside of scheduled or normal work hours, a cellular or mobile device can be a significant benefit. Based on job duties, certain employees may qualify to be provided a stipend to cover the business use of personal cell phones. The college provides access to e-mail and calendaring through Blackberry Enterprise enabled phones. Other phones are currently not supported for access to these services.

Due to the requirement to comply with IRS regulations regarding personal use of institutionally owned devices and the difficulty and time intensive manual labor required to identify, track and determine personal versus business use, the College will no longer provide cell phone service to individual employees. In short, it will be up to the individual employee to claim business use based on appropriate documentation of personally owned cell phones, either as a reimbursement from the College or as a business deduction on their personal tax return.

The level of institutional cost for cell phone service has rapidly increased over the past few years. To bring costs more into line with the level of institutional benefit, a stipend regulation for cost sharing has been adopted. This regulation assumes that for most employees the device will be used for both personal and business use.

Certain employees may qualify for the college to provide an institutional stipend to cover the presumed business use of personal cell phones and service. The stipend will be considered taxable income to the employee. The level of cash subsidy (stipend) will be determined by a person's job duties as it relates to cell phone use and access. Guidelines to categorize cellular use as mandatory, beneficial or incidental are determined by the department head. The stipend includes the cost of service plus equipment. The college will review and set the amounts to be provided for stipends and reimbursement on an annual basis. Institutional Stipend This regulation institutes an institutional stipend to cover presumed business use of personal cell phones for certain employees

Institutional Stipend

This regulation institutes an institutional stipend to cover presumed business use of personal cell phones for certain employees.

1. Employee responsibilities: The employee will purchase cellular phone service and equipment and assume responsibility for vendor terms and conditions. The employee is responsible for plan choices, service levels, calling areas, service and phone features, termination clauses, and payment terms and penalties. The employee is also responsible for the purchase, loss, damage, insurance, and/or replacement of phone equipment.

2. Guidelines to receive a stipend: Based on job duties as it relates to cell phones, three categories are identified to determine if the employee should be provided a stipend to offset the cost of a personal cell phone and service.
 - a. Mandatory--the institution requires an employee to have a cell phone to fulfill job duties. The President upon recommendation from an area Vice President will approve qualifying employees in this category. Employees in this category have duties that require access by the college while away from the office or in off-hour situations. Service is required for "on-call" personnel to be contacted in the event of an emergency or service need. Service is provided for life or safety requirements.
 - b. Beneficial--the use of a cell phone is not mandatory but is considered highly beneficial to an employee to fulfill job duties. An area Vice President will approve the stipend paid to employees in their area that qualify under this category. Service is provided so that an employee can work more efficiently, or that their working conditions require that they are away from traditional communications resources. Simple convenience is not sufficient to qualify for a monthly stipend.
 - c. Incidental or occasional use – reimbursement for business use of a personal device would be allowed at a fixed rate for all others. This would be in the form of a business related reimbursement request instead of a monthly stipend.
3. Levels of stipend payment: There are many cell phone carriers with varying plans for phone equipment and service. The payment levels are intended to cover a presumed level of business use of personally owned service and equipment in keeping with institutional benefit. The regulation assumes that for most employees the device will be used for both personal and business use, therefore the overall costs are shared.
 - a. Basic Use/Voice Service – this stipend level is intended to cover a portion of the employee's expense for monthly service costs and a contribution toward the cost of equipment and accessories. This stipend level would cover basic/voice cellular service to meet institutional job duties.

- b. Enhanced Use/Voice + Data Service – this stipend level is intended to cover a portion of the employee’s expense for monthly service costs and a contribution toward the cost of equipment and accessories. This stipend level would include voice service, plus data phone or Smartphone features that provide access to e-mail or web based services that would be required to meet institutional job duties. This service would apply to Coaches and managers.
- c. Mandatory Use/Full Voice + Data Service – this stipend level is intended to cover a substantial portion of the employee’s personal expense for monthly service costs, equipment and accessories. This stipend level would apply to members of the Executive Leadership Team and to approved directors.
- d. Incidental/Occasional Use – this reimbursement level will be a “per-minute flat rate” with appropriate documentation provided by the employee.

Amounts listed in each category above will be reviewed and set annually by the Vice President for Finance, Administration and Human Resources and approved by the Executive Leadership Team. The stipend amounts will be listed on the annual **Cell Phone Stipend Agreement**. The reimbursement flat rate can be obtained from the Business Office.

4. Additional Regulation Guidelines:

- a. The stipend amount will be considered taxable income to the employee and added to their monthly paycheck. The stipend levels are set to provide for the additional tax burden an employee would incur.
- b. The department of an employee receiving a monthly stipend, or incidental use reimbursement will provide the appropriate budget funding.
- c. A **Cell Phone Stipend Agreement** will be completed by the employee and approved by the area Vice President or President. Updates or changes to cell phone service (phone numbers, voice/data vs. voice only, stipend amount, etc...) will be reported promptly to the employee’s department head. The list of users by departments will be approved for renewal each year and reported to the area Vice President or President.
- d. If the employee resigns, is terminated, transfers departments, or no longer qualifies for an institutional stipend; the area Vice President will promptly notify the Business Office to discontinue the stipend payment.
- e. The employee’s supervisor and area Vice President or President are responsible for an annual review of the business need for a cell phone stipend and whether the agreement should be continued.
- f. Exceptions: there may be rare circumstances where the stipend level must be adjusted due to extenuating conditions. The President upon recommendation from a Vice President will approve exceptions.
- g. Certain “departmental assigned phones” will be provided by the College.
- h. If the level of expense by the employee exceeds the stipend amounts received from the College, the employee could claim the overage (with sufficient IRS documentation) on their personal tax return.

Guidelines for Mobile Phone Use

1. Personal use – the stipend regulation assumes that the cell phone will be used for both personal and business calls. Since the stipend amount is taxable as income, the employee is not required to track business vs. personal use to report to the college.
2. Institutional benefit – the stipend agreement requires that the personally owned device is available for business access. An employee receiving a stipend must maintain active cell phone service. The employee agrees to carry the cell phone with them, keep it charged and in operational condition, and be accessible for business use as required by their department head or supervisor.
3. Appropriate use – the employee agrees to use the phone in ways consistent with college regulations 8200, 8300, 8400 and all applicable local, state or federal laws. Inappropriate and unlawful use of cell phone features, such as camera equipment, is prohibited.
4. Use of a cell phone while operating a vehicle – cell phones users must be aware of state and municipal laws regarding the use of phones while driving. The laws vary widely by location. In addition, use of phones while driving can cause hazardous distraction, especially in adverse weather, heavy traffic, or limited visibility conditions.
5. Wireless network - The College has provided wireless access to campus resources in three its four locations. The wireless network is accessible from wireless laptops, netbooks, Mac's and PC's that have current antivirus software and can run the Cisco Clean Access application. Since a phone cannot yet support these applications it is in the best interest of the college to not allow access to the wireless network with mobile phones or PDA's.
6. Campus resources – Access to college e-mail and calendaring services is only supported with a Blackberry phone that has been enabled to work in an enterprise environment. Regulations 8200, 8300 and 8400 apply when using a mobile device to access campus Resources.
7. Phone security – To help secure the data that could be stored on the phone it is important to password protect the Blackberry phone.
8. Loss or theft – Report loss or theft of phone within 24 hours.

Departmental Provided Mobile Phones

There are some circumstances where a “departmentally assigned cell phone” may be provided by the College that is not assigned to a specific individual. In these cases, the College will provide cell phone service and equipment.

1. Service and equipment procurement – Business Office will arrange for service and phone equipment as appropriate.
2. Monthly billing statements from the carrier – Business Office will process the carrier invoices for payment. The invoice breaks down the costs by individual telephone number including voice and data service plans, special features, plus any equipment that might have been purchased for that phone number. When new service is ordered Business Office requires a budget number from the responsible department to associate

with the new phone number.

3. Departmental bill back – Business Office allocates the full amount of each individual billing statement to the responsible departmental budget number on a monthly basis. These charges are submitted electronically and employees will not get additional paperwork or summaries other than what is available through the normal budget review process. However, budget managers may contact Business Office at any time to obtain additional copies of the detailed billing statements that have been billed to the department. In the event that billing errors are detected by Business Office, or reported to Business Office, the carrier representative is contacted to make adjustments in subsequent billing periods.
4. Usage tracking and review - It is the responsibility of the department to review monthly billing statements. Employees should confirm the usage charges and review any additional features or equipment included on the statement.
(Approved 7-25-11)

Privacy Notification

The college will use reasonable efforts to maintain the privacy of users accessing its Web site and portal. As with all online services, however, SFCC cannot guarantee users of its Web site and portal absolute privacy over their use. In some cases, user information may be subject to disclosure under state or federal public record or freedom of information laws. Further, while the college has in place a variety of security measures to safeguard against illegal access of information obtained through its Web site and portal, the college cannot provide complete assurance against illegal access. Additionally, information obtained through the college's Web site and portal may be disclosed in the course of a civil or criminal investigation.

This policy informs you of the information that we may collect from you, what we do with it, to whom it may be disseminated, and how you can access it.

Network Traffic

In the course of ensuring network security and consistent service for all users, the college employs software programs to monitor network traffic, identify unauthorized access or access to nonpublic information and to detect computer viruses and other software that might damage college computers or the network. In the course of such monitoring, these programs may detect such information as e-mail headers, addresses from network packets and other information. Information from these activities is used only for the purpose of maintaining the security and performance of the college's networks and computer systems. Personally identifiable information from these activities is not released to external parties without your consent unless required by law.

Information Automatically Collected

When you browse through any Web site and portal, certain information about you can be collected. We automatically collect and temporarily store the following information about your visit:

- the date and time of your visit;
- IP address; • browser type, operating system and language;
- the pages you visited; and
- the address of the Web site from which you came.

We use this information for statistical purposes and to help us make our site more useful to visitors. This site makes no attempt to identify individual visitors from this information.

Cookies

Cookies are pieces of information stored by your Web browser on behalf of a Web site. Portions of our site may use cookies to carry data about your current session at the site from one Web page to the next. We do not forward cookies to any external parties. If you prefer not to receive cookies, you may turn them off in your browser, or may set your browser to ask you before accepting a new cookie.

Information Voluntarily Provided by You

We may collect voluntary information from you on our Web site or portal in a variety of ways: through surveys, online forms and e-mails, an authentication feature, and the use of electronic payment functionality. This information can be data that could reasonably be used to identify you, including your name, address, telephone number, e-mail address, Social Security number, birth date, bank account information, credit card information, or any combination of information that could be used to identify you.

Any Web site or other electronic means that conducts online research with human subjects are required to follow the provisions of the college's Institutional Review Board (IRB)

Web sites that collect individually identifiable information and provide services to children 12 and under may also be required to comply with provisions of the Children's Online Privacy Protection Act (COPPA).

Disclosure

We will not sell, exchange or otherwise distribute your personally identifiable information without your consent. Personal data may be released, however, pursuant to a request for such data in accordance with state or federal public record or freedom of information laws, or in the course of a civil or criminal investigation. Further, if you are a student at the college, any personal data released by the college shall be done in accordance with the federal Family and Educational Rights and Privacy Act (FERPA).

In addition, the information that you voluntarily submit will be disclosed only to SFCC employees or officials, or those under contract with SFCC, with a "need to know" for purposes of fulfilling their job responsibilities. The information may be used to answer your questions, respond to any requests for assistance, authenticate you for access to certain transactions and information, process and give you credit for any payment transactions, aid in the planning, design and development of the Web site, and fulfill the college's legal obligations.

Security

Because e-mail sent to the college is not encrypted, you should not send messages containing information that you consider highly sensitive to any address on this Web site.

We use standard security measures to ensure that information provided by you, including your personally identifiable information, is not lost, misused, altered, or unintentionally destroyed. We also use software to monitor network traffic to identify unauthorized attempts to upload or change information, or otherwise cause damage. Except for those grounds previously stated, no attempts are made to identify individual users or their usage habits. The transmission of registration IDs and passwords, personalization information, and payment information is encrypted.

Your Access

The college may maintain personal data you disclosed during your use of the Web site or portal. If you would like to review your personal data, please contact the college. Student data is maintained by the Student Services Office and employee data is maintained by the Human Resources Office.

External Links

Our Web site and portal have links to many other non-profit, educational, and governmental institutions, and in a few cases, private organizations. You are subject to those sites' Privacy Policy when you leave this site. Reference in the college's Web site or portal to any specific service, company, or organization does not constitute its endorsement or recommendation by State Fair Community College. SFCC is not responsible for the contents of any "off-site" Web page referenced from our server. (Approved 5/19/2008)