

Section	Policy Statement
2.1 Risk Management	Risk Management, in simple terms, is the identification, control, and minimization or elimination of security risks within an acceptable cost.
	Each SFA program official shall assess the risk to systems under their control and determine the acceptable level of risk.
	Every system shall document final risk determinations and related management approvals shall be documented and maintained on file.
2.1.1 Risk Assessment	A risk assessment is an assessment of threats and vulnerabilities of information and information processing facilities, the likelihood of their occurrence, and the impact to the organization
	Every system shall conduct a risk assessment upon a change in security posture.
	The risk assessment shall consist of a documented analysis defining the vulnerabilities, threat sources (both natural and manmade), system flaws and weaknesses, and effectiveness of current or proposed safeguards required to lower potential loss.
	Each risk assessment shall include the date the system risk assessment was completed.
	Every system shall perform a risk assessment before the approval of design specifications for new systems.
	Every system shall perform a risk assessment and documented each time a major change occurs to the system, facilities, or other conditions.
	Every system shall perform a risk assessment a minimum of every five years.
	Every system shall conduct a risk assessment prior to authorizing a system for processing.
2.1.1.1 Sensitivity Analysis	An analysis of the criticality, sensitivity, and integrity of the information handled by each SFA system shall be described.
	Analysts/programmers who will use the system to help design appropriate security controls and also include internal and external auditors evaluating system security measures shall be included in performing the sensitivity assessment
	The sensitivity analysis shall contain both a general description of sensitivity and a list of applicable laws, regulations, and policies that establish specific requirements for confidentiality, integrity, or availability of data/information in the system.
	If the system processes records subject to the Privacy Act, include the number and title of the Privacy Act system(s) of records and whether the system(s) are used for computer matching activities.
	In the sensitivity analysis, indicate if the protection requirement is high, medium, or low for each of the following three categories: confidentiality, integrity, and availability.
2.1.2 Risk Mitigation	
2.1.2.1 Business Impact Analysis	Every system shall conduct a mission/business impact analysis prior to implementing findings of the risk assessment.
2.1.2.2 Consequence Assessment	Every system shall conduct a consequence assessment, which estimates the degree of harm or loss that could occur prior to implementing findings of the risk assessment.
2.1.2.3 Countermeasure Analysis	With input from SFA managers, Every system shall conduct a countermeasure analysis, which determines whether the security requirements in place adequately mitigate vulnerabilities.
	A cost benefit analysis shall be conducted to support decisions on the most cost-effective countermeasures to security risk.
2.2 Security Control Reviews	Every system shall perform an independent review of security controls at minimum every three years or every time a significant change occurs.

Section	Policy Statement
	Every system shall conduct a periodic review of the operating system to ensure the configuration prevents circumvention of the security software and application controls.
2.2.1 A-130	Every system shall document description of the type of review and findings, including information about the last independent audit or review of system and who conducted the review. An indication shall be made if the review identified a deficiency reportable under OMB A-123 or the Federal Managers' Financial Integrity Act if there is no assignment of security responsibility, no security plan, or no authorization to process for a system.
	Every system shall routinely test and examinations of key controls, i.e., network scans, analyses of router and switch setting, and penetration testing.
2.2.2 NIST Self-Assessment	Every system shall conduct a routine self-assessment every three years.
2.2.3 Corrective Action Plans	Management shall discuss findings and recommendations of the Corrective Action Plan, including information concerning correction of deficiencies or completion of recommendations, and ensure that significant weaknesses have been reported and corrective actions are effectively implemented.
2.3 System Security Plan	The system security plan shall discuss the system and its relationship with all interconnected systems, and contain the topics prescribed in NIST Special Publications 800-18.
2.3.1 General Policy	The system security plan shall be developed, updated, reviewed, and adjusted periodically to reflect current conditions and risks.
2.3.2 Configuration Management	Security plans should be dated for ease of tracking modifications and approvals.
2.3.3 Document Control	Security plans should be marked, handled, and controlled to a determined level of sensitivity.
2.3.4 Enterprise Policy	A summary of the plan shall be incorporated into the strategic IRM plan.
	Security controls shall be consistent with and an integral part of IT architecture of the agency.
2.4 Rules of Behavior	Rules of Behavior shall reflect administrative and technical security controls in the system.
2.4.1 General Policy	The Rules of Behavior shall be made available to every user prior to receiving authorization for access to the system, and it is recommended that the document contain a signature page for each user to acknowledge receipt.
	A set of rules of behavior shall be established for each system by managers at all levels to control access to, and use of equipment that permits access to any SFA system.
	The Rules of Behavior shall clearly delineate responsibilities and expected behavior of system users, and hold users responsible for their own actions by stating consequences of inconsistent behavior or noncompliance.
	The Rules of Behavior shall contain termination procedures for a friendly and unfriendly termination.
	Differentiation should be made between rules that must always be enforced versus rules that are conditional or optional, and guidelines that express what is forbidden unless expressly authorized versus what is permitted unless expressly forbidden.
2.4.2 Specific Policy for Users	The Rules of Behavior shall state that terminals will not be left unattended or unsecured while connected to a network.
	The Rules of Behavior shall state that sensitive media must be locked away when not in use, and computers and terminals should not be left logged on while unattended (Clear Desk and Clear Screen Policy).
	The Rules of Behavior shall state that users must abide by software licensing laws, and will prohibit the use of unauthorized software.

Section	Policy Statement
	The Rules of Behavior shall state that individual modems are not allowed on departmental PCs connected to the network.
	The Rules of Behavior shall include appropriate limits on interconnections to other systems and define service provision and restoration priorities, including matters such as work at home, dial-in access, connection to Internet, use of copyrighted works, unofficial use of government equipment, the assignment and limitation of system privileges, and individual accountability.
	The Rules of Behavior will include guidance on password selection and usage, including requirements that passwords should be kept confidential, not shared, not be recycled, not based on easily guessed information, not recorded on paper at their desk, etc.
2.5 Solution Life Cycle	All SFA systems shall follow the SFA SLC methodology for security.
2.5.1 General	A status shall be indicated for each system, chosen from the following: Operational (system is operating), Under development (the system is being designed, developed, or implemented), Undergoing a major modification (the system is undergoing a major conversion or transition. (If more than one status is selected, list the part of the system covered under each). If a system is under development or undergoing a major modification, methods shall be provided to assure upfront security requirements.
2.5.2 Vision	Detailed security objectives for the system shall be defined.
2.5.2.1 Business Case	The budget request shall include the security resources required for the system. The Investment Review Board shall ensure any investment request includes needed security requests.
	The business case shall document the resources required for adequately securing the system.
	Capacity demands and projections shall be taken into consideration in order to reduce the threat of system overloading and the subsequent inability to support user services.
	The following terms shall be considered for inclusion in a contract or statement of work: asset protection; target level of service and unacceptable levels of service; liability of the contracted parties; access control agreements; the rights to monitor user activity, revoke user access, and audit contractual responsibility; the reporting structure and reporting format; involvement with subcontractors; controls to be used against malicious software; and arrangements for reporting and investigating security incidents.
2.5.3 Definition	
2.5.3.1 Sensitivity Assessment	Every system shall perform sensitivity assessment of the system.
2.5.2.2 Security Requirements	Security requirements of the system must be identified and defined, and a determination of each security measure shall be implemented and tested.
2.5.4 Construction	
2.5.4.1 RFP Requirements	Requirements in the solicitation documents shall permit updating security controls as new threats/vulnerabilities and as new technologies are implemented.
2.5.4.2 Testing Procedures	Appropriate security controls with associated evaluation and test procedures shall be developed before the procurement action.
2.5.4.3 Security Requirements	Security requirements shall be identified during system design.
	The solicitation documents (RFPs) shall include security requirements and evaluation/test procedures.
	If this is a purchased commercial application or the application contains commercial, off-the-shelf components, security requirements shall be identified and included in the acquisition specifications.
	A description of any specifications that were used and whether they are being maintained must be included.

Section	Policy Statement
2.5.4.4 Risk	Every system shall perform an initial risk assessment to determine security requirements.
	A written agreement with program officials on the countermeasures employed and residual risk shall exist.
2.5.5 Deployment	
2.5.5.1 Certification and Accreditation	Every system shall request written authorization prior to operation either on an interim basis with planned corrective action or full authorization.
	The certification testing of security controls must be conducted and documented.
2.5.5.2 Configuration Management	Changes shall be controlled as programs progress through testing to final approval.
	The application shall undergo a technical evaluation to ensure that it meets applicable federal laws, regulations, policies, guidelines, and standards.
2.5.5.3 Security Awareness	Implementing and testing security measures, including security awareness training for all personnel with security and control responsibilities, shall be completed.
2.5.5.4 Post-acceptance Security Controls	If new security controls were added to the application or support system, additional acceptance tests of any new controls shall be performed, system documentation shall be updated, the security controls shall be tested, and the system shall be recertified.
2.5.5.5 Design Reviews and System Tests	Results of the design reviews and systems tests, when they were conducted, and who conducted them, should be fully documented, updated, and maintained in the organization records.
	Design reviews and systems tests shall be performed prior to placing the system into operation to assure it meets security specifications.
	If operational information is to be used during testing, a separate authorization is required each time the information is to be copied into the test application system. After testing is complete, all operational information shall be erased from the test application system.
2.5.6 Support	
2.5.6.1 Audits and Reviews	Security measurements inherent in the system shall be monitored through audit and periodic reviews. Audits and monitoring shall be described.
	It shall be determined whether the system is operating correctly from a technical standpoint, whether it meets users' information management needs from a business standpoint, and whether it is wee-managed from a resource utilization perspective.
2.5.6.2 Security Plan	The system security plan shall be developed, approved, and kept current.
2.5.6.3 Operational Assurance	Operational assurance shall be described.
2.5.6.4 Security Operations	Security operations and administration shall be described.
2.5.7 Retirement	
2.5.7.1 Information Disposal	Every system shall describe the methods of how information or media is purged, overwritten, degaussed, or destroyed and how media sanitization is destroyed.
2.5.7.2 Information Archival	Official electronic records shall be properly archived.
2.6 Certification and Accreditation	Prior to initial system operation, system/application shall be certified and accredited.
	In-place safeguards shall be operating as intended prior to authorizing a system for processing.
	A technical and/or security evaluation shall be completed prior to authorizing a system for processing.

Section	Policy Statement
	Every system shall meet all applicable federal laws, regulations, policies, guidelines, and standards.
	An IATO may be obtained for a period not to exceed 6 months when the following has been met: (1)A Full Risk Assessment (2)Security Plan (Draft) (3)Project Plan for Full Accreditation.
	All systems shall be recertified every 3 years or upon major modification.
	Refer to SFA's C&A program manual for guidance and procedures.
	Accreditation is recorded in a letter from the DAA to the business or system manager.
	If a system is post-IOC, and has not been certified and accredited, the sstem owner shall create a plan to obtain C&A.
2.7 Security Awareness and Training	Each SFA employee shall receive a copy of the rules of behavior, which forms the basis for security awareness and training.
2.7.1 Training	Computer Security Awareness training shall occur within 30 days of employment and must comply with the computer Security Act and NIST 800-16. (ED policy says it must occur within 6 months of employment within ED)
	Procedures shall be set in place to ensure that each employee receives adequate training to fulfill their security responsibilities. Employee training type and frequency should be documented and monitored.
2.7.2 Refresher Training	Mandatory annual refresher training shall ensure that personnel remain abreast of current issues and concerns.
2.7.3 Awareness	Methods shall be employed to make employees aware of system security.
	Awareness briefings shall meet the requirements of the Computer Security Act and NIST 800-16.
2.7.4 Contractor	SFA contractor employees shall receive the same level of security awareness and training as federal employees, and this training requirement shall be included, as appropriate, in all contracts.
	Computer Security Awareness training shall occur within 30 days of contract award.
2.8 System Interconnections	System Interconnections are not allowed unless expressly documented in an MOU/MOA/SLA.
	Written authorization shall detail the rules of behavior and controls that must be maintained by the interconnecting systems.
	Written management authorization shall be obtained prior to connecting with other systems and/or sharing sensitive data/information (OMB A-130), including a list of interconnected systems (including Internet).
	Every system shall document whether or not the application is processed at a facility outside of the organization's control.
	Outsourced contracts shall include: how legal requirements are met; physical and logical controls to be used to restrict and limit access to sensitive information to only authorized users; the expected availability of services to be maintained in the event of a disaster; levels of physical security for outsourced equipment; and the right to audit.

Section	Policy Statement
3.1 Personnel Security	Hiring, transfer, and termination procedures shall be established.
	Documented job descriptions that accurately reflect assigned duties and responsibilities and that segregated duties and sensitivity level shall be established.
	There shall be a documented process for requesting, establishing, issuing, and closing user accounts.
	A nondisclosure statement shall be required if individual needs access to privileged information.
	A submitted letter through contract representative shall be required for contractors to gain access to sensitive information.
	When appropriate, terms and conditions of employment shall state that security responsibilities extend outside of the workplace (for example telecommuting, etc.)
3.1.1 Position Sensitivity Level	Positions shall be reviewed for sensitivity level or, if already employed by SFA, a planned date for completion of position sensitivity analysis shall be stated.
3.1.2 Background Screening	Appropriate background screening for assigned positions shall be completed prior to granting access and reviewed periodically thereafter.
	Every system shall describe conditions for allowing system access prior to completion of background screening and compensating controls to mitigate associated risk.
3.1.3 Separation of Duties	Distinct and sensitive systems support functions shall be performed by different individuals to ensure that no individual has all necessary authority or information access which could result in fraudulent activity.
	Whenever possible, development, test and operational facilities shall be separated to facilitate segregation of duties and prevent unwanted alteration and modification of operational systems.
3.1.4 Least Privilege	Formal policies shall be described that define the authority that will be granted to each user or class of users. User access shall be restricted to data files, to processing capability, or to peripherals and type of access to the minimum necessary to perform job.
3.2 Physical and Environmental Protection	Adequate physical security controls shall be implemented that are commensurate with the risks of physical damage or access.
	Secure areas shall have a clearly defined security perimeter, with appropriate barriers and access controls.
3.2.1 Supporting Utility Security	Electric power distribution, heating plants, water, sewage, and other supporting utilities shall be periodically reviewed for risk of failure.
3.2.1.1 Air Conditioning	Heating and air conditioning systems shall be regularly maintained.
3.2.1.2 Water	Plumbing lines shall be known and shall not endanger system, and plumbing leaks shall be addressed.
3.2.1.3 Power	An uninterruptible power supply or backup generator shall be provided.
3.2.2 Fire Control	Fire suppression and prevention devices shall be installed and working.
	Fire ignition sources, such as failures of electronic devices or wiring, improper storage materials, and the possibility of arson, shall be reviewed periodically.
3.2.3 Facilities	Access to facilities shall be controlled through the use of guards, identification badges, or entry devices such as keycards.
3.2.3.1 Visitors	Visitors, contractors, and maintenance personnel shall be authenticated through the use of preplanned appointments and identification checks, and shall also be escorted when in restricted or sensitive areas.

Section	Policy Statement
	Access to sensitive information shall be restricted to authorized personnel only.
3.2.3.2 Access	Management and supervisors shall limit access to controlled areas based on valid need for access and shall also regularly review the list of persons with physical access to sensitive facilities.
	Emergency exit and re-entry procedures shall ensure that only authorized personnel are allowed to re-enter after fire drills, etc.
	Unused keys or other entry devices shall be secured.
	Physical accesses shall be monitored through audit trails and apparent security violations shall be investigated and remedial action shall be taken.
	Controlled areas shall be determined by a risk assessment.
	Access to telecommunications hardware or facilities shall be restricted and monitored.
3.2.3.3 Static Entry Codes	Access controls shall be addressed.
	Entry codes shall be changed periodically.
3.2.3.4 Suspicious Activities	Suspicious access activity shall be investigated and appropriate action shall be taken.
3.2.4 Data Intercept	Data shall be protected from interception. Physical access to data transmission lines shall be controlled and computer monitors shall be located to eliminate viewing by unauthorized persons.
3.2.5 Media Labeling and Logging	Deposits and withdrawals of tapes and other storage media from the library shall be authorized and logged.
	All media containing sensitive information shall display a sensitive information label.
3.3 Production, Input/Output Controls	
3.3.1 Electronic Media Sanitation	Every system shall establish procedures for sanitizing electronic media for reuse and storing or destroying damaged/spoiled media.
3.3.2 User Support	Every system shall provide help desk or other user support that offers advice.
3.3.3 Hardcopy Destruction	Every system shall establish procedures for shredding or destroying hardcopy media when it is no longer needed. These procedures shall include some form of logging the destruction or other form of audit trail.
	Controls shall be in place for transporting or mailing media or printed output.
3.3.4 Storage	Every system shall establish procedures and protection controls to ensure physical protection of media storage vault/library.
3.3.5 Labeling	External labeling shall include special handling instructions.
3.3.6 Access	Every system shall establish procedures to ensure that unauthorized individuals cannot read, copy, alter, or steal printed or electronic information, and that only authorized users pick up, receive, or deliver input and output information and media.
	Authorization shall be required for the removal of all media from the organization, and an audit trail shall be maintained to record all such removals.
3.3.7 Logging	Every system shall maintain operator logs for all systems, including such entries as system start and finish times, system errors encountered and the corrective actions taken, batches run, etc. All entries shall be annotated by time and the operators name.

Section	Policy Statement
3.4 Contingency Planning/Disaster Recovery Plan	Every system shall describe the procedures (contingency plan) that would be followed to ensure the application continues to be processed if the supporting IT systems were unavailable, and detailed plans shall be provided as an attachment.
3.4.1 General Plans	A comprehensive plan shall be developed, documented, and tested prior to authorizing a system for processing.
	The contingency plan shall be approved by key affected parties, in particular System Manager and the SSO, and distributed to all appropriate personnel.
	The plan shall be considered, at a minimum, sensitive, with access limited to a "need to know" basis, and shall be stored securely offsite.
	Every system shall assign responsibilities for recovery.
	Every system shall provide a copy of all DRPs and contingency plans to PO CSO.
	Contingency planning shall incorporate the results of the latest Risk Assessment in order to focus attention on events that have the highest likelihood of disrupting service.
	Contingency plans and Disaster Recovery plans shall include the conditions necessary for activating the plan, including who is to be involved in the decision before each plan is activated.
	Every system shall include resumption procedures for returning to normal business operations in the plans.
3.4.1.1 Contingency Plan	Every system shall establish processing priorities and approved by management.
	Every system shall identify the most critical and sensitive operations and their supporting computer resources.
	Every system shall test contingency plans to permit continuity of mission-critical functions in the event of a catastrophic event.
	Emergency procedures shall have required time-scales for recovery and restoration of specified services.
3.4.1.2 Disaster Recovery Plan	Every system shall document disaster recovery procedures.
	Every system shall structural collapse.
3.4.1.3 Backup Plan	Every system shall backup procedures, including frequency (daily, weekly, monthly) and scope (full backup, incremental backup, and differential backup).
	Every system shall determine a minimum level of backup information to ensure all essential business information and software can be recovered in case of media failure or a disaster. At least three generations/cycles of back-up information shall be retained for important applications.
	System personnel shall ensure appropriate backups are performed as directed by the business manager.
	Every system shall stored backup tapes in a secure, off-site location; daily incremental backups shall be stored on-site; critical data files shall be backed up nightly.
	System defaults shall be reset after being restored from a backup.
3.4.1.4 Emergency Plan	Every system shall document formal written emergency operating procedures.
3.4.2 Testing	Every system shall document contingency/disaster recovery plans for all supporting IT systems and networks and plans , periodically tested, readjusted, and briefed to DAA.
	Every system shall test contingency, disaster, and emergency plans biennially by system personnel.
	Following each test, every system shall reassess and update contingency/disaster recovery plans to ensure its continued effectivity.

Section	Policy Statement
3.4.2.1 Alternate Processing Site	The backup storage site and alternate site shall be geographically removed from the primary site and physically protected.
	If appropriate, every system shall use an alternate processing site with a contract or interagency agreement in place.
	Every system shall maintain the system/application documentation at an off-site location.
	Every system shall maintain detailed instructions for restoring operations.
3.5 Data Integrity	There shall not be unauthorized ability to enter maliciously, or accidentally alter, or destroy information.
3.5.1 Virus Detection and Elimination	Every system shall install virus detection and elimination software. Once installed, every system shall procedures for routinely updating virus signature files, automatic and/or manual virus scans (automatic scan on network log-in, automatic scan on client/server power on, automatic scan on disk), and screening non-text files.
	Every system shall establish procedures to verify information regarding malicious software, and ensure that incoming warnings are accurate and not a hoax, including verification using reliable internet sites, reputable journals, etc.
	All information obtained from the Internet shall be considered suspect until confirmed by another source.
3.5.2 Reconciliation	Every system shall establish procedures to reconcile data, including a description of the actions taken to resolve any discrepancies.
3.5.3 Verification	Every system shall use integrity verification programs by applications to look for evidence of data tampering, errors, and omissions. Techniques include consistency and reasonableness checks and validation during data entry and processing.
	Every system shall establish procedures for responding to validation errors.
	Every system shall incorporate validation checks that would detect corruption of correctly entered data by processing errors or deliberate acts. Additionally, every system shall validate output data to ensure the processing of correctly stored data is correct and appropriate.
3.5.4 Message Authentication	Every system shall use message authentication in the application to ensure that the sender of a message is known and that the message has not been altered during a transmission.
3.5.5 Performance Measurements	Every system shall use system performance monitoring to analyze system performance logs in real time to look for availability problems, including active attacks and system and network slowdowns and crashes.
3.5.6 Intrusion Detection	Every system shall include a description of intrusion detection tools installed on the system, where they are placed, the type of processes detected/reported, and the procedures for handling instructions.
	Every system shall conduct periodic reviews on the software and data content of critical systems. All unapproved files or unauthorized amendments shall be formally investigated.
	Every system shall routinely review Intrusion detection reports and suspected incidents shall be handled accordingly.
3.5.7 Penetration Testing	Every system shall perform penetration testing on the system and procedures every system shall establish procedures to ensure that they are conducted appropriately. Included in this section should be descriptions of the hardware and software, policies, standards, procedures, approvals related to automated information system security in the application/system on which it is processed, backup and contingency activities, and descriptions of user and operator procedures.

Section	Policy Statement
3.6 Documentation	Every system shall maintain a System Security Plan.
	Every system shall maintain a list of documentation maintained for the application.
	Every system shall maintain a written agreement regarding how data is shared between interconnected systems (memoranda of understanding with interfacing systems).
	Every system shall maintain application documentation, requirements, and specifications.
	Every system shall maintain software and hardware testing procedures and results.
	Every system shall maintain standard operating procedures that support all operations of the application or general support system.
	Every system shall maintain user manuals to explain how software/hardware is to be used.
	Every system shall maintain vendor-supplied vendor documentation of software and hardware.
	Every system shall maintain certification and accreditation documents and statements authorizing a system to process.
	Every system shall maintain a list of support contacts in case of unexpected difficulties or system errors.
3.7 Configuration Management	Every system shall include a description on the hardware and system software maintenance controls in place or planned.
3.7.1 General	It shall be the responsibility of the CCB to provide an assessment of the security impact of each change or modification against security requirements and accreditation conditions issued by DAA.
	It shall be the responsibility of the CCB that the security representative attends CCB.
	It shall be the responsibility of the SSO to recommend approval of changes based on system security.
	CCB shall be formed within each PO to process, evaluate, and recommend approval or disapproval of proposed system configuration changes.
3.7.2 Configuration Control Board	Every system shall describe Configuration management procedures for the system.
	A formal change control process shall be put in place for the system requiring that all changes to the application software are to be tested and approved before being put into production.
	Every system shall software change requests forms to document requests and related approvals.
	Version control that allows association of system components to the appropriate system version shall be considered.
	Every system shall consider procedures for ensuring that contingency plans and other associated documentation are updated to reflect system changes.
	Every system shall use software distribution implementation orders including effective date provided to all locations.
	All new and revised hardware and software shall be authorized, tested, approved, and documented before distribution and implementation.
3.7.2.1 Change Management	Every system shall describe change identification, approval, and documentation procedures.
	An impact analysis shall be conducted to determine the effect of proposed changes on existing security controls, including the required training needed for both technical and user communities to implement the control.
3.7.2.1.1 Documentation	All changes to application software shall be documented.

Section	Policy Statement
	Procedures for testing and/or approving system components (operating system, other system, utility, applications) shall be considered prior to promoting to production.
3.7.2.1.2 <i>Testing</i>	The type of test data to be used (live or made-up) shall be specified.
	Test results shall be documented.
	Detailed system specifications shall be prepared and reviewed by management.
3.7.2.1.3 <i>Approval</i>	Special procedures for performance of emergency repair and maintenance shall be considered.
3.7.2.1.4 <i>Emergency Changes</i>	Emergency change procedures and how the emergency fixes are handled/to be handled shall be documented and approved by management, either prior to the change or after the fact.
3.7.3 Procedures and Guidance	Every system shall describe restrictions/controls on those who perform maintenance and repair activities, both on-site and off-site (i.e., escort of maintenance personnel, sanitization of devices removed from the site, etc.).
3.7.3.1 Maintenance and Repair	All vendor-supplied default security parameters shall be reinitialized to more secure/most restrictive settings.
	Every system shall describe procedures used for controlling remote maintenance services where diagnostic procedures or maintenance is performed through telecommunications arrangements.
	Implementation of changes shall take place at such times and in such a way as to limit disturbing the business process involved.
3.7.3.2 Illegal Software	Whatever is not expressly allowed is denied.
	There shall be organizational policies for handling and protecting against illegal use of copyrighted software or shareware, and the use of copyrighted software, shareware, and personally owned software/equipment shall be documented.
	Periodic audits shall be conducted of users' computers to ensure that only legally licensed copies of software are installed.
	Procedures shall contain provisions for individual and management responsibilities and accountability, including penalties.
	If a copyrighted commercial off-the-shelf product/shareware is used, sufficient licensed copies of the software shall be purchased for all of the systems on which this application will be processed.
3.7.3.3 Application Licensing	Hardware/software warranties shall be managed to minimize the cost of upgrades and cost-reimbursements or replacement for deficiencies.
	It shall be stated whether the government owns the software, if the software was developed in-house or under contract, or if the application software was received from another federal agency with the understanding that it was federal government property.
3.8 Incident Response Capability	
3.8.1 General	Intrusions detection tools, automated audit logs, penetration testing, and other preventative measures shall be employed to provide help to users when a security incident occurs in the system.
3.8.2 Preventative Measures	Privately owned software or utilities shall not be used on Departmental computers without specific authorization.
	Media shall be free of all viruses before being used with Department's computers .
	Procedures shall be in place for recognizing, handling, and reporting incidents.

Section	Policy Statement
3.8.3 Incident Identification and Resolution	Incidents shall be monitored and tracked until resolved.
3.8.3.1 Incident Identification	<p>Security alerts and security incidents shall be analyzed and remedial actions shall be taken.</p> <p>Users are required to notify any observed or suspected security weaknesses in, or threats to, the organizations systems or services to management and/or system administrators as soon as possible. They should <u>not</u> attempt to prove a suspected weakness on their own.</p> <p>Software malfunctions shall be reported and handled.</p>
3.8.3.2 Post Incident	<p>Incident handling procedures and control techniques shall be modified after an incident occurs.</p> <p>Audit trails and other evidence shall be collected and secured for analysis and as potential evidence.</p> <p>Incidents shall be reported to FedCIRC, NIPC, and local law enforcement when necessary.</p>
3.8.4 Information Sharing	<p>Incident information and common vulnerabilities or threats shall be shared with interconnected systems.</p> <p>SFA Management shall assign specific individual(s) to receive and respond to alerts/advisories, vendor patches, exploited vulnerabilities, etc.</p>

Section	Policy Statement
4.1 Identification and Authentication	Each system user shall be uniquely identified and verified by the system before being granted access.
	Every system shall describe the passwords, tokens, biometrics, and other methods used to identify and authenticate.
	Every system shall describe how the application identifies access to the system.
	Security controls shall be able to detect unauthorized access attempts.
	Passwords shall be transmitted and stored with one-way encryption.
	Vendor-supplied/default passwords shall be replaced immediately.
	Passwords shall not be displayed when entered.
	Every system shall describe the number of invalid access attempts that may occur for a given user identifier or access location (terminal or port), and the actions taken when that limit is exceeded shall be included.
	Every system shall describe the self-protection techniques for user authentication mechanism.
	Log in procedures shall limit the amount of information about the system until after a successful log-in has occurred. This shall include: not displaying system or application identifiers until after a successful log-in; not providing help messages during the log-on procedure that would assist an unauthorized user; not validating any portion of the log-in information until all components have been completed, and not indicating which part of the log-in data was incorrect.
4.1.1 General Policy	Procedures shall be in place for handling lost and compromised passwords.
	Passwords shall be distributed securely and users shall be informed not to reveal their passwords to anyone (social engineering).
	User ID and password shall be changed in the event of employee transfer, termination, retirement, or suspicion that the password has been disclosed.
	Before access is granted, the following shall be checked: the user has authorization from the system owner to access the system; the level of access is appropriate for the user's business purpose; segregation of duties has not been compromised; the user has been provided a copy of the Rules of Behavior for the system and has signed a statement indicating that they understand and agree to the Rules.
	Any systems' privileges (any features allowing a user to override system or application control) shall be identified and associated with the categories of staff that would them. An authorization process and record of privileges that may be allocated shall be maintained, and the process shall be completed before any privileges are granted.
4.1.2 Identification Accountability	The system shall correlate actions to users via the creation of unique user IDs for each individual user. Group IDs shall be permitted only necessary.
	Privileges (any features allowing a user to override system or application control) shall be assigned to a different user ID than that used for normal business use.
	User IDs shall not give indication of the user's privilege level.
	Every system shall describe how the access control mechanisms support individual accountability and audit trails (e.g., passwords are associated with a user identifier that is assigned to a single individual).
	Guest accounts are not allowed on EDNet.
4.1.3 Host Based Identification	If host-based authentication is used, it shall be indicated. (This is an access control approach that grants access based on the identity of the host originating the request, instead of the individual user requesting access.)

Section	Policy Statement
4.1.4 Biometrics	Every system shall describe any biometrics and token controls that are used and how they are implemented on the system. (Indicate if special hardware readers are required, if users are required to use a unique PIN, who selects the pin, etc.)
4.1.5 Public Key Infrastructure	Every system shall describe how digital signatures or electronic signatures will be used. PKI technology shall conform with FIPS 186-1, Digital Signature Standard and FIPS 180-1, Secure Hash Standard issued by NIST, unless a waiver has been granted. If a waiver has been granted, the name and title of the official granting the waiver shall be included.
	Every system shall describe cryptographic key management procedures for key generation, distribution, storage, entry, use, destruction, and archiving.
4.1.6 Passwords	
4.1.6.1 Frequency of Change	Passwords shall be changed at least every ninety days or earlier if needed. Every system shall describe how password changes are enforced and who changes the passwords.
	If users will maintain their own password, it shall be ensured that they are provided with an initial secure password that they will be forced to change immediately.
	Temporary passwords (for use when a user forgets their password) shall only be given after first positively identifying the user. The temporary password shall only be given to users in a secure method, and shall require the user to change it immediately.
4.1.6.2 Format	Passwords shall be a minimum of six to eight characters in a combination of alpha, numeric, upper/lower case or special characters, and shall meet FIPS Publication 112 standards.
	Password policy shall be documented, including the specific information on allowable character set, password length (maximums and minimums), password aging time frames and enforcement approach, and number of generations of expired passwords disallowed for use.
4.1.6.2.1 Compliance	Procedures shall be put in place to determine compliance with password policies.
	Password crackers/checkers shall be used.
4.1.6.3 Scripts with Passwords	Every system shall describe the procedures for limiting access scripts with embedded passwords (e.g., scripts with embedded passwords are prohibited, scripts with embedded passwords are allowed only for batch applications).
4.1.7 Bypassing Controls	Every system shall describe policies that provide for bypassing user authentication requirements, single-sign-on technologies (e.g., host-to-host authentication servers, user-to-host identifier, and group user identifiers) and any compensating controls.
	Every system shall determine whether emergency or temporary access is authorized.
4.1.8 Access Control Lists	A current list of authorized users and their access shall be created, maintained, and approved. This access control list shall be encrypted and meet federal standards.
	It shall be indicated how often Access Control Lists are reviewed (at least every six months) to identify and remove users who have left the organization (inactive users), users whose duties no longer require access to the application, or redundant user IDs and accounts.
	Authorization for privileged access rights shall be reviewed at least every three months to check if privileges should still be provided, and that no unauthorized privileges have been obtained.
	Access to network services shall be controlled to the granularity of an individual user.
4.2 Logical Access Controls	Logical access controls are the system-based mechanisms used to specify who or what is to have access to a specific system resource and the type of access that is permitted.

Section	Policy Statement
4.2.1 General	Every system shall describe the controls in place to authorize or restrict the activities of users and system personnel within the application.
	Every system shall describe hardware or software features that are designed to permit only authorized access to or within the application.
	Trust relationships among hosts and external entities shall be appropriately restricted.
	Access controls shall reside at the network, operating system, and application level to restrict users to the level of information to which they are authorized to gain access.
4.2.2 Application	Every system shall indicate if the security software allows application owners to restrict the access rights of other application users, the general support system administrator, or operators to the application programs, data, or files.
	Access to all program libraries, system software, and system hardware shall be restricted and controlled.
	Privileges (any features allowing a user to override system or application control) shall be allocated to individuals on a need-to-use or event-by-event basis, i.e. per the minimum required for their job and only when needed.
	Every system shall describe controls to detect unauthorized transaction attempts by authorized and/or unauthorized users.
	Logical access controls shall restrict users to authorized transactions and functions.
	Every system shall describe restrictions to prevent users from accessing the system or applications outside of normal work hours or on weekends.
	Access to security software shall be restricted to security administrators.
	Inactive terminals in high-risk locations shall shut down after a defined period of inactivity, closing all applications, clearing the terminal screen, and closing the network session.
4.2.3 Files	Internal security labels shall be used to control access to specific information types or files, and shall specify protective measures. Additional handling instructions shall be indicated.
	Access shall be restricted to files at the logical view or field.
	Files shall not be downloaded to a network or shared drive.
4.2.4 Delegate Permission	Every system shall describe policy or logical access controls that regulate how users may delegate access permissions or make copies of files or information accessible to other users.
	Only the object owner shall grant access to an individual user or specified user group.
4.2.5 Desktop	Users shall disable Java.
	Terminals shall automatically log off and screensavers shall lock the system after a period of inactivity.
	Network connections shall automatically disconnect at the end of a session.
4.2.6 Firewall and Proxy	If the public accesses the system, controls shall be in place and implemented to protect the integrity of the application and the confidence of the public.
	Every system shall describe any type of secure gateway or firewall in use, including its configuration (e.g., configured to restrict access to critical system resources and to disallow certain types of traffic to pass through to the system).
	Insecure protocols (UDP, ftp, etc) shall be disabled.
	Internet services leaving or entering a departmental IT system will be controlled via firewall or proxy devices.
	Information shall be provided regarding any port protection devices used to require specific access authorization to the communication ports, including the configuration of the port protection devices, and if additional passwords or tokens are required.

Section	Policy Statement
4.2.7 Encryption	Every system shall describe cryptography, specifically digital signatures and encryption.
	All sensitive information shall be encrypted before being sent over the Internet. Unencrypted Departmental material cannot be posted to a publicly accessible Internet site without prior approval.
	Every system shall describe procedures for key generation, distribution, storage, use, destruction, and archiving, and encryption shall meet federal standards.
	In addition to securely managing secret and private keys, public keys shall be protected to prevent forging a digital signature by replacing the public key. Public keys shall be protected using public key certificates. There shall be procedures detailing how the certificates are generated and controlled.
4.2.8 Network	Every system shall describe whether encryption is used to prevent unauthorized access to sensitive files as part of the system or application access control procedures. If encryption is used primarily for authentication, include this information in that section.
	There shall be logical controls for telecommunication access.
	All unused network services shall be deactivated.
	IP addresses shall not be published.
	Every system shall describe network diagrams and documentation on setups of routers and switches.
	Communication software shall be implemented to restrict access through specific terminals.
	Devices that provide access mediation services shall include facilities to enforce access control.
	Authorization procedures shall determine which network and network services are allowed to be accessed, and who gets to access them.
	It shall be determined whether networks should use enforced paths to restrict routes used between user terminals and the computer services that the user is authorized to use.
4.2.9 System Interconnection	Security controls of the system and interconnected systems shall be reviewed.
	A list of interconnected systems (including Internet), their names/unique identifiers, and a description of the interaction(s) among systems shall be included.
	Every system shall describe the sensitivity level of each system.
	Every system shall describe the System of Record, if applicable.
	Every system shall describe the name and title of authorizing management officials and the date of authorization.
	Every system shall discuss security concerns and considerations, and the Rules of Behavior of the other systems that need to be considered in the protection of the system, including organizations owning the other systems.
	Every system shall determine whether the software resides on an open network used by the general public or with overseas access.
	If the application is running on a system that is connected to the Internet or other WANs, additional hardware or technical controls shall be installed and implemented to provide protection against unauthorized system penetration.
4.2.10 Fraud Waste and Abuse	The use of government equipment and software utilities for anything other than government-approved purposes is prohibited.
4.2.11 Web Policy	The CIO is responsible for maintenance and security of all Web servers.
	The SSO is responsible for all servers and services security for each Web server.
	Web servers shall be hosted behind a firewall and Web services shall have appropriate access control.
	Web services shall be accredited, including penetration testing. Refer to C&A.

Section	Policy Statement
	Disaster recovery plans and contingency plans shall be developed for each website. Refer to Contingency Plan.
	Measures shall be in place to detect unauthorized access to Web servers and services.
	All users shall be authenticated at the firewall when they connect to Department internal computers via the Internet.
	Each Web page shall have a designated author or maintainer.
	All publicly writeable directories will be reviewed and cleared each evening.
4.2.11.1 Web Site Privacy Policy	Each publicly accessible Web site shall provide a privacy and security notice to users upon initial access.
	Information protected by the Privacy Act shall not be posted on publicly accessible Web servers.
4.2.12 Warning Banners	A DOJ approved standardized log-on banners shall be placed on the system to warn unauthorized users that they have accessed a U.S. government system and can be punished.
	All department networks shall display a warning notice before user login to include: Authorized Use Only warning, Consent to Monitoring notice, not identify the type of computers, network, or operating system.
4.2.13 Remote Access	Dial-in access shall be monitored.
	Approval by the DCS is required for dial-in security.
	Controls shall be put in place to allow users to access the system remotely. Remote access via dial-in modem will be an auditable event.
	Additional security beyond user ID and password shall be incorporated into the dial-up policy.
	Remote access to diagnostic ports shall be securely controlled.
4.3 Audit Trails	
4.3.1 Review	Audit trails shall be reviewed frequently and according to strict guidelines.
	Audit trails shall be used as online tools to help identify problems other than intrusions as they occur.
	Access to online audit logs shall be strictly controlled. Controls shall be in place to protect against unauthorized changes and operational problems.
	Automated tools shall be used to review audit records in real time or near real time.
	Appropriate system-level or application-level administrator shall review the audit trails following a known system or application software problem, a known violation of existing requirements by a user, or some unexplained system or user problem.
	The organization shall use the many types of tools that have been developed to help reduce the amount of information contained in audit records, as well as to distill useful information from the raw data.
4.3.2 Content	All activity involving access to and modification of sensitive or critical files shall be logged.
	Audit trails shall provide accountability by providing a trace of user actions.
	Audit trails shall support after-the-fact investigations of how, when, and why normal operations ceased.
	Audit trail shall have capability of being queried by user ID, terminal ID, application name, date and time, or some other set of parameters to run reports of selected information.
	Audit trails shall include sufficient information to establish what events occurred and who (or what) caused them. In general, an event record shall specify: Type of event; When the event occurred; User ID associated with the event; and Program or command used to initiate the event.
	Audit trails shall provide record of the number of successful and rejected system access attempts, data access attempts, and other resource access attempts.

Section	Policy Statement
	Audit trails shall be designed and implemented to record appropriate information that can assist in intrusion detection.
	Audit trail clocks shall be kept synchronized to an agreed upon standard to avoid discrediting the validity of the logs during an investigation. Procedures shall be in place to check and correct any deviations in the time.
4.3.3 Access Control	The confidentiality of audit trail information shall be protected if, for example, it records personal information about users.
	If off-line storage of audit logs are retained for a period of time, access to audit logs shall be strictly controlled.
4.3.4 Keystroke Monitoring	Keystroke monitoring shall be used and users shall be notified.
	Whenever keystroke monitoring is used, reference to the policy and the means of notification shall be provided. Also indication of whether the DOJ has reviewed the policy shall also be provided
4.3.5 Separation of Duties	There shall be a separation of duties between security personnel who administer the access control function and those who administer the audit trail.