DAS Department of Administrative Services

Internal Operations Manual

SUBJECT: Information Technology Security **NUMBER:** 107-01-080

DIVISION: Director's Office **EFFECTIVE DATE:** 06-22-00

APPROVED:

POLICY/ PURPOSE: This policy is designed to clarify the responsibilities of management and systems users to help protect the Department of Administrative Services (DAS) information and information systems and bring about a higher level of information security.

AUTHORITY: All DAS Employees.

APPLICABILITY:
DAS IRMD Policy 03-07 Notification of Products for Trial or Evaluation
DAS IRMD Policy 03-08 Software License Agreements
DAS IRMD Policy 03-12 Electronic Mail
DAS IRMD Policy 03-13 Using the Internet
DAS IRMD Policy 03-16 Security, Contingency and Disaster Recovery Planning
DAS IRMD Policy 03-21 Acceptable Use of State Electronic Information Systems
DAS HRSD Policy 50.050.01 Telecommuting
DAS Internal Operations Manual Policy 107-01-010 Use of DAS Electronic Systems

ATTACHMENTS: Computer Security User Declaration Form

DEFINITIONS:

- **Approving Authority** – The individual with top level approval and signature authority for all DAS Information Technology (IT) policy; currently the Chief Information Officer (IRMD Administrator).
- **Enterprise Network** – Information technology infrastructure aggregated across an entire organization or group of organizations utilizing a coherent and standardized architecture and design.
- **Integrity** – The ability to ensure the system software, applications, information, hardware configuration, connectivity, and privilege system settings cannot be altered during storage or transmission.
- **IT Management** – Managers who have any type of computer system under their direct control.
- **IT Security Plan** – The unique processes, within each division, that are implemented in order to accomplish the goals of the IT Security Policy.
- **Life Cycle Management** – The internal control structure and ongoing management of a product or process across its useful life.
- **User Account (User ID and Password)** – In a computer system a user is recognized by unique identifiers known as a User ID and Password. These identifiers are known only to the system and the user, and used by the system to authenticate a specific user.
- **Virus** – Computer programs containing malicious code that are written to cause some form of intentional damage to computer systems or networks.

GUIDELINES:

I. GENERAL

A. Information technology (IT) policy awareness is the responsibility of the DAS senior management. Divisions are responsible for the security of their stand-alone computing resources. The Information Resources Management Division (IRMD) and the divisions share the responsibility for the security of DAS shared computing resources. Ultimately, it is every user's responsibility to safeguard the information to which they have access, making IT security the job of every state employee. Virtually everyone who manages, designs, programs, operates, or uses information contributes to meeting the goals and objectives of this IT Security Policy.

B. IT Management shall implement internal system safeguards to ensure users are held accountable for their actions. Users who fail to follow mandatory requirements for IT security may be subject to personnel action or dismissal.

C. To prevent a virus from infecting IT systems, users should be aware of and employ basic anti-virus practices such as: utilizing virus prevention software, using only authorized application software, and following agency computer virus procedures.

D. IT Management must ensure system operations and information remain inviolate and are provided protections commensurate with their sensitivity. Requisite protection consists of a combination of controls designed to ensure integrity, availability, and confidentiality.

II. RESPONSIBILITIES

A. **Chief Information Officer (CIO)** – Evaluates overall IT security requirements and provides specific direction to Division Administrators, IT Managers, system developers, and users relative to the risk evident in the IT security platform. Responsible for all aspects of security compliance for IT systems. Specific duties include:
1. Providing direction for IT security policy.
2. Ensuring compliance with IT security policy.
3. Ensuring information ownership is established for each IT system to include: accountability, access rights, and special handling requirements for systems containing sensitive or confidential information.
4. Approving alternative safeguards.
5. Ensuring employees are properly trained or provided training.

B. **Technical Council** – Designated by DAS Division Administrators to review IT policy and make recommendations to Executive Staff.

C. **Division Administrators** – Responsible for the security of IT systems under their control and the development and implementation of their own divisional IT security plan, working in consultation with the DAS IT security designee(s), and following all relevant state standards and security policies. Specific duties include:
1. Providing staff guidance regarding the IT security policy.
2. Ensuring compliance with IT security policy.
3. Ensuring information ownership is established for each IT system under their direct control to include: accountability, access rights, and special handling requirements for systems containing sensitive or confidential information.
4. Ensuring employees are properly trained or provided training.
5. Developing and implementing a divisional IT security plan.

D. **Managers** – Responsible for system security within their specific area of control. They are also responsible for ensuring that reasonable computer security practices are implemented and that every employee under their direct supervision is aware of the DAS IT Security Policy. DAS Managers are responsible for ensuring that computers within their scope of responsibility are accessed, used, maintained, and when appropriate, disposed of according to approved security practices. General duties include:
   1. Ensuring users under their supervision have appropriate clearances prior to being given access to a computer or system.
   2. Ensuring reasonable safeguards for computer security are implemented.
   3. Reviewing IT projects within their scope of responsibility to ensure appropriate controls are in place.
   4. Assisting with the ongoing administration of the agency-wide security policy.
   5. Ensuring that protective measures are initiated if a security incident occurs.
   6. Reporting significant security incidents to the CIO, Internal Audit, and IT Security Personnel.
   7. Reporting information about departing or terminating staff to IT Operations immediately via phone followed by electronic mail.

E. **IT Managers** – Responsible for the secure operation of all systems, ensuring they are accessed, used, maintained, and when appropriate, disposed of according to approved security practices. Responsible for implementing internal system safeguards to ensure users are held accountable for their actions. General duties include:
   1. Ensuring all users and vendors have appropriate clearances, authorizations, and security training prior to being given access to an IT system.
   2. Ensuring safeguards are appropriate for system security and are addressed in system documentation.
   3. Reviewing all proposed changes to system software and hardware to determine if security safeguards have been addressed.
   4. Maintaining a current version of system documentation.
   5. Assisting with the maintenance of agency-wide security policy.
   6. Ensuring that protective measures are initiated if a security incident occurs.
   7. Reporting significant security incidents to the CIO and IT Security Personnel.
   8. Conducting regular evaluations of known system vulnerabilities to ascertain if additional safeguards are necessary.
   9. When available, ensuring audit trail and intrusion detection reports are reviewed on a regular basis.
   10. Directing the development and review of IT contingency/disaster recovery plans.

F. **IT Security Personnel or Designee** – Appointed by the CIO and responsible for the secure operation of all systems, ensuring they are accessed, used, maintained, and disposed of according to approved security practices. General duties include:
   1. Verifying IT users and vendors have appropriate clearances, authorization, and security training prior to being given access to an IT system.
   2. Ensuring IT safeguards are appropriate for the system and are addressed in system documentation.
   3. Reviewing all proposed changes to system software and hardware to determine if security safeguards are affected, reporting any discrepancies to IT Management and the CIO.
   4. Reviewing and assisting with the maintenance of system documentation.
   5. Maintaining an agency-wide IT security policy.
   6. Initiating protective or corrective measures if an IT security incident occurs, and reporting significant incidents to the CIO, Internal Audit, and appropriate IT Management.
   7. Evaluating known system vulnerabilities to ascertain if additional safeguards are needed.
   8. Reviewing audit trails and intrusion detection reports, when available.

9. Assisting in the development of IT contingency/disaster recovery plans.
10. Initiating risk analysis at least every two years.
11. Providing assistance to other state agencies in the areas of risk analysis, IT security policy development, incident response and investigation, and user awareness.
12. Conducting annual compliance reviews to sustain optimal security levels.

G. **System Administrators** – Responsible for the administration of a computer system. They manage access to the system and observe the system for any signs of unusual activity. General duties include:
1. Assigning agency users appropriate access to IT systems.
2. Verifying users and vendors have appropriate clearances, authorization, and security awareness prior to being given access to a system.
3. Utilizing whatever safeguards are appropriate for, and approved by, IT Management for systems security.
4. Maintaining a working knowledge of any system under System Administrator authority and direct control, and a general knowledge of all other DAS systems.
5. Assisting in the review of proposed changes to system software or hardware when required in determining if security safeguards are affected. Reporting any discrepancies to IT Management and IT Security Personnel.
6. Assisting with the maintenance of systems documentation.
7. Assisting with the maintenance of agency-wide IT policy.
8. Initiating protective or corrective measures if a security incident occurs, and reporting all such incidents to IT Management and IT Security Personnel.
9. Evaluating known system vulnerabilities to ascertain if additional safeguards are needed.
10. Reviewing audit trail and intrusion reports daily.
11. Assisting in the development of IT contingency plans.
12. Ensuring that, whenever the system allows, the IT system screen displays a warning message before logon (minimum of one sentence) that lets the user know that unauthorized access to the IT system and software is prohibited. Example: "UNAUTHORIZED USE OF THIS COMPUTER SYSTEM MAY SUBJECT YOU TO CRIMINAL PROSECUTION. EVIDENCE COLLECTED DURING MONITORING MAY BE USED FOR ADMINISTRATIVE, CRIMINAL OR OTHER ADVERSE ACTION. USE OF THIS SYSTEM CONSTITUTES CONSENT TO MONITORING FOR THESE PURPOSES."

H. **Program/Project Managers** – Considered the "owners" of the system or application they are managing or developing and its information. General duties include:
1. Including IT Security Personnel early in the development life cycle of all IT projects to help identify and select appropriate security controls.
2. Implementing appropriate security controls during the program/project development process.
3. Following all applicable IT security policies.
4. Ensuring that all information in the IT system or application is identified and classified as to level of sensitivity.
5. Ensuring project quality assurance reviews are performed to minimize the risk of errors and to ensure the integrity of the systems and information.
6. Providing assistance, as needed, to the IT Security Personnel during acceptance testing and certification to ensure that security elements are understood by IT Security Personnel.
7. Assessing their information for level of sensitivity and protecting it.

I. **Users** – Individuals who have access to, or use of, any state computing resource are expected to:
   1. Protect their passwords and not share them with others, unless directed by the Division Administrators or the CIO.
   2. Protect their network and system IDs.
   3. Assess their information for level of sensitivity and protect it.
   4. Protect their unattended terminal or workstation, and log-off when not in use.
   5. Protect against viruses by virus checking all disks and software from external sources.
   6. Protect their equipment from abuse.
   7. Protect their area by putting away sensitive materials when they are absent.
   8. Protect their files by appropriately saving and storing them.
   9. Protect their media through safe storage and destruction.
   10. Protect against disaster by following disaster emergency procedures.
   11. Report all security violations immediately to their supervisor.
   12. Comply with all applicable laws and organizational policies.

III. SYSTEM ACCESS

A. All DAS systems will have an access control policy (facilities, systems, and information) that defines the intention and strategy of the organization to prevent unauthorized system access.

B. Employees, consultants, and contractors who design, develop, operate, or maintain IT systems shall undergo appropriate background investigations and authorizations for access to system components, output, or documentation.

C. No DAS employee or vendor personnel shall allow or assist in the unauthorized access of any individual to a restricted area within DAS offices.

D. All visitors to restricted premises, not previously cleared or identified by badge, shall be escorted.

IV. USE OF THE IT SYSTEM

A. All users of IT systems must receive appropriate clearances to use a system from IT Management, System Administrators, application administrators (persons who may or may not be within IRMD who authorize access to a given application), or the IT Security Personnel or Designee. This permission must be written, which will include the assignment of a user account (User ID and Password) or issuance of a microcomputer. Users must immediately, following assignment, change their password.

B. All users of an IT system must receive security awareness training, either in a formal classroom setting or by other means such as user awareness brochures, on-line or electronic mail training, or individual instruction from the IT personnel who installs or sets up the workstation.

C. All IT system use is for official business only as specified in DAS policy 107.01.010.

D. All users must report suspicious activity to their supervisor or IT Security Personnel. Suspicious activity includes suspected misuse of government resources; use of the system by an unauthorized party; illegal copying of software; or strange activity on a computer system which may be caused by a computer virus or other malicious logic.

V. PROPER USE OF EQUIPMENT AND SOFTWARE

A. Equipment

1. All equipment must be maintained in such a way as to protect any sensitive information from unauthorized disclosure or destruction.
2. Maintenance personnel should be cleared (background checked) to the highest level of information processed on any IT system they will access.
3. The use of computer equipment not obtained or provided by the agency is restricted. Specific approval from IT Management must be obtained before introducing any privately-owned or contractor-owned equipment.
4. Sensitive information must be completely erased from magnetic media prior to surplus, reuse, or destruction. Accepted techniques for sanitizing media before being reissued for general use or targeted for disposal are physical destruction, degaussing, and overwriting.
5. Personal use of state systems is restricted. DAS IRMD Policy 03-21 governs the appropriate use of state systems.

B. Software

1. The use of software not obtained or provided by the organization will be restricted without prior approval. This includes public domain software, proprietary software, evaluation software, software downloaded from bulletin boards, and personally owned copies of software. DAS IRMD Policy 03-07 governs the use of software acquired for evaluation purposes.
2. The use of software purchased by the organization is governed by the terms and agreements established by the software vendors. IT Management or a designee will verify that employees adhere to all software copyright and licensing agreements and that the software is tracked for compliance. DAS IRMD Policy 03-08 governs software licensing.
3. Personal computer software products may not be copied except to the limit provided by contract. Employees or contractors who make additional copies to avoid the cost of acquiring one lawfully can be held personally liable. Managers purchasing software protected by quantity licenses must ensure a tracking system is in place to control the copy and distribution of the proprietary software.
4. All software loaded on a system must be scanned for viruses.

VI. MANAGEMENT OF USER IDS AND PASSWORDS

A. User IDs

1. Each User ID is to be assigned to only one person at a time.
2. User IDs are not to be shared with another person.
3. User IDs shall be a minimum of six characters.
4. A record of user assignment must be kept for a minimum of three years after a user leaves the organization.
5. Before reuse of a User ID, all previous access authorizations and their associated directories and files must be removed from the system.
6. A user shall have only three attempts to log into the system. After the maximum number of incorrect attempts, the system will lock the user out. Action from the System Administrator is to be required to reactivate the account.
7. Each user must acknowledge receipt of a User ID and Password by signing a statement that details his or her responsibility for protecting this information prior to being issued a password.
8. A User ID must be suspended by the System Administrator for any of the following reasons:
   a. Termination of employment or contract (within 24 hours).
   b. Nonuse of account for six consecutive months (one year for RACF).
   c. Notification of security violation (by management direction).
   d. As directed by the CIO.

B. **Passwords**

1. System password files should be protected as confidential information.
2. Passwords must never be stored in clear text.
3. The maximum lifetime for all passwords should be no longer than 90 days.
4. Passwords must be at least seven alpha and numeric characters in length and should contain both upper and lower case letters.
5. Passwords must not spell a common word or name.
6. Passwords must not be repeated within a 12-month period.
7. Users must not use personal information for their passwords (e.g., birth dates, home address, etc.).
8. Users are not to share passwords with anyone, unless directed by their manager or the CIO. Users will keep passwords safe and confidential at all times. Requisite protection consists of a combination of controls designed to ensure integrity, availability, and confidentiality.

VII. HANDLING OF CONFIDENTIAL, SENSITIVE, OR GENERAL INFORMATION

A. All sensitive output, media, and media containers should be marked to accurately reflect the information classification: confidential, sensitive, or general. Confidential or sensitive information includes, but is not limited to passwords, encryption keys, program source code, financial transactions, and personnel records.

B. Confidential information is not to be sent via the Internet or transmitted by modem unless security controls, such as the appropriate level of encryption, are in place.

C. Recipients of confidential information shall be made aware of the classification of the information.

D. Transmission of confidential information shall be by means that preclude unauthorized disclosure.

E. Transmittal documents shall call attention to the presence of confidential attachments.

F. Records containing confidential information shall be transported in a manner that precludes disclosure of the contents.

VIII. MINIMUM SECURITY REQUIREMENTS

A. **Access** – System Administrators shall implement an access control policy that will positively identify each user who is authorized to access a system prior to granting access.

B. **Accountability** – DAS IT Management shall implement internal system safeguards to ensure users are held accountable for their actions. Individual application access authority is the responsibility of the application administrator. Where available, an automated audit trail shall be implemented that documents violations as follows:
1. The identity of each person and device having access.
2. The time of access.
3. The user's activities.
4. All activities that might modify, bypass, or negate safeguards.
5. All relevant actions associated with period processing.
6. Any changes to security level or categories of information.

C. **Audit and Reporting** – Where available, System Administrators shall maintain an audit trail so all actions affecting system security can be traced.

D. **Design Documentation** – IT Management shall maintain up-to-date system documentation to ensure all areas of the system are understood and thus protected from intrusion.

E. **Discretionary Access Control** – System Administrators shall restrict access to files based on the identity of individuals or defined groups of individuals, to protect them from unauthorized access and to limit propagation of access rights.

F. **Electronic Mail** – Electronic mail is primarily for business use. It is not to be used for the distribution of confidential information. It is not private and may be accessed by the state at any time. DAS IRMD Policy 03-12 governs the acceptable use of the state's electronic mail systems.

G. **Identification and Authentication** – System Administrators shall identify each individual user of the system prior to allowing activity on that system, and establish passwords to authenticate the user's identity.

H. **Internet Use** – Use of the Internet is for state business. DAS IRMD Policy 03-13 governs the appropriate use of the Internet.

I. **Labeling** – Users shall label all information media and media containers with identifying information that accurately reflects what the information is, its level of sensitivity, and the current date.

J. **Least Privilege** – System Administrators and application administrators shall ensure IT systems and applications function in a manner that allows each user to have access only to information to which the user is entitled and no more. Open-access applications, such as time sheets, etc., may be excepted. *Specifically, least privilege means that access is to be provided at the minimum level required for the user to perform their regular job duties.*

K. **Object Reuse** – System Administrators shall eliminate all residual information from a medium (page frame, disk sector, and magnetic tape) before reassignment of that medium from one subject to another.

L. **Users** – All users shall exercise good judgement, keeping in mind the particular sensitivity of the data, when sharing or reassigning media for reuse.

M. **Physical Controls** – Users shall protect hardware, software, documentation, and information from unauthorized disclosure, destruction, or modification.

N. **Remote Access** – Remote access to DAS owned computers must be approved by the appropriate Division Administrator and the CIO, prior to gaining access. Division Administrators shall assess each request and determine the risk, prior to requesting approval by the CIO. Documentation logs for all remote access must be maintained by the IT Security Personnel or Designee. All access to DAS systems must conform to DAS HRSD policy 50.050.01.

O. **Security Training and Awareness** – At the direction of the CIO, the DAS IT Security Designee shall establish a security training and awareness program that will ensure all users responsible for IT systems or information are aware of proper operational and security-related procedures. IT security-specific training may be delivered formally (individual or classroom) or through written communications.

IX. NETWORK SECURITY REQUIREMENTS

A. **Network Safeguards** – Necessary safeguards must be approved by the CIO, IT Management, and IT Security Personnel before any (internal or external) IT system is connected to the network.

B. **Network Security Architecture and Design** – An enterprise network must possess a coherent network security architecture and design. It should be developed with attention to security requirements, mechanisms, and assurances commensurate with the sensitivity of information being managed.

X. LIFE CYCLE MANAGEMENT

A. Planning

1. Planning for IT will incorporate the principles of life cycle management, providing a consistent and specific approach for determining short- and long-range objectives, documenting accomplishments, developing security, mapping proposals to budget requests, and assuring the implementation of appropriate cost-effective protective measures.

2. Operational security requirements are to be incorporated into all IT systems. Adequate internal controls are needed during IT planning and design so that the recording, processing, and reporting of information is properly performed during the operation of the system.

B. Internal Controls

1. Internal controls will ensure conformance with applicable security regulations, policy, and requirements.

2. Minimum accomplishments required during the life cycle management phase include:

   a. Working with IT Security Personnel, develop security specifications based on identified security requirements and consideration of potential threats and vulnerabilities.

   b. Identifying risk areas and definition of risk reduction measures, management approaches, and plans.

   c. Security testing and evaluation to certify that technical security features and other safeguards satisfy specified security requirements before the initiation of operational testing.

   d. Establishing procedures for ensuring the continuous use of approved security safeguards during the production and deployment phase.

   e. Ensuring security safeguards are in use during the operations and support phase.

   f. Ensuring IT compliance reviews are conducted annually to sustain optimal security levels.

PROCEDURES

I. IT POLICY DEVELOPMENT

Step	Responsible Party	Action
1.	IT Security Personnel	• Drafts IT Security Policy and sends to the Technical Council, the CIO, and Executive Staff for review and approval.
2.	Technical Council	• The Technical Council will review the IT security policies for appropriate content, and provide comment to the IRMD IT Security Personnel.
3.	Chief Information Officer (CIO)	• Receives input from the IT Security Personnel, approves final draft of the policy and sends to Executive Staff with recommendation.
4.	Executive Staff	• Reviews policy and either approves the policy or returns it to the IT Security Personnel for revision.

II. SYSTEMS SECURITY

Step	Responsible Party	Action
1.	IT Manager/Supervisor	• Notifies System Administrator of reassignment and access level of personnel or arrival of new employee within 24 hours.
2.	System Administrator	• Assigns system IDs and initial password. Verbally provides user with password requirements, and provides them with a copy of the IT Security Policy with the Computer Security User Declaration attachment.
3.	User	• Acquires ID and password in person from System Administrator and immediately changes password. • Reads IT Security Policy and signs the Computer Security User Declaration. • Returns signed Computer Security User Declaration to IT Security Personnel within three days of ID and password assignment.
4.	IT Manager/Supervisor	• Notifies System Administrator of moving or departing personnel within 24 hours of scheduled departure, unless otherwise directed by DAS Personnel Division.
5.	System Administrator	• Remove departing personnel from all system access within 24 hours of notification, or as directed by the CIO, or DAS Personnel Division.

III. PHYSICAL SECURITY

Step	Responsible Party	Action
1.	IT Manager/Supervisor	• Provides DAS Facilities Division with a written request for building access/computer room access.
2.	Facilities Personnel	• Creates necessary access in video badge system and assigns photo ID.
3.	IT Manager/Supervisor	• Receives notification of departing personnel by the Facilities Division within 24 hours of the individual's departure, or as directed by DAS Personnel Division.

4.	Facilities Personnel	• Removes departing personnel from building/computer room access within 24 hours of notification, or as directed by the CIO or DAS Personnel Division.

IV. IT PERSONNEL AND VENDOR CLEARANCES FOR COMPUTER ROOM AND SYSTEMS ACCESS

Step	Responsible Party	Action
1.	IT Manager	• Notifies LEDS in writing of new IT personnel assignment. Requests background check.
2.	LEDS	• Performs background check, and notifies hiring manager in writing of results.
3.	Project Manager	• Notifies LEDS in writing of request to perform a vendor background check.
4.	LEDS	• Notifies Project Manager of background check results.

V. INCIDENT REPORTING

Step	Responsible Party	Action
1.	Employee/User	Reports security incidents immediately by contacting the IT Security Personnel or Designee. Incident reports may be received both verbally and in writing and shall be investigated by the IT Security Personnel within three days, or as directed by the CIO or DAS Personnel Division.
2.	IT Security Personnel	Notifies the CIO of all significant security incidents. Maintains a procedure for investigating security incidents and keeps a permanent record of all such incidents.

COMPUTER SECURITY USERS DECLARATION

I declare that I have read the Department of Administrative Services Information Technology Security Policy. Furthermore, I understand that I shall:

Use passwords and keep them secret.

Create passwords that are at least seven characters long, have both letters and numbers, that do not spell a word or a name, and do not contain personal data.

Use passwords that consist of both numbers and letters.

Protect sensitive data/information by following applicable policies and procedures.

Protect my computer by logging off when I am gone for the day or for extended periods of time.

Protect equipment assigned to me by keeping it safe from harm.

Scan all computer disks from home and external sources for viruses before I use them on my computer.

Not install any software unless authorized to do so.

Use only authorized hardware and software.

Protect my work area, media, and files, against all threats and report any incidents that occur to the CIO, IT security personnel, or designee.

Not download software from the Internet unless specifically authorized to do so by the CIO or designee.

Comply with all applicable laws and organizational policies and procedures.

_____ _____

Employee Date Agency Authority Date

I agree that by signing this document I am declaring that I have read and understand the Information Technology Security Policy and Procedure, and that if I fail to follow mandatory requirements outlined in the Policy or Procedure that I may be subject to personnel action or dismissal.