

Information Technology Management, Security and Use Policy

Revision 2.2

January 24, 2013

**Document Configuration Control**

|  |  |  |
| --- | --- | --- |
| **Version** | **Release Date** | **Summary of Changes** |
| Version 1.0 | Sept 10, 2005 | Draft Versions based on versions of U.S. ED Handbooks |
| Version 2.0 | Jan 5, 2006 | Updated document with changes from reviews from within SEDL. |
| Version 2.1 | May 26, 2011 | Revisions, clarifications and adaptations to current systems. |
| Version 2.2 | January 24, 2013 | Revisions, clarifications, and updates based on internal reviews |
| Version 2.3 |  |  |
|  |  |  |

**Table Of Contents**

**1. INTRODUCTION**

1.1 PURPOSE ............................................................................................................ 5

1.2 SCOPE ................................................................................................................ 5

1.3 SEDL SECURITY FUNDAMENTALS..................................................................... 5

1.4 COMPLIANCE ..................................................................................................... 6

1.5 EXCEPTIONS....................................................................................................... 6

1.6 APPLICABILITY .................................................................................................. 6

1.7 POLICY DOCUMENT ADMINISTRATION .............................................................. 7

1.8 REFERENCES ...................................................................................................... 7

1.9 SECURITY AND PRIVACY ORGANIZATION .......................................................... 8

1.10 ROLES AND RESPONSIBILITIES ........................................................................... 8

1.11 DOCUMENT STRUCTURE .................................................................................... 8

**2 ENTERPRISE MANAGEMENT CONTROLS ......................................... 9**

2.1 RISK MANAGEMENT ........................................................................................ 9

2.2 SECURITY CONTROL REVIEWS ......................................................................... 9

2.3 SYSTEM SECURITY PLAN ............................................................................... 10

2.4 RULES OF BEHAVIOR ..................................................................................... 11

2.5 SOLUTION LIFE CYCLE................................................................................... 11

2.6 CERTIFICATION AND ACCREDITATION ........................................................... 12

2.7 SECURITY AND PRIVACY AWARENESS AND TRAINING ................................... 12

2.8 SYSTEM INTERCONNECTIONS ......................................................................... 12

**3 OPERATIONAL CONTROLS ................................................................ 13**

3.1 PERSONNEL SECURITY .................................................................................. 13

*3.1.1 Establishing and Terminating Accounts .......................................... 13*

*3.1.2 Position Descriptions...................................................................... 14*

*3.1.3 Sensitivity/Risk Levels ..................................................................... 14*

*3.1.4 Background Screening .................................................................... 14*

*3.1.5 Use of External Connections .......................................................... 14*

*3.1.6 Nondisclosure and Confidentiality Agreements.............................. 14*

*3.1.7 Segregation of Duties...................................................................... 14*

*3.1.8 Compliance ..................................................................................... 15*

3.2 PHYSICAL AND ENVIRONMENTAL PROTECTION ........................................... 15

*3.2.1 Physical Access Controls ............................................................... 15*

*3.2.2 Environmental Controls................................................................. 16*

3.3 PRODUCTION INPUT/OUTPUT CONTROLS ..................................................... 16

3.4 CONTINGENCY PLANNING............................................................................ 16

*3.4.1 Plan Maintenance .......................................................................... 17*

*3.4.2 Alternate Site Capability................................................................ 17*

*3.4.3 System Backup ............................................................................... 17*

3.5 DATA INTEGRITY ........................................................................................ 18

*3.5.1 Virus Detection and Elimination ................................................... 18*

*3.5.2 Verification .................................................................................... 18*

*3.5.3 Reconciliation ................................................................................ 18*

*3.5.4 Message Authentication ................................................................. 18*

*3.5.5 Performance Measurements.......................................................... 18*

*3.5.6 Intrusion Detection ....................................................................... 18*

*3.5.7 Penetration Testing ....................................................................... 19*

3.6 DOCUMENTATION ...................................................................................... 19

3.7 CONFIGURATION MANAGEMENT................................................................ 20

*3.7.1 Configuration Control ..................................................................20*

*3.7.2 Configuration and Management Documentation .........................21*

3.8 INCIDENT RESPONSE ...................................................................................22

*3.8.1 Information Sharing......................................................................22*

*3.8.2 Incident Identification ...................................................................22*

*3.8.3 Post Incident Activities .................................................................22*

**4 TECHNICAL CONTROLS ....................................................................23**

4.1 IDENTIFICATION AND AUTHENTICATION ..................................................... 23

*4.1.1 System Login ................................................................................. 23*

*4.1.2 Passwords ..................................................................................... 24*

*4.1.3 PKI and Biometrics....................................................................... 25*

4.2 LOGICAL ACCESS CONTROLS (AUTHORIZATION/ACCESS CONTROLS) ........ 25

*4.2.1 Access Control List ................................................................................... 26*

*4.2.2 Internet or Public Access .......................................................................... 26*

*4.2.3 Remote Access........................................................................................... 27*

4.3 AUDIT TRAILS............................................................................................. 27

4.4 SOFTWARE.................................................................................................. 28

**5 Roles/Designees ....................................................................................... 28**

**APPENDIX A: TERMS OF USE...................................................................... 29**

**1 INTRODUCTION**

**1.1 Purpose**

The purpose of this document is to describe SEDL's Information Technology Management, Security, and Use policies. These policies reflect SEDL management’s decisions, intentions, definitions, and rules on information security and protection of proprietary and private information. These policies are the first line of protection for SEDL systems as they set forth the minimum level of security required at SEDL and establish the criteria against which SEDL will measure its success in maintaining such security.

SEDL staff are encouraged to use SEDL's telecommunications resources (i.e., telephonic, computing, electronic networking, and related peripheral equipment) to the maximum extent possible in performing their duties to efficiently and productively meet SEDL's mission. All staff have the responsibility to use these resources in a professional, ethical, and lawful manner as described in this document. These resources, and all that is contained within them, belong to SEDL, and they should be used primarily for authorized business purposes. A small, reasonable amount of personal use of these resources is allowed, provided that use complies with these policies.

**1.2 Scope**

SEDL's Information Technology Management, Security, and Use policies provide the foundation for various detailed information security and privacy guidelines, standards, processes and procedures.

SEDL information security and privacy is comprised of organizational, technical and management measures necessary to safeguard information assets (especially personal and proprietary information) against unauthorized access, disclosure, duplication, denial of use, modification, diversion, destruction, loss, theft, or misuse –whether malicious or accidental. Information security and privacy jurisdiction covers all information assets beginning with the electronic or manual input of data and ending when the data are transferred to non-SEDL systems, persons or facilities.

These policies address security and privacy requirements exclusively for SEDL assets, personnel, facilities, and contracted resources. Separate Department of Education resources and facilities (including EDNET and its components, the voice and data communication circuits managed by the Department, and document storage and handling by Department components separate from SEDL) are addressed by the Department of Education’s Information Technology Security Policy, and are outside the scope of SEDL Information Security and Privacy policies.

**1.3 SEDL Security Fundamentals**

SEDL systems must protect the confidentiality, integrity and availability of all information assets. The following high-level fundamentals provide the basis for all information security activities. These principles are simple, broad statements that form a "Constitution" for information security that are tailored to the needs of SEDL:

**Individual Accountability**

Each individual is responsible for his or her actions in safeguarding SEDL information assets.

**Need-to-Know and Need-to-Do (Least Privilege)**

Each individual is authorized access to only those SEDL information assets required to perform his or her job.

**Separation of Duties and Functions**

Operation/Production- No single individual may have exclusive control over a particular SEDL information asset or process.

Development- To ensure stability of SEDL computing environment, there should be a separation of duties among development, testing and production tasks.

Dividing critical functions among different individuals ensures that no individual has all necessary authority or information access, which could result in fraudulent activity.

**Principle of Proportionality**

Information security and privacy measures will be implemented in reasonable proportion to the identified risks they are designed to protect against and the business value of the assets they protect.

**Security and Privacy by Design**

SEDL security is developed as part of a Solution Life Cycle process. From the initial concept to retirement, SEDL integrates security controls into its systems and applications. All security solutions must integrate into an overall strategic security architecture.

All SEDL policies, guidelines, and standards and practices must be consistent with these principles.

**1.4 Compliance**

Compliance with Information Security Policies is mandatory. If an individual (a SEDL employee or contractor) violates the provisions in this policy, either by negligence or intent, SEDL may take appropriate disciplinary action in accordance with organizational or departmental standards of conduct, contract provisions, or SEDL’s disciplinary or termination policies. Any violations of this policy that may also constitute criminal offenses will be reported to law enforcement authorities as appropriate.

**1.5 Exceptions**

Any portion of this policy is subject to waiver, based on a decision by SEDL's Chief Executive Officer (CEO) that, either:

* Other controls (technical or procedural) limit the risk substantially enough to make the additional control required by this policy needless;
* The risk the policy aims to minimize is already substantially remote; or
* The cost of implementing the policy is not commensurate with the protection offered by the policy.

Each such waiver must be approved in writing by the CEO and countersigned by SEDL's Chief Information Officer.

**1.6 Applicability**

This policy applies to all SEDL operations. SEDL employees, consultants, contractors, interns, temporary employees, or other parties accessing SEDL information assets are subject to this policy and have the same responsibilities as SEDL employees.

Partner organizations, such as schools, lenders, guarantors and servicers, and their employees have parallel responsibilities for security and privacy set forth in various program participation agreements and contracts or regulator guidelines.

**1.7 Policy Document Administration**

The SEDL Information Technology Team will review Information Security Policies as often as necessary but no less than annually. Additional policies may be issued as the need arises, and will be incorporated into the Information Technology Management, Security, and Use Policy document.

**1.8 References**

This document is based on standards contained in the following documents. Its goal is to meet or exceed the minimum requirements for overall regulatory compliance and in doing so also meets the federal and state guidelines of the organizations for which SEDL works, or seeks to work:

NIST 800-18, Guide for Developing Security Plans for Information Technology Systems

NIST Special Publication 800-26, Self-Assessment Guide for Information Technology Systems[[1]](#footnote-1)

International Standard – Information Technology – Code of Practice for Information Security Management 17799:2000

U.S. Dept of Education Information Technology Security Policy

The Privacy Act of 1974

The Federal Information Security Management Act (FISMA)

Handbook OIG-1, Handbook for Personnel Security-Suitability Program

U.S. Dept of Education Information Technology Contingency Planning Guide

U.S. Dept of Education Risk Assessment Handbook

These documents provide a comprehensive set of baseline policies comprising federal and international best practices in information security and privacy.

SEDL information security and privacy strategies are long-term directions that serve as the basis for adequate planning and security solutions to meet SEDL business needs now and in the future.

SEDL information security is multi-dimensional. To be effective, information security requires constant review of the following strategies:

* Information security tools, methods, and practices will not rely on secrecy or obscurity to be effective.
* Information security decisions will be based on risk analyses and assessment methods that include – to the extent possible – metrics that capture the short and long-term business value of alternatives.
* Information security will include periodic reviews of the business value of security measures already in place.

**1.9 Security and Privacy Organization**

All those who use SEDL information assets are implicitly part of the SEDL security and privacy organization. This resulting virtual organization must make sure security policies are in place and managed accordingly. Effective management of SEDL information requires that everyone who has access to SEDL information assets:

* Understands security roles and responsibilities.
* Manages risks so appropriate measures can be taken to protect the confidentiality, integrity and availability of SEDL information assets.
* Participates in awareness programs to make sure security policies are communicated and understood.
* Reports security incidents, violations, and known vulnerabilities to management and to SEDL’s Information Technology Team.
* Makes sure that the outsourcing of information services to a third-party service provider does not introduce degradation of information security beyond that accepted as a business risk.

**1.10 Roles and Responsibilities**

SEDL assigns security and privacy responsibilities to numerous individuals, with ultimate responsibility for these matters assigned to the Chief Executive Officer (CEO).

Security responsibility may be delegated or reassigned to another position. SEDL’s primary objective is to make sure an identified individual or group performs all security functions. The CEO delegates much of his/her operational security responsibilities to the Program Managers. A Program Manager has budgetary and operational control of the systems within his/her program unit. Program Managers rely upon the Chief Information Officer (CIO) to oversee and manage the security of individual systems. The CIO appoints, in writing, a System Security Officer (SSO) to manage the administrative details of system security, including the system’s documentation, personnel clearances, and interaction with contractor support security professionals.

The CIO, in addition to managing several SEDL systems, writes Information Security Policies, standards, and guidelines, provides security awareness and training to SEDL employees and contractors, and responds to security matters presented by SEDL personnel. The CIO delegates much of this responsibility to the System Security Officer (SSO). The SSO manages the SEDL security and privacy program and actively supports the program units in the development and maintenance of systems worthy of trust.

**1.11 Document Structure**

In addition to this Introduction, this policy document is divided into three sections:

2.0 Enterprise Management Controls,

3.0 System Operational Controls, and

4.0 System Technical Controls.

This document’s format follows the outline of NIST Special Publication 800-18, Guide for Developing Security Plans for Information Systems. Formatting the policy in this way is intended to aid policy implementation in SEDL System Security Plans.

**2 ENTERPRISE MANAGEMENT CONTROLS**

The Enterprise Management Controls section outlines security topics that are normally addressed by management in the organization's information security program. In general, these controls focus on the management of the information security program and the management of risk within the organization. The types of control measures are consistent with the need for protecting the general support system, major application or application.

Program Managers are responsible for implementing risk-based, cost effective security controls. Procedures based on these policies provide security protection for information collected or maintained on the information systems for which they are responsible.

**2.1 Risk Management**

The information processed by each SEDL system must be analyzed to determine its level of sensitivity. The analysis will consider how critical the system is to SEDL’s business processes and the impact to critical SEDL functions if the confidentiality, integrity

and/or availability of the system and the data it contains were compromised.

The sensitivity analysis must contain both a general description of sensitivity and a list of applicable laws, regulations, and policies that establish specific requirements for confidentiality, integrity, and availability of data/information in the system. It should

also indicate if the information’s sensitivity level is high, medium, or low for each of the three categories. If the system processes information subject to the Privacy Act, the SSO must document the number and title of the Privacy Act system of records in the system’s security plan and whether the systems are used for computer matching activities.

SEDL systems practice information security throughout their entire life cycle. Each SEDL Program Manager must budget for and oversee the completion of risk assessments for all Information Technology (IT) systems under his/her control. These assessments must be updated every three years at a minimum by an independent evaluator, or whenever a major change[[2]](#footnote-2) to the system occurs. Each assessment must include the name of the assessor and the date the assessment was completed. In partnership with the Systems Security Officer, the Program Manager must:

* Supervise an assessment of the risk to each IT system for which he/she is responsible that considers internal and external threats to the confidentiality, integrity and availability of the system and to data supporting SEDL’s business operations.
* Determine the effectiveness of any countermeasures or risk mitigations for the system(s) being assessed and whether they are adequate.
* Supervise a mission/business impact analysis to determine potential effects of unmitigated risks on the mission or business process the IT system supports, to include an estimated degree of harm or loss that could occur if corrective actions are not taken.
* On the basis of the impact analysis, recommend corrective or mitigating actions to bring the system risk to a level the System Owner is willing to accept.
* Propose an implementation schedule and milestones with cost estimates for mitigating unacceptable risks.
* Monitor updates of a system’s security plan with new procedures.
* Maintain a list of known system vulnerabilities, system flaws, or weaknesses that could be exploited by the threat source, including those accepted as risk-based decisions.

The SSO must maintain on file the risk assessment reports and related management approvals.

**2.2 Security Control Reviews**

The Chief Information Officer is responsible for periodic management testing and evaluation of the effectiveness of security control policies, procedures and techniques, and for remediation of any noted deficiencies found during these tests. Security controls of the SEDL system and any connected system must be consistent with, and an integral part of, the SEDL IT architecture.

Every SEDL system must also undergo tests and examinations, (i.e. network scans, penetration testing) of key controls on a routine basis. If significant weaknesses are found, SEDL must take remedial or corrective actions and report them to SEDL management.

The System Security Officer must conduct an annual routine self-assessment, in NIST 800-26 format. Additionally, another independent evaluator should conduct an independent review. The findings from these reviews will be reported to OMB as required by the Federal Information Security Management Act (FISMA) if performed as a result of a project or contract which stipulates it. SEDL takes all system reviews seriously and dedicates adequate resources to appropriately address any deficiencies reported in the review. Similar to the requirement in risk management, the System Security Officer must aggressively implement appropriate actions to mitigate any findings in order to bring the system risk to a level the Designated Approval Authority is willing to accept.

**2.3 System Security Plan**

SEDL must have an approved system security plan. The plan will be written in the format and containing the topics prescribed in NIST Special Publication 800-18 for completeness. The system security plan must describe the system and its relationship with all interconnected systems. The system security plan must contain synopses of supporting documents (i.e. Disaster Recover Plan, Configuration Management Plan, etc,) and, although not required, may contain these supporting documents as appendices. The SSO must review and update the security plan at least annually to reflect current conditions and risks. Security plans must be dated to ease tracking of modifications and approvals, and a summary of the plan must be incorporated into the strategic IT Blueprint of SEDL. A proper system security plan is necessary in order for a system to pass the certification process if one is required for a federal or state contract.

**2.4 Rules of Behavior**

SEDL has a written Rules of Behavior for each SEDL system. These Rules of Behavior reflect administrative as well as technical security controls. They also delineate responsibilities, detail the expected behavior of all individuals with access to the system and define penalties for violation. The Rules of Behavior are published on SEDL's Intranet and are signed by every developer, maintainer, and user of the system, including non-SEDL users.. These rules describes the use of, and access to, SEDL systems and set appropriate limits on any interconnected equipment that permits access to them. The Rules of Behavior contain procedures for friendly and unfriendly termination of employment.

SEDL Rules of Behavior differentiate between actions that are forbidden unless expressly authorized versus what is permitted unless expressly forbidden.

The Rules of Behavior must include, but are not limited to, such actions as:

* Work at home,
* Protection of Privacy Act information,
* Reporting violations,
* Dial-in access, RDP, VPN
* Consent to monitoring,
* Connection to the Internet,
* Use of copyrighted works,
* Limitations on the unofficial use of equipment,
* The assignment and limitation of system privileges,
* Individual accountability, and
* Consequences for violating the rules of behavior.

Appendix A contains a copy of SEDL's Rules of Behavior. Every SEDL staff member must sign these Rules of Behavior and provide the signed copy to SEDL's System Security Officer. All non-SEDL staff must agree to these rules of behavior prior to gaining access to SEDL's guest network.

**2.5 Solution Life Cycle**

Every component of SEDL's system must follow the SEDL System Security Process Guide maintained by the System Security Officer. The System Security Process Guide is divided into six phases:

1. Vision

2. Definition

3. Construction

4. Deployment

5. Support

6. Retirement

Each phase of the lifecycle contains a corresponding security requirements checklist to be completed at the conclusion of each phase by the System Security Officer (SSO). No system may proceed to the next lifecycle phase until the security checklist is complete

and signed by the SSO and Program Manager.

**2.6 Certification and Accreditation**

SEDL General Support Systems (GSS) and Major Applications (MAs) must perform the Certification and Accreditation (C&A) process before becoming operational. GSSs and applications are categorized into one of five certification tiers. The level of documentation and testing necessary for the C&A process depends on the certification tier category determined for each GSS or application.

The C&A process is divided into four phases, with a series of requirements within each phase. The phases are designed to be performed concurrently with the SEDL System Security Process Guide. SEDL systems attempt to comply with the Department of Education Certification and Accreditation Guidelines for a measure of comparison as they often will mirror the requirements required by other agencies with which SEDL works.

**2.7 Security and Privacy Awareness and Training**

All SEDL employees are responsible for the confidentiality, integrity and availability of SEDL information systems. The Chief Information Officer must monitor and document the training of information security personnel who support SEDL systems to make sure they continually receive the necessary training to achieve the system's security and privacy objectives.

In addition, every SEDL employee should receive annual information security awareness training that is adequate to fulfill his or her security responsibilities. Program Managers must monitor employee training, both type and frequency.

**2.8 System Interconnections**

SEDL must conduct a security control review of every system and interconnected systems on a periodic basis. The Chief Information Officer must authorize all Memoranda of Understanding (MOU) or Trading Partner Agreements between SEDL systems and any interconnected systems. The MOUs and Trading Partner Agreements go into further granularity regarding requirements for interconnections. Every system must have a network diagram and documentation of any interconnected systems including access to the Internet, its names/unique identifiers, and a description of the interaction(s) between or among them included within the System’s Security Plan.

When obtaining system support or development services, SEDL’s contract agreements must include, but are not limited to:

* How legal security and privacy 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 natural disaster or other interruption of normal processing; and
* Levels of physical security for outsourced equipment;
* SEDL’s right to audit systems as required;
* Security screening of contractor personnel and security training requirements for contractor personnel; and
* Language requiring a contractor to inform the SEDL Chief Information Officer and SSO when contract personnel depart from the contract.

**3 OPERATIONAL CONTROLS**

The System Operational Controls section addresses security controls that are 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 rely on management activities as well as technical controls.

**3.1 Personnel Security**

SEDL information security depends heavily on individuals, and the controls placed on the individual. Each user must adhere to standards of conduct that protect the confidentiality, integrity and availability of information networks and the data they contain, transmit or process.

The CIO and SSO are responsible for implementing and validating reasonable and prudent personnel security controls to protect the confidentiality and integrity of the data and/or information maintained by SEDL, and to protect the availability of the networks that maintain, process or transmit that data and/or information. These controls are intended to assure the trustworthiness of all individuals who are allowed to access SEDL networks. This process has several vital components, which include:

* Requesting, establishing, issuing, and closing user accounts,
* Documenting duties in a job position description,
* Determining the sensitivity/risk level of each position,
* Establishing background screening commensurate with access level sensitivity and Departmental requirements,
* Use of external connections or transportable computers,
* Use of confidentiality agreements,
* Segregation of duties, and
* Assuring compliance with the process.

**3.1.1 Establishing and Terminating Accounts**

The SSO must use a documented process for requesting, establishing, issuing, and closing all user accounts. This process must include linkages to the human resource and contracting functions involved in new hires, transfers, contract award, oversight, and termination of employment. All user accounts must be regularly reviewed and kept current.

The SSO must identify any system privileges or features, which would allow a user to override system or application controls, and associate these privileges with the categories of staff that would use them. The SSO must maintain an authorization process and record of privileges. The SSO must review authorization for privileged access rights at least quarterly to see if privileged access is still required, and to make sure users have not been erroneously assigned unauthorized privileges.

**3.1.2 Position Descriptions**

Program Managers must establish job descriptions that accurately document assigned duties and responsibilities. The SSO must use these job descriptions when designating the sensitivity levels of these positions.

**3.1.3 Sensitivity/Risk Levels**

Program Managers must classify the sensitivity of each position. When determining a position’s sensitivity, consideration must be given to the laws, regulations, and policies that establish specific requirements for the protection of data and information an individual may affect (e.g. the Privacy Act and the Financial Services Modernization Act, referred to as the Gramm-Leach-Bliley Act).

**3.1.4 Background Screening**

Each SEDL employee or contractor should undergo an appropriate background screening for his or her assigned positions prior to obtaining access to SEDL systems. The amount of screening directly relates to the sensitivity level of the particular job position (SEDL references the Handbook OIG-1 for examples of implementation procedures). Additionally, if an employee or contractor’s position changes, SEDL must update the background screening commensurate with the position.

Every system must have documentation that describes the conditions for access to that system, especially when it is necessary to grant access prior to the completion of a background screening. The documentation also must state the compensating controls (e.g. accompanying an individual in a sensitive area) that will be used to mitigate associated risk.

**3.1.5 Use of External Connections**

When appropriate, terms and conditions of employment must state that security responsibilities extend outside of the workplace (e.g. telecommuting, travel, etc). SEDL Program Managers must approve all external connections in advance, and comply with SEDL security standards. Individuals in possession of portable computers or storage media containing sensitive SEDL information must not leave such equipment unattended at any time unless the information has been properly safeguarded. Such individuals take full responsibility and accountability for the equipment and the data it contains. SEDL’s policies on transportable computing devices govern the use of laptops, two-way messaging devices, pagers, etc.

**3.1.6 Nondisclosure and Confidentiality Agreements**

All SEDL employees and contractors that access sensitive information must sign a nondisclosure and/or confidentiality agreement covering the privileged/sensitive data or information with which they will come in contact by accessing SEDL networks. Statutes, regulations and internal SEDL policy define the data or information to be covered under such agreements. The annual Information Security Awareness Briefing must reemphasize the nondisclosure and confidentiality agreements.

**3.1.7 Segregation of Duties**

The CEO must create formal procedures defining the authority granted to each user or class of users. Users must only receive the minimum access(es) necessary to perform their jobs. SEDL must separate system support functions to avoid allowing a single individual to perform multiple sensitive processes. Whenever possible, development, test and operational facilities must be separated to support this segregation of duties and prevent unwanted alteration or modification of operational systems. At least two persons must possess security expertise in every important computer, network or telecommunication related area. Key personnel must take regularly scheduled vacations and periodically rotate job/shift responsibilities. Having back-up expertise prevents undue interruptions in a system’s service and also increases the likelihood that unauthorized or abusive acts will be detected.

**3.1.8 Compliance**

On at least an annual basis, the Program Managers must validate compliance with personnel security controls for all personnel under their supervision.

**3.2 Physical and Environmental Protection**

Physical and environmental security measures must protect SEDL’s systems, buildings, and related supporting infrastructures against any physical threats. Therefore, SEDL must implement physical security controls commensurate with the risks of physical damage or access.

**3.2.1 Physical Access Controls**

SEDL must control access to facilities and rooms that house systems and their output through the use of guards, identification badges, and/or entry devices such as keycards to prevent unauthorized entry. SEDL must establish emergency exit and reentry procedures to protect assets during an emergency and to prevent unauthorized reentry into facilities after the emergency ends. SEDL facility personnel and system users must securely store unused keys, keycards or other entry devices used to enter sensitive areas and return these devices when no longer needed.

SEDL personnel must authenticate visitors, contractors, and maintenance personnel through the use of preplanned appointments and identification checks, and must escort these persons when in restricted or sensitive areas.

Restricted or sensitive areas must have clearly defined security perimeters, with appropriate access controls that must restrict access to these areas to authorized personnel only and grant access in a way that creates an audit trail. Audit logs must be reviewed periodically for suspicious activity. If applicable, facility personnel must change entry codes periodically. SEDL management and supervisors must regularly review the list of persons with physical access to these areas. SEDL personnel must report all suspicious activity and/or security violations to management.

To protect data from unauthorized disclosure, SEDL personnel and contractors must locate computer monitors displaying sensitive data in areas that prevent viewing by unauthorized personnel. SEDL personnel must restrict and monitor physical access to data and telecommunication transmission lines and their housing facilities. In the case of portable/mobile devices, personnel must encrypt data files that contain information designated as "sensitive."

**3.2.2 Environmental Controls**

To protect SEDL’s supporting utilities, such as electric power distribution nodes and lines, heating/air conditioning facilities and units, water pipes, etc. SEDL must maintain and periodically review its environmental assets for risk of failure. In particular, SEDL must locate water circulation systems and piping in such a way as to prevent them from representing an environmental risk to critical electrical and/or data processing facilities. Facility personnel must implement controls to mitigate natural disasters (floods, earthquakes, tornadoes, etc.) as well as man-made disasters such as fire, water-line breaks, sewage problems, etc. Since power outages/spikes occur more frequently than most other utility problems, facilities must provide uninterruptible power supplies or backup generators to areas that support sensitive and vital SEDL systems to allow critical systems to shut down without damage or loss of data. Where feasible, facilities must have alternate environmental controls, such as power sources, redundant air conditioning, etc. to maintain the functionality of critical data systems.

**3.3 Production Input/Output Controls**

All SEDL systems must have procedures controlling system production inputs and outputs. Every SEDL system user must have access to a help desk or other user support system capable of providing assistance to authorized users of the system in the event of an incident involving the input or output of data.

SEDL must ensure that unauthorized individuals cannot read, copy, alter or remove any printed or electronic information for their own use or the use of another. Only authorized users may pick up, receive, or deliver input and output information and media.

SEDL Program Managers must establish procedures and protection controls to safeguard the storage of media. Movement of sensitive media from or into storage or restricted areas must be logged and an audit trail must be maintained to record all such movements. Security personnel must establish and maintain controls for transporting or mailing media or printed output.

SEDL must establish procedures for shredding or destroying sensitive hardcopy media when no longer needed or when damaged/spoiled. These procedures must include a logging form to keep track of the destruction. Every system also must have procedures for sanitizing SEDL electronic media for reuse, storage or destruction when no longer needed or if it becomes damaged/spoiled. Best practices dictate the destruction of data 90 days after it is not longer required.

**3.4 Contingency Planning**

SEDL’s Contingency Planning policy defines the emergency operating procedures that must be followed to make sure SEDL’s critical functions continue to operate and support IT systems in the event of disruptions, both large and small. Emergency procedures must have timelines for recovery and restoration of specified services prioritized by the system’s mission criticality. SEDL must regularly review and test backup and restoration procedures.

SEDL must identify, prioritize and document its most critical and sensitive functions and operations, and the information system resources that support those functions. SEDL General Support Systems (GSS) and Major Applications (MAs) are divided into different Tier levels based upon their evaluated sensitivity and criticality levels. SEDL must assess the changes to the processing priorities for each system and obtain approval by the CEO.

SEDL uses the Tier level to determine if a continuity of support plan is needed or a continuity of support and disaster recovery plan is necessary. Tier 1 and 2 need only a continuity of support plan. The continuity of support plans and disaster recovery plans must have detailed procedures for restoring operation of the system, including the personnel responsible and the timeline within which the SEDL system must be returned to normal business operations. For systems restored from original software, system administrators must reset all system defaults. SEDL must train personnel responsible to execute contingency procedures on SEDL systems.

The SSO for SEDL systems must complete a comprehensive continuity of support plan prior to the starting the authorization process. An existing system, when preparing for reauthorization, also must have a comprehensive continuity of support plan before granting authorization for processing. All continuity of support plans must incorporate the results of the latest risk assessments to focus attention on the most likely disrupting events. The SSO must distribute the continuity of support plan to appropriate personnel.

**3.4.1 Plan Maintenance**

Each continuity of support plan must specify conditions necessary for activating the plan and who is to be involved in the activation decision. The CIO and SSO must review and approve the continuity of support plans and apprise the CEO of updated versions. In addition to the primary operating location, SEDL must store plans at a secure offsite facility along with all necessary documentation for operating and/or restoring each of SEDL’s systems and applications. Additionally, SEDL must maintain copies of key vendor contracts that impact the operation or restoration of core SEDL functions at this location.

At least annually, the SSO must conduct and document tests of their continuity of support/disaster recovery plans. The SSO must readjust and update the continuity of support plans and disaster recovery plans as necessary to continue their effectiveness. Program Managers must inform the Designated Accrediting Authority (DAA) and the CEO of the results of the testing and any resulting readjustments to the plans.

**3.4.2 Alternate Site Capability**

The CIO and SSO supporting SEDL General Support Systems (GSSs) or Major Applications (MAs) must plan for the use of a secure alternate processing site geographically removed from its primary site. Such alternate processing sites may only operate with a contract or service level agreement in place that includes the appropriate standards of confidentiality, integrity and availability.

**3.4.3 System Backup**

Every system must have documented backup procedures, which include frequency (daily, weekly, monthly) and scope (full backup, incremental backup, and/or differential

backup). The SSO must backup all systems’ critical data files nightly and move the files to a geographically separate location each day. System personnel must ensure that all essential business information and software can be recovered up to the most recent system backup preceding any contingency event. System backups must be completed at least weekly. More frequent backups are required for critical systems or processes whose data is updated frequently. At least three generations/cycles of backup information must be retained for mission critical or mission important systems.

**3.5 Data Integrity**

It is the responsibility of SEDL Program Managers to maintain the controls necessary to protect the integrity of data and information processed within their units. The SSO must document data integrity procedures to describe how the system detects and prevents any unauthorized alteration or destruction of data, caused by either malicious or accidental means.

**3.5.1 Virus Detection and Elimination**

SEDL must install virus detection and elimination software on every system and their applicable devices. Once installed, the SSO must establish procedures for routine updates to virus signature files, including automatic and/or manual virus scans. Users must scan untrusted removable media. Virus scanning must include screening non- text files.

**3.5.2 Verification**

SEDL systems must use integrity verification programs that meet the integrity requirements of the system. Such verification programs must look for evidence of deliberate acts such as data tampering, as well as data entry errors, corruption of correctly entered data and omissions. Techniques must include consistency and reasonableness checks and validation during data entry and processing.

**3.5.3 Reconciliation**

Every system must establish procedures to reconcile data transfers, including a description of the actions taken to resolve any discrepancies.

**3.5.4 Message Authentication**

SEDL systems with requirements for non-repudiation and medium or high integrity must have written procedures on the use of message authentication. Message authentication is used both to verify identity of the sender of a message and determine whether or not the message has been altered during transmission. SEDL personnel must review these procedures at least annually to sustain their continued validity.

**3.5.5 Performance Measurements**

Every system must use system performance monitoring to create and analyze system performance logs for availability problems, including active attacks and system and network slowdowns and crashes. Commensurate with the system’s availability requirements, personnel may need to analyze performance logs on a near real-time basis. SEDL's SSO must establish written procedures if their system requires near real-time performance analysis. The SSO also must identify whether the system’s availability level can operate using periodic performance sampling or other less demanding controls. These procedures must be reviewed at least annually.

**3.5.6 Intrusion Detection**

SEDL 's SSO must monitor current status of intrusion detection tools on SEDL's information systems and networks.. The SSO must inform the CIO whenever intrusion detection tools are implemented or modified. The records must include a description of intrusion detection tools installed on the system, where they are placed, the type of processes detected/reported, and the handling procedures. System logs must be reviewed for anomalies on a daily basis, using automated or manual methods. Additionally, SEDL's SSO must routinely review intrusion detection reports after suspected incidents, and assign responsibility for incident resolution and lessons learned. The CIO must be informed of the status of intrusion detection related issues.

In order to validate intrusion detection tools, SEDL Program Managers must conduct periodic reviews on the software and data content of the systems for which they are responsible. All unapproved files or amendments discovered during such reviews are subject to a formal review process to determine the level of risk such unapproved software/data content represents, and the extent to which intrusion detection or other tools may not have performed adequately to alert system operators to the unauthorized installation(s). SEDL must maintain formal documentation concerning all such reviews.

**3.5.7 Penetration Testing**

SEDL Program Managers must request the penetration testing performed on the system(s) for which they are responsible. In addition, they must establish procedures for each system to ensure that the penetration testing is conducted appropriately and on a periodic basis. The SSO must record results of such testing and report on the ensuing corrective actions.

**3.6 Documentation**

Every SEDL system must have sufficient security documentation to describe adequately the security controls and procedures governing the operation and maintenance of the system. At a minimum, SEDL's System Security Officer (SSO) must maintain the following documentation for all SEDL Major Applications and General Support Systems:

* A current System Security Plan.
* Certification and Accreditation documents and statements authorizing a system to process, including all required appendices.
* A log of service packs, patches upgrades, etc. for the system, and the order of installation.
* A network diagram and documentation on placement and configuration of firewalls, intrusion detection sensors or other security software or appliances.
* Standard operating procedures that support all operations of the application or general support system.
* User manuals to explain correct usage of software/hardware.
* Vendor-supplied documentation of software and hardware.
* Application documentation, requirements, and specifications per the system’s current contract.
* Software and hardware testing procedures and results.

The SSO must know the locations and latest version numbers of all required documentation.

**3.7 Configuration Management**

The CIO must create a configuration management plan that describes the hardware and system software maintenance controls in place and the process by which configuration controls will be maintained for that system.

This must include an established, systematic process for addressing the introduction of new configurations into SEDL systems and networks to make sure software upgrades or security patches work in the intended way and do not adversely impact other security or functionality aspects of the system. Therefore, all SEDL systems must have the following configuration change controls in place.

**3.7.1 Configuration Controls**

The CIO must establish procedures to address configuration changes unique to the system. SEDL must create a formal change control process for each system requiring tests and approval for any change before entering into production. The procedures must include the following:

* Every system must use software change request forms to document requests and related approvals.
* Every system must use version control, allowing association of system components to the appropriate system version.
* The SSO must be a member of the configuration control group and make recommendations on proposed changes.

**3.7.1.1 Change Management**

The SSO must make sure every system for which he/she has responsibility follows the configuration management process, including descriptions and enforcement of change identification, approval, and documentation procedures. The SSO must make recommendations on the required training needed for both technical and user communities to implement new configurations and controls.

SEDL change management processes must include the following:

* Impact Analysis to determine the effect of proposed changes on existing security controls, including the required training needed to implement the control.
* Documentation of all changes to application software along with the procedures used for testing and/or approving changes to system components prior to proceeding to the production environment.
* Specification of the type of test data to be used (live or made-up) in the testing process.
* If live data is to be used, specification of the process for assuring the confidentiality and integrity of the data. Prior to this, the DAA must approve the usage of the live data.
* Documentation of test results and, upon implementation, Program Manager’s review of the updated detailed system specifications.
* Documentation describing the distribution and implementation of new or revised software, including effective date for all locations.
* Consideration of special procedures for performance of emergency repair, emergency maintenance, and interim authorization for processing.
* Documentation of emergency change procedures, which must be approved by management within a maximum of five days. These procedures must be dynamic and regularly updated to draw upon actual experiences with emergencies.
* Timely updates to system security plans, Continuity of Support Plans, and other associated documentation.

**3.7.2 Configuration and Management Documentation**

The SSO must develop procedures to restrict or control the activities of those who perform maintenance and repair activities, both on-site and off-site. These procedures must fully consider the criticality of the system and the need to protect the confidentiality, integrity and availability of the data and information it contains and/or processes. SEDL Program Managers must specify the procedures that reflect issues such as the escort of maintenance personnel, sanitization of devices removed from the site, and other issues relevant to the systems under his/her control. The SSO may document these procedures in a Configuration Management Plan and/or in the system’s security plan.

**3.7.2.1 Maintenance and Repair**

The CEO, CIO, and the SSO must review all default security parameters to correlate with system sensitivity requirements. In most instances, default security settings should be set to a restrictive setting. Where necessary, use the most restrictive settings.

The SSO must describe procedures used to control remote maintenance services. Remote system maintenance can only be approved by the DAA during the C&A process. The SSO must implement access controls and other security precautions to prevent potentially malicious code, such as "back doors," from being used to evade authentication and authorization protections. Implementation of maintenance or repairs must take place at such times and under such circumstances so as to minimize impacts to business processes.

The SSO periodically must review SEDL systems to identify and, eliminate unnecessary services (e.g. FTP, HTTP,). Depending on the cost to remove and the importance of the service, the DAA can make a risk based decision on allowing certain services to remain. The system, though, should be upgraded to remove the unnecessary service as soon as possible. Additionally, the SSO periodically must review systems for known vulnerabilities and current installation of software patches. These reviews are separate from the C&A review conducted by the DAA.

**3.7.2.2 Unapproved Software**

Software installation and use must follow the principle that whatever is not expressly allowed is denied. SEDL must establish organizational procedures for dealing with, and protecting against, the inappropriate use of copyrighted software. If SEDL uses a copyrighted product, sufficient licensed copies of the software must be purchased for each system on which the application will be processed.

Installation of personal software on SEDL’s assets is prohibited unless approved in writing from the CIO. In the unusual instance where personally owned software/equipment is used for processing SEDL business, the user must document each instance including provisions to protect software copyrights and inform their supervisor in writing. SEDL must perform periodic audits of SEDL computers to make sure users do not install unapproved software.

**3.7.2.3 Application Ownership**

Contracts must clearly specify whether the ownership the software or if the application software was received from another entity with the understanding that it was SEDL’s property.

**3.8 Incident Response**

The confidentiality, integrity and availability of SEDL networked systems will depend in part on the preventative security measures to deter or inhibit attacks. SEDL must employ intrusion detection tools, firewalls, automated audit logs, and other preventative measures to assist system security staff when a security incident occurs in a system.

SEDL must adequately train system security personnel to recognize security incidents. SEDL must establish procedures for reporting and responding to those incidents. Once identified, SEDL must monitor and track an incident until resolved, and maintain documentation concerning the incident and its resolution.

**3.8.1 Information Sharing**

SEDL must share information regarding incidents and common vulnerabilities or threats with SEDL system personnel and appropriate managers of systems and networks interconnected with SEDL as appropriate or required by contract.

SEDL management must assign specific individual(s) to receive and respond to alerts/advisories, vendor patches, exploited vulnerabilities, etc.

**3.8.2 Incident Identification**

SEDL must adequately train system security personnel to recognize security incidents. Non-security personnel must never attempt to prove suspected weaknesses on their own, as SEDL must treat this act as an actual attack that may result in heavy penalties, including termination of employment.

Users must notify SEDL CIO, SSO, and/or system administrators as soon as possible regarding any observed or suspected security weaknesses in, or threats to, SEDL systems or services. Once reported, SEDL must analyze security alerts and security incidents and take appropriate actions. Users must report software malfunctions and report the malfunction using the same procedures.

The SSO must report incidents to the CEO. The CEO will forward these reports to appropriate parties for further dissemination.

**3.8.3 Post Incident Activities**

SEDL Program Managers and the SSO must review incident handling procedures and control techniques after each incident and, when necessary, modify the procedures to prevent recurrence and improve response techniques/methods. In addition, SEDL Program Managers and the SSO must collect and secure audit trails and other tracking mechanisms for analysis and use as potential evidence.

**4 TECHNICAL CONTROLS**

The System Technical Controls section focuses on security controls that the system executes as opposed to controls performed by people. These controls depend on the proper functioning of the system for their effectiveness.

**4.1 Identification and Authentication**

Each SEDL system must use identification and authentication procedures to prevent unauthorized use or access. Before granting initial access to an SEDL system, the SSO must verify the following:

* The user has authorization from the system owner and supervisor to access the system,
* The level of access is appropriate for the user's business purpose,
* The access will not compromise segregation of duties,
* The user received a copy of the Rules of Behavior for the system and has signed a statement indicating that he/she understands and agrees to the Rules, and
* Completion (for high-risk positions) or initiation (for low-medium risk positions of proper background screening.

SEDL systems must correlate actions to users via the creation of unique user IDs for each individual user. These IDs must not give any indication of a user’s privilege level (i.e., Administrator, etc.). SEDL must permit and approve Group IDs only when necessary. Any user who requires special privileges or features beyond their primary job function, which would allow them to override system or application controls, must use an additional user ID different than that used for normal business purposes. Along with user IDs, SEDL systems must have documentation describing whether passwords, tokens, biometrics or other methods are used for access purposes and how the access control mechanisms will support individual accountability and audit trails. At a minimum, these access control methods should be associated with the unique user IDs.

Security controls must be able to detect unauthorized and/or invalid attempts to access SEDL systems. The number of invalid access attempts that may occur for a given user ID or access location (i.e. terminal or port) must be determined and documented. Within the documentation, the SSO must include the actions taken when that limit is exceeded.

When a SEDL system allows bypassing of user authentication requirements, (for example, single-sign-on technologies, host-to-host authentication servers, user-to-host identifier, and group user identifiers), the SSO must document the governing procedures, as well as any compensating controls and whether emergency or temporary access is authorized. Host-based authentication, granting access based on the identity of the host originating the request instead of the individual user requesting access, is permitted to control access. If this method is used on SEDL systems, it must be documented and controls put in place to remove access authorization when hosts no longer have legitimate access.

**4.1.1 System Login**

Login procedures should include an appropriate banner containing the following warning:

*You are about to access* SEDL's *restricted computer network intended for authorized users only. You should have no expectation of privacy in your use of this network. Use of this network constitutes consent to monitoring, retrieval, and disclosure of any information stored within the network for any purpose including criminal prosecution.*

The banner must include a "click through" requirement so that the person logging in must agree to the terms before accessing the SEDL system.

Login procedures must also limit the amount of information displayed about the system and its functions until after a user has successfully logged in. SEDL systems must not display the following during login:

* System or application identifiers,
* Help messages, and
* Validation of any portion of the login information, for example, not indicating which part of the login data was correct or incorrect.

In addition, SEDL systems’ logins must mask a user’s password during login.

**4.1.2 Passwords**

If passwords are the access control method used for authentication to an SEDL system, the SSO must document password procedures for each system. The documentation must include specific information regarding allowable character sets, password length (maximums and minimums), password aging time frames and enforcement approach, and the number of generations of expired passwords disallowed for use. Acceptable SEDL passwords must contain a minimum of eight characters in length and include a combination of at least one of each of the following to meet or exceed FIPS Publication 112 standards:

* English uppercase letters (A-Z)
* English lowercase letters (a-z)
* Westernized Arabic numerals (0-9)
* Non-alphanumeric special characters (!, @, #, $, &, \*)

Any vendor-supplied and/or default passwords on SEDL systems must be changed immediately. If users maintain their own passwords, an initial password will be distributed to the user in a secure manner. Immediately upon initial login, the user will be forced to change their password. Temporary passwords (if a user forgets their password) must only be given after positively identifying the user. The temporary password must also be distributed to the user in a secure manner, and users must change it immediately upon initial login. Users will be informed not to write down or reveal their passwords to anyone. Procedures must be in place for handling lost and/or compromised passwords. Passwords that can be associated to an individual account must be encrypted in transit, and all passwords must be encrypted while stored.

Procedures must be in place describing creation of emergency passwords. These procedures must include who may authorize, duration of password validity, and criteria for granting emergency access.

Every system must establish procedures to enforce password changes and identify who changes their passwords. To determine if user passwords meet the minimum standard, SEDL must establish procedures (such as using password crackers/checkers) to determine compliance. Use of such tools must be limited to only those persons expressly authorized by the SSO. The SSO must record the authorization and specify the locations, systems and duration covered by the authorization.

Every SEDL system must have procedures that describe how it limits access scripts with embedded passwords (e.g., scripts with embedded passwords are prohibited, or scripts with embedded passwords are allowed only for specific (i.e. batch, etc.) applications).

SEDL systems will have a lockout mechanism for system access; after three unsuccessful login attempts in a row, users will not be allowed to access the system again until they reset their password or contact an administrator, etc.

**4.1.3 PKI and Biometrics**

SEDL or SEDL contractor's use of public/private key cryptography (including SSL) must conform to applicable NIST FIPS. The applicable waiver policy is described in Section 1.5, *Exceptions*. Every system using cryptographic technology must have procedures documented in the System Security Plan describing cryptographic key management procedures for key generation, distribution, storage, entry, use, destruction, and archiving.

Documentation for every SEDL system must describe whether encryption is used to prevent unauthorized access to sensitive data stores or transfers.

Biometrics and/or tokens are permitted as other access control methods to authenticate users to their systems. Systems using these methods must describe the controls used and how they are implemented on the system. Documentation must indicate if any special hardware (such as card readers) is required, if users are required to use a unique Personal Identification Number (PIN), and who selects the PIN.

**4.2 Logical Access Controls (Authorization/Access Controls)**

SEDL’s logical access security controls are system-based mechanisms that must restrict users to authorized transactions and functions only. These controls must detect and log unauthorized transaction attempts by authorized and unauthorized users and must reside at the application, operating system, and/or network level, depending on the system.

Access controls for SEDL systems and networks must:

* Deny access to systems by undefined users or anonymous accounts,
* Limit and monitor the usage of administrator and other powerful accounts,
* Suspend or delay access capability after a specific number of unsuccessful logon attempts,
* Disconnect automatically at the end of a session,
* Remove obsolete user accounts as soon as a system user leaves SEDL,
* Suspend inactive accounts after 90 days,
* Remove redundant user IDs, accounts, and role-based accounts from resource access lists,
* Protect Audit Logs through strict access controls, and
* Protect the confidentiality of sensitive information during data transfers and storage.

Every SEDL system must have a security plan that describes the specific security controls for hardware and software features that are designed to permit only authorized access to or within an application, its data, or other files. In addition, every SEDL system must have documentation that describes any restrictions to prevent users from accessing the system or its applications outside of normal work hours or on weekends. SEDL Program Managers must establish procedures to restrict and control access to all program libraries, system software, and system hardware. Access to security software and hardware is restricted to security administrators. Any privileges allowing a user to override these system or application security controls may only be granted to individual users when it is determined that the user needs these privileges to perform his or her job. When granted, such privileges must be at the minimum level necessary to complete the specific job.

The CIO must assign a person(s) to review protocols with known vulnerabilities, such as UDP and TFTP, and receive approval for their use prior to implementation from the CEO and the DAA. Documentation for every system must describe any type of secure gateway or firewall in use, including its configuration. If installed, firewalls must meet the standards set forth in the SEDL Enterprise Technical Architecture document. System personnel must disable unused system features, services, protocols and ports. System personnel must also reinitialize all vendor supplied default security parameters to more secure settings. Documentation regarding any port protection devices requiring specific access authorization to the communication ports must include the configuration of the port protection devices and whether additional passwords or tokens are required.

**4.2.1 Access Control List**

The CEO must assign an employee to create and maintain a current list of authorized users and their access. The CEO must approve the list before its implementation. This Access Control List (ACL) must be protected to prevent unauthorized access or viewing of the file. The person(s) responsible for the ACL must remove users who no longer have access rights from the ACL. To corroborate this process, system personnel must review ACLs 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 system, invalid users, and redundant user IDs and accounts.

**4.2.2 Internet or Public Access**

If an application is running on an SEDL system that is connected to the Internet or other WAN, SEDL must install additional technical security controls to provide protection against unauthorized system penetration. Authorization procedures must determine which network and network services are allowed and who is authorized to access them.

If the public accesses a SEDL system, SEDL must develop and implement security controls to protect the integrity of the application and the confidence of the public. Each SEDL web page (unique site) must have a designated author or administrator who is responsible for ensuring web page security. If a server contains information protected by the Privacy Act, it must not be accessible without proper authorization. Additionally, the website should provide notice that it contains Privacy Act information, and give notice of the consequences of unauthorized disclosure. Users wishing to access internal SEDL systems via the Internet must be authenticated.

**4.2.3 Remote Access**

An SEDL user may only be authorized to telecommute (i.e., dial-in, VPN, etc.) after he/she has submitted a request to the supervisor. If the supervisor approves the request, it will be submitted to the SSO for review and decision regarding the request. Appropriate system personnel must monitor all dial-in access. All requests that are granted must be documented, including duration required and reviewed.

**4.3 Audit Trails**

SEDL audit trail records must maintain a log of system and network activity both by system or application processes and by user activity for a minimum of one year. In conjunction with appropriate tools and procedures, audit trails must provide individual accountability, a means to reconstruct events, detect intrusions, and identify problems. These tools will assist the SSO in investigating suspicious activity and take appropriate actions. SEDL must strictly control and protect access to audit logs and automated tools against unauthorized changes and/or operational problems. This is especially necessary if authorized security personnel can review the logs online and/or if they contain personal information about SEDL users. To access and review audit logs, the reviewer must be an appropriate system-level or application-level administrator. The SSO must approve authorization to view logs. Logs must be reviewed at least weekly or after a known system or application software problem, a known violation of existing requirements by a user, or some unexplained system or user problem. The use of automated tools is recommended to help interpret information contained in audit records, discard irrelevant or mundane task information, as well as to distill useful information from the raw data.

SEDL audit logs must include:

* Information on all activity involving access to and modification of sensitive or critical files and/or directories.
* Sufficient information to establish what events occurred, and who or what caused them. In general, an event record must specify:
  + Type of event;
  + When the event occurred;
  + User ID associated with the event; and
  + Program or command used to initiate the event.
* Records of the number of successful and rejected system access attempts, data access attempts, and other resource access attempts.

The audit logs must have the capability of being queried by user ID, terminal ID, application name, date and time, or some other set of parameters in order to run reports of selected information. Audit trail clocks and machine clocks must be synchronized to an agreed upon standard to avoid discrediting the validity of the logs during an investigation. The SSO must develop procedures to check and correct any deviations in the time.

Whenever SEDL uses keystroke monitoring, the SSO must document the procedures. SEDL must segregate the duties between SEDL security personnel who administer the

access control functions and those who administer audit functions. This is to protect

audit functions and/or access control functions from being intentionally or unintentionally reconfigured.

**4.4 Software**

Usage of open source software in SEDL is permitted under controlled circumstances. For more information, please review the SEDL Open Source Software Usage Guide.

**5.0 ROLES/Designees**

Chief Executive Officer (CEO) - Wesley A. Hoover

Chief Information Officer (CIO) - Stuart Ferguson with technical assistance from consultant Jon Wyrick, Beyond Secure

System Security Officer (SSO) - Cliff Pierron with technical assistance from consultant Jon Wyrick, Beyond Secure

Program Managers: Assigned by project (e.g., Vicki Dimock, Melissa Dodson, Robin Jarvis, Christine Moses-Egan, Michael Vaden-Kiernan, John Westbrook)

Web developer: Assigned by project (e.g., Brian Litke, John Middleton, Eric Waters, Luis Martinez)

Designated Approval Authority (DAA) - Entity funding a project (e.g., U.S. Department of Education)

**APPENDIX A: TERMS OF SERVICE AND ACCEPTABLE USE**

**The following will appear on the screen and must be accepted before logging in to the SEDL Guest Network.**

**Terms of Service and Acceptable Use for SEDL Guest Network**

BY CLICKING ON "LOGIN", YOU REPRESENT THAT YOU HAVE READ, UNDERSTAND AND AGREE TO THESE TERMS OF SERVICE.

You are about to access SEDL's restricted computer network intended for authorized users only. You should have no expectation of privacy in your use of this network. Use of this network constitutes consent to monitoring, retrieval, and disclosure of any information stored within the network for any purpose including criminal prosecution.

All users shall use SEDL’s computing and network resources in a legal, ethical, and responsible manner, consistent with the professional and educational purposes for which it is provided. Activities conducted online shall not violate any applicable law or regulation or the rights of SEDL or any third party. Additional detail is provided in the SEDL Security Policy.

Users are expected to secure their devices when they are using wireless network services. Windows computers must have active antivirus software. Antivirus signature files and operating system security patches must be kept up to date. SEDL reserves the right to monitor computing devices and network services and to block or disconnect non-compliant computers from the SEDL network. Users using the wireless network should also use secure remote access procedures, e.g., passwords should never be disclosed to anyone or shared.

Use of SEDL's wireless network is entirely at the risk of the user. The service is provided “as is” and “as available”. SEDL disclaims all liability for loss of confidential information or damages resulting from that loss.

**Terms of Service and Acceptable Use for SEDL Information Technology Systems for all SEDL staff.**

BY SIGNING BELOW, I REPRESENT THAT I HAVE READ, UNDERSTAND AND AGREE TO THESE TERMS OF SERVICE AND ACCEPTABLE USE.

All users shall use SEDL’s computing and network resources in a legal, ethical, and responsible manner, consistent with the professional and educational purposes for which it is provided. Activities conducted with SEDL systems shall not violate any applicable law or regulation or the rights of SEDL or any third party. Additional detail regarding security and use is provided in the SEDL Information Technology Management, Security, and Use Policy, which is accessible to all staff through SEDL's Intranet at

(http://www.sedl.org/cgi-bin/mysql/staff/index.cgi?group=sedl\_policies\_handbook).

Users are expected to secure their devices when they are using wireless network services. Windows computers must have active antivirus software. Antivirus signature files and operating system security patches must be kept up to date.

SEDL staff may not install any hardware or software on any SEDL telecommunications resource without prior written authorization of SEDL's CIO or designee.

SEDL reserves the right to monitor any aspect or use of its computing devices and network services and to block or disconnect non-compliant computers from the SEDL network. Users using the wireless network should also use secure remote access procedures, e.g., passwords should never be disclosed to anyone or shared.

**Passwords.** Acceptable SEDL passwords must contain a minimum of eight characters in length and include a combination of at least one of each of the following to meet or exceed FIPS Publication 112 standards:

* English uppercase letters (A-Z)
* English lowercase letters (a-z)
* Westernized Arabic numerals (0-9)
* Non-alphanumeric special characters ( ) ` ~ ! @ # $ % ^ & \* - + = | \ { } [ ] : ; " ' < > , . ? /

**Protection of SEDL Intellectual Property and Proprietary Information.**

*Working on SEDL files outside of SEDL equipment/network.* To ensure the security of SEDL intellectual property and project data with which SEDL has been entrusted, staff will utilize encryption to protect sensitive data, including any with personally identifiable information, which is sent electronically or transported on a computing device outside of SEDL’s offices. Files should be encrypted using TrueCrypt or comparable software on portables and data drives, including but not limited to USB drives.

*Cloud technology.* SEDL limits the use of cloud technology for SEDL business processes and sensitive information. Use of cloud technology must be preapproved by SEDL’s CIO before SEDL information or project data is hosted there. When cloud technology is in use, a test of the security and permissions used to protect the hosted information must be performed prior to use.

*Use of SEDL equipment on other networks (home, hotels, wireless).* In general, it is best to minimize use of SEDL equipment on external networks and limit it to occasions where your work or travel requires it. When SEDL computing devices are used on other networks, access to SEDL’s intranet resources are restricted and staff must use VPN software to access SEDL’s private network. If you suspect your computer may have been infected by malware while traveling or while connected to an untrusted network, notify SEDL’s network administrator.

**Personal Use.** Small, reasonable amounts of personal use of SEDL’s telecommunications resources are permitted as long as such use is consistent with this usage policy. Staff should exercise good judgment regarding the reasonableness of personal use and should never use SEDL resources for personal commercial, political, or religious activities. Also, in such personal use, the staff member should avoid any mention in the text of the message of their affiliation with SEDL including use of a SEDL business electronic signature. Personal telecommunications equipment (for example, cell phones, camera phones, PDAs, and other such devices) shall not be used to create disruptions in the SEDL work environment or to, in any way, compromise the security of SEDL’s proprietary information or staff members. Any personal telecommunications equipment or devices that are connected to SEDL's network infrastructure become subject to SEDL's acceptable use policy, including the right to monitor use.

**E-mail.** Because of the large volume of e-mails SEDL sends and receives, staff should not store e-mail messages on SEDL’s mail servers, making a regular practice of deleting e-mails once they have been read. If a particular e-mail needs to be saved, it should be printed, archived, or saved to a mail folder on a local hard disk.

Because this email retention policy is not intended to destroy any evidence that might conceivably be relevant to any pending matter or potential dispute, its implementation may be suspended in whole or in part from time to time in the event SEDL’s President and CEO is properly notified and directs that email should be saved in connection with any pending matter, potential dispute, or other proceeding.

Finally, information transmitted as part of a staff member’s identifying signature on any business email should be limited to that contained on the staff member’s SEDL business card.

SEDL reserves the right to update this policy as needed and required.

Printed Name

Signature Date

1. 800-26 includes requirements from OMB A-130 Appendix III, FISCAM, and Computer Security Act. [↑](#footnote-ref-1)
2. The Program Manager, in consultation with SSO, will determine if a change is considered major. The CIO. would usually serve as a change control checks and balances [↑](#footnote-ref-2)