

1 INTRODUCTION

1.1 Purpose

SFA's Information Security Policies cover all of the management decisions, intentions, definitions, and rules relating to information security, and thus define SFA's Information Security Management Program. These policies determine the minimum level of security required at SFA and establish the criteria against which results are measured. These SFA Information Security Policies provide the foundation for the various information security guidelines, standards and processes and procedures.

1.2 Scope

Information security refers to the provision of organizational, technical and management measures necessary to safeguard information asset against unauthorized access, disclosure, duplication, denial of use, modification, diversion, destruction, loss, theft, or misuse, both malicious and accidental. Information security jurisdiction covers all information assets (the property of the U.S. Government) in the U.S. and begins with the electronic input of data and ends with its output on an electronic or non-electronic output medium.

In the interest of brevity "information security" may be omitted in the text. However, the reader should keep in mind that this entire policy set relates only to the subject of information security. Additionally, this policy encompasses systems and system users, not infrastructure.

1.3 SFA Security Fundamentals

The following high-level fundamentals provide the basis for all information security activities:

- **Individual Accountability**
Each individual is responsible for his or her actions, as it relates to the safeguarding of SFA information assets.
- **Need-to-Know and Need-to-Do (Least Privilege)**
Each individual is only authorized to access such SFA information assets that are required for performance of his or her job.
- **Separation of Duties and Functions**
To ensure that no one individual has exclusive control over a particular information asset or process, there should be a real and lasting separation of authority and responsibility. In addition, to ensure stability of SFA computing environment, there should be separation of development and production tasks.
- **Principle of Proportionality**
Information security measures should be implemented in reasonable proportion to the risk and business value they intend to protect.
- **Maintenance of Trust**
Security should be maintained at the level that will not compromise the integrity of the trusted environment.
- **Security by Design**
To ensure a sound security environment, single point solutions are discouraged and will be integrated within an overall strategic security architecture. Information security policies, guidelines, standards and day-to-day execution of the Information Security Program will always be consistent with these principles. The Principles are

simple, broad statements that form a "Constitution" for information security, tailored to the needs of SFA.

1.4 Compliance

Compliance with information security policies is mandatory. If an individual violates the provisions in an information security policy, either by negligence or intent, SFA reserves the right to take appropriate disciplinary action in accordance with SFA's rules of behavior.

1.5 Exceptions

Exceptions to any policy as a result of a risk-based decision must be approved by the SFA CIO, which may require higher level management authorization. All exceptions to policies will be formally recorded, tracked, and reviewed by the SFA Management.

1.6 Applicability

Information security policies apply to all information assets, processes, and all SFA employees. Outside consultants, contractors, temporaries, or third parties accessing SFA information assets are subject to the same information security requirements, and have the same information security responsibilities, as SFA's partners and employees.

All individuals are obligated to continue protecting SFA's information by observing information security policies after their termination of employment with SFA.

1.7 Policy Administration

Information security policies will be reviewed as often as necessary but no less than annually. Additional policies may be issued as needs arise, and will be incorporated into the Information Security Policies document.

1.8 References

This document is based on guidance extracted from the following documents:

- NIST 800-18, Guide for Developing Security for IT Systems
- NIST Special Publication 800-XX, Self-Assessment Guide for Information Technology Systems
- International Standard – Information Technology – Code of Practice for Information Security Management
- U.S. Dept of Education Information Technology Security Policy

These documents provide a comprehensive set of baseline controls comprising best practices in information security. By adopting these controls and practices, SFA ensures that the "due care" and "due diligence" requirements are met.

1.9 Strategies

SFA information security strategies are long-term directions that serve as the basis for adequate planning and security solutions to meet the SFA business needs now and in the future. SFA information security is multi-dimensional. To be effective, information security requires continuing consideration of the following:

- Information security tools, methods, and practices will not rely on secrecy in order to be effective.
- Information security decisions and issue dispositions will be based on risk analysis and assessment methods that include metrics that capture the short- and long-term business value of alternatives.
- Information security includes continuing reviews of the business value of the security measures already in place.
- Information security management evolves to global methods and global standards with execution and accountability distributed by region and/or business entities when appropriate.

1.10 Security Organization

All individuals who introduce or use SFA information assets must ensure that security policies are in place and managed accordingly. Effective management of information security requires that:

- Everyone who has access to SFA information assets understands security roles and responsibilities.
- Information security risks are managed so that appropriate measures can be taken to protect SFA information assets.
- Awareness programs are created to ensure that security policies are communicated.
- Security incidents, violations, and known vulnerabilities are reported to management and the Information Security Group.
- Outsourcing of information services to a third party service provider does not introduce any degradation of information security.

1.11 Roles and Responsibilities

TBD

1.12 Document Structure

This policy document is divided into three categories: Enterprise Management Controls, System Operational Controls, and System Technical Controls. The format of the document maps closely to NIST Special Publication 800-18. This feature will aid in the implementation of the policy in the form of System Security Plans.

1.12.1 Management Controls

The Management Controls section addresses security topics that can be characterized as managerial. They are techniques and concerns that are normally addressed by management in the organization's computer security program. In general, they focus on the management of the computer security program and the management of risk within the organization. The types of control measures shall be consistent with the need for protection of the major application or general support system.

1.12.2 Operational Controls

The Operational Controls section addresses security controls that focus on controls that are, broadly speaking, implemented and executed by people (as opposed to systems). These controls are put in place to improve the security of a particular system (or group of systems). They often require technical or specialized expertise and often rely upon management activities as well as technical controls.

1.12.3 Technical Controls

The Technical Controls section focuses on security controls that the computer system executes. These controls are dependent upon the proper functioning of the system for their effectiveness. The implementation of technical controls, however, always requires significant operational considerations and should be consistent with the management of security within the organization.