



**ato**  
AIR TRAFFIC ORGANIZATION

# EN ROUTE AUTOMATION MODERNIZATION (ERAM) Rules of Behavior

Version 1.0

February 29, 2008

---

Prepared by:

Federal Aviation Administration  
ERAM Security

## Table of Contents

<b>1.0 Introduction.....</b>	<b>1</b>
1.1 Responsibilities .....	1
<b>2.0 Other Policies, Procedures, and Directives.....</b>	<b>3</b>
<b>3.0 Application Rules .....</b>	<b>3</b>
3.1 Training.....	3
3.2 ERAM Access by Nonusers.....	3
3.3 Telecommunication.....	4
3.4 Remote Access.....	4
3.5 Internet Usage .....	5
3.6 Electronic Mail (E-Mail).....	5
3.7 Software Copyright Licenses .....	5
<b>4. Appropriate Use .....</b>	<b>6</b>
4.1 User Identification and Password Responsibilities.....	6
4.1.1 ATC User Account Management.....	7
4.1.2 ATC User Password Expiration.....	7
4.1.3 ATC Supervisor Account Management Responsibilities .....	7
4.2 ERAM and Other Systems Interconnections .....	8
4.3 Circumventing Security Measures .....	8
4.4 Reporting Security Weaknesses.....	8
4.5 Protecting ERAM Security Controls .....	9
<b>5. Role-Based Access Controls.....</b>	<b>9</b>
<b>6. Employee Termination .....</b>	<b>9</b>
<b>7. Noncompliance .....</b>	<b>10</b>
<b>8. Information Technology Professionals and Users with Elevated (Administrator) Rights: .....</b>	<b>10</b>
<b>ACKNOWLEDGEMENT: .....</b>	<b>10</b>
<b>APPENDIX A    Acronyms.....</b>	<b>11</b>

# **En-Route Automation Modernization Rules of Behavior**

## **1.0 Introduction**

It is the responsibility of each user to assure the confidentiality, integrity, and availability of En Route Automation Modernization (ERAM) information, and information systems. The ERAM Rules of Behavior are to be followed by all ERAM users. These rules are to be made available to every user upon successful completion of ERAM training and at least on an annual basis. These rules shall also govern the actions of non-ERAM personnel given access to ERAM information systems.

Rules of Behavior are part of a comprehensive program to provide complete information security. These guidelines are established to hold users accountable for their actions and hold users responsible for information security. Rules of Behavior establish standards of behavior in recognition of the fact that knowledgeable users are the foundation of a successful security program. Users need to understand that taking personal responsibility for the security of their system and the information it contains is an essential component of their job.

These Rules extend to all Federal Aviation Administration (FAA) Air Traffic Organization (ATO) personnel and any other persons using ATO systems or accessing FAA ATO systems under formally established agreements. This includes any FAA or Department of Transportation (DOT) employee, contractor, subcontractor, consultant, and other federally funded users. All users should be fully aware of, and abide by, FAA security policies as well as related Federal policy contained in the Privacy Act, and Freedom of Information Act.

## **1.1 Responsibilities**

The Information Systems Security Officer (ISSO) is responsible for ensuring that an adequate level of protection is afforded ERAM by applying an appropriate combination of technical, administrative, and management controls. FAA Order 1370.82A enumerates the duties of the ISSO. The ISSO is responsible for assuring that vulnerability analyses of representative segments of ERAM are conducted at least annually. Analysis is required whenever major system upgrades are performed to determine if existing and planned security controls are sufficient to counter present and anticipated threats in an ever-changing information systems environment. The ISSO will devote close attention to those new and evolving technologies, systems, and applications that have the potential to uncover vulnerabilities in the ERAM security posture.

The William J. Hughes Technical Center (WJHTC) is responsible for providing second-level support for System Management, System Maintenance activities, and ERAM system engineering. Additionally, it is the responsibility of the WJHTC to review, investigate, and provide incident response for all received security alerts. Security alerts that impact the mission of ERAM, impact other National Airspace System (NAS)

ERAM Rules of Behavior

systems, or affect NAS safety must be reported to DOT Cyber Security Management Center (CSMC) and Security Information Group (SIG).

The Site Manager (SM) at each ARTCC will assist the ISSO in administering the ERAM security program, as directed by FAA Order 1370.82A and the ERAM Security and Policy Procedures Document.

The site System Security Administrator (SA) will perform all prescribed duties. This includes such duties as;

- The creation, modification, and deletion of user accounts
- The assignment of user privileges based on the concepts of role-based access and least privilege
- Issuance of initial user passwords
- The acknowledgement of security alerts received at the Monitor and Control (M&C) station
- Audit log maintenance, to include log rotation and shipping security alerts and system logs received in the Operational Environment to the WJHTC in accordance with established procedures.

Each user will adhere to the procedures contained in the Rules of Behavior. If users subject to these procedures have suggestions for improving security procedures, technical measures, or security controls, they should consult their SM.

The ERAM Site Manager for this facility is

(Name) \_\_\_\_\_

(Organization)\_\_\_\_\_

(Telephone number)\_\_\_\_\_.

The ERAM site System Security Administrator for this facility is

(Name) \_\_\_\_\_

(Organization)\_\_\_\_\_

(Telephone number)\_\_\_\_\_.

The Information System Security Officer for this system is

(Name) Tayo Olagunju\_\_\_\_\_

(Organization) ATO-E\_\_\_\_\_

(Telephone number) 202.385.8376\_\_\_\_\_.

## 2.0 Other Policies, Procedures, and Directives

The Rules of Behavior do not supersede or negate existing policy documents. The Rules of Behavior support and supplement the objectives of those directives by defining key rules and behaviors each user must observe while interacting with ERAM. The rules are consistent with the applicable laws, regulations, circulars, publications, orders, standards, handbooks, and documentation identified below:

- The Freedom of Information Act, as amended in 2002, 5 U.S.C. § 552
- Federal Information Security Management Act (FISMA) of 2002, Public Law 107-347, Title III
- Federal Information Processing Standards Publication (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004
- FIPS 140-2, Security Requirements for Cryptographic Modules, May 2001
- NIST Special Publication (SP) 800-53, Recommended Security Controls for Federal Information Systems, February 2005
- Office of Management and Budget (OMB) Memorandum M-06-16, Protection of Sensitive Agency Information, June 23, 2006
- The Privacy Act of 1974, as amended by The Computer Matching and Privacy Protection Act of 1988; 5 U.S.C. § 552a, and § 208 of the E-Government Act
- OMB A-130 Circular, Appendix III:  
[http://www.whitehouse.gov/omb/circulars/a130/a130appendix\\_iii.html](http://www.whitehouse.gov/omb/circulars/a130/a130appendix_iii.html)
- OMB, *Security of Federal Automated Information Resources*, Appendix III to OMB A-130, Management of Federal Information Resources, November 28, 2000
- *Homeland Security Presidential Directive/HSPD-7*, December 17, 2003
- FAA Order 1370.82A, *Information Systems Security Program*, September 11, 2006
- FAA Order 1370.97, *FAA Use of Non-FAA Workstations*, April 15, 2007

## 3.0 Application Rules

This section outlines how to apply the Rules of Behavior to ERAM users

### 3.1 Training

In addition to annual FAA Security and Hazardous Materials Security Awareness Virtual initiative (ASHSAVI), all users must receive task-oriented performance and security training prior to being granted access to ERAM.

### 3.2 ERAM Access by Nonusers

Law enforcement, regulatory, and government oversight personnel may require access to ERAM in the performance of their duties. The ISSO or SM will advise such persons of the Rules of Behavior and solicit their cooperation in adherence to those rules. The NAS

## ERAM Rules of Behavior

Change Proposal process must be followed before access is granted to ERAM. When access by any agency or interagency group exceeds twenty (20) working days, the SM will designate as a user, each individual from such an agency or group who requires access to ERAM. The ISSO will grant such persons continued access to ERAM, upon execution of the Rules of Behavior. The ISSO will terminate such access when the Administrator, FAA, or a designee and a responsible representative of the external agency agree that access to ERAM by its personnel is no longer required.

### 3.3 Telecommunication

The FAA Telecommuting Handbook addresses a supervisor's authority to permit specific persons to perform assigned duties outside the normal office setting. The directive stipulates that such arrangements meet all of the following criteria:

1. Supervisors and employees must agree to the terms of the working arrangement and record this agreement in writing.
2. The agreement must identify the site(s) at which telecommuting work will be performed.
3. The agreement must contain telephone contact information.
4. The agreement must describe the telecommuter's work schedule.

There is no requirement, concept of operations, or policy supporting telecommuting by personnel using or maintaining ERAM.

### 3.4 Remote Access

Remote access in ERAM is limited to the ERAM support network at the WJHTC and support network at the ARTCCs. All remote access from outside of the ERAM support network must originate from the WJHTC. Remote access communications to the ARTCC support network from the WJHTC support network must pass through the WJHTC support router. **Remote access to the ERAM operational network is prohibited.**

Remote Access must be via authorized access methods. The current authorized access method to the Mission Support/Administrative networking environment is Virtual Private Network (VPN) issued by [FAA Telecommunications Infrastructure Program \(FTI/FRAC\)](#)

- Take precautions to secure government information and information resources.
- Do not alter the configuration, including installing software or peripherals, on government equipment unless authorized.
- Use only authorized licensed software on government equipment; do not violate Federal copyright laws.
- In accordance with [FAA Order 1370.97, FAA Use of Non-FAA Workstations](#):
  - Adhere to all provisions or agreements related to off-site work.

## ERAM Rules of Behavior

- Use virus protection software on off-site systems and keep it up-to-date.

The WJHTC provides the authority to allow users remote access to ERAM support system components for FAA employees or contractors from their home or office. Remote access has been included into the system design to provide access to second-level support maintenance activities for security administrators who are not physically located near ERAM components. This logical service is protected by several layers of restrictive controls. These layers include specific hardware and applications to communicate securely with ERAM components and user identification and authentication mechanisms to register valid users. Perimeter networking devices will allow or deny communications destined for ERAM or requests from unauthorized sources.

Remote Access provides:

- Remote access to the ERAM support network for properly-cleared users only from Government-Furnished Equipment, which contains the necessary software and hardware needed to connect remotely
- The ability to work remotely in emergency, contingency, or Disaster Recovery situations
- A scan of the user's computer-security profile prior to allowing access of any kind to ensure at least the bare essential security components and configuration are in place.

Remote access users agree to protect the privacy and security of all ERAM data and equipment in the same manner as required when working at the office.

### **3.5 Internet Usage**

Access to and from the Internet from ERAM operational network assets is prohibited. Access to the Internet using ERAM support systems is authorized only through the FTI/FRAC remote access point and is restricted to only allow communications into ERAM through a Virtual Private Network connection using Government-Furnished Equipment. ERAM design, system software, and security controls do not allow ERAM support assets access to the Internet outside of the VPN connection.

### **3.6 Electronic Mail (E-Mail)**

User e-mail is not allowed, enabled, or supported on ERAM.

### **3.7 Software Copyright Licenses**

The WJHTC is responsible for maintaining, obtaining, and procuring required licenses and informing users of license requirements. Specific questions regarding software copyright licenses will be addressed to the WJHTC. Software not provided by the WJHTC is prohibited on ERAM.

## 4. Appropriate Use

ERAM hardware and software are for official government purposes. A user is authorized access to ERAM information resources for official purposes only and will receive access only after completing ERAM training. All activities not expressly permitted or prohibited, include, but are not limited to, the following:

- Taking information from ERAM for personal use, whether for profit, or any other purpose, or no purpose at all.
- Disclosing information about ERAM (or allowing it to be disclosed) to a nonuser without prior authorization.
- Using ERAM to store or develop personal information, such as address lists or data used in a personally-owned business, consulting business, or a second job.
- Use of ERAM communications features for political or other, non-business purposes, particularly any material any reader may find offensive.
- Using ERAM to record and store personal contact information for immediate family members, physicians, clergy, child or adult care providers, veterinarians, auto repair specialists, etc. Users are cautioned that personal information they record in message or word processing files are neither afforded nor eligible for privacy protection.
- No personal information will be downloaded to ERAM from any other system.

### 4.1 User Identification and Password Responsibilities

A user may not disclose his/her personal user identification or password or those of any other user to any person without the prior permission of the SM. A user may not allow another person to use an identification card or device designated for his/her personal use without the prior permission of the SM. In accordance with FAA Order 1370.92, passwords must meet the following criteria:

- The password must not contain all or part the user's account name
- The password must not repeat two characters in succession.
- The password must be at least eight characters in length and contain characters from three of the following four categories:
  - ⇒ English uppercase characters (A through Z)
  - ⇒ English lowercase characters (a through z)
  - ⇒ Base 10 digits (0 through 9)
  - ⇒ Non-alphabetic characters (e.g., !, \$, #, %)

Passwords will be changed at least every 180 days. Previously-used passwords cannot be reused for a minimum of a thirty-month period. Users are required to protect their passwords and other account information to the best of their ability. Users are prohibited from storing passwords in non-electronic form, to include, but not limited to, recording passwords on "Post-Its" or other loose paper items, taping the password beneath the keyboard or mice or on displays and sharing passwords with colleagues. In accordance

## ERAM Rules of Behavior

with FAA Order 6000.15D, user sessions will be locked out after three unsuccessful login attempts. ERAM users must contact the SA to unlock locked accounts.

Users are required to change their passwords before taking extended leave lasting longer than 15 days to avoid possible account lockout while they are away.

### **4.1.1 ATC User Account Management**

ATC users must contact their supervisor to create an account to access ERAM information systems. The following password characteristics are required for the ATC user's strong password before access is granted to AT Specialist workstations.

- Minimum length of eight characters
- Maximum length of 12 characters
- All alphabetic characters must be upper-case
- Must contain two or more numeric characters
- Must contain two or more alphabetic characters
- Must contain one or more special characters
- If the first character is numeric, the first three characters must be numeric
- If the last character is numeric, the last three characters must be numeric

When a strong password is first created for a user profile, the first 5 characters must be alphanumeric, because they will be used to initialize the user's simple password. The remaining 3 to 7 characters must be alphanumeric or one of the special characters defined in special characters.

Before taking leave it is the responsibility of the ATC user to change their strong password. This is accomplished by notifying the ATC user's Supervisor that a password change is needed.

In the event that an ATC user forgets, or has suspicion that their account information has been compromised, the user must immediately notify their Supervisor.

### **4.1.2 ATC User Password Expiration**

The ATC user will receive a warning message 30 days prior to the expiration of the strong password. If an ATC user fails to change the strong password prior to the expiration date and the expiration date has been reached or exceeded and the user attempts to login, the login will fail and a warning message will remind the user to change their password. ATC users must change their strong password after the expiration date has passed before access to ERAM is granted. There is no expiration date for ATC user simple passwords.

### **4.1.3 ATC Supervisor Account Management Responsibilities**

The Supervisor is responsible for investigating and correcting ATC user account incidents. The Supervisor is also responsible for enforcing password changes on an ATC user on a non-active sector before relieving the current ATC user. The use of account

## ERAM Rules of Behavior

information that does not belong to the ATC user to log the ATC user into ERAM is prohibited.

### **4.2 ERAM and Other Systems Interconnections**

The ISSO will review the NAS Change Proposals regarding the interconnections of systems documentation. The ISSO will verify that written Memorandums of Understanding (MOU) and/or Memorandums of Agreement (MOA) are developed jointly between the WJHTC and the connecting system. The MOUs and/or MOAs will be approved prior to authorization of any interconnection of any system to ERAM. If the MOUs and/or MOAs do not exist, the ISSO will recommend to the WJHTC that such interfaces not be authorized or established; and, if currently in place, the interface will be disconnected.

A user may not connect ERAM to any other information system without prior permission of the ISSO.

### **4.3 Circumventing Security Measures**

Except as directed by the ISSO or SM for the purpose of testing and validating ERAM security controls, users will not attempt to circumvent any ERAM procedural or technical measures used to protect the security of the system and the information it contains.

### **4.4 Reporting Security Weaknesses**

ERAM users are obligated to report any discovered or noted technical or procedural security weaknesses as soon as possible, to the SA WJHTC helpdesk, and ISSO. The WJHTC helpdesk phone number is 1(800) 377-0308 and is staffed 24/7.

- Report security incidents, or any incidents of suspected fraud, waste or misuse of FAA systems to appropriate officials.
- For Administrative and Mission Support Systems, if you have any reason to believe that security has been or could be compromised; notify your manager, System Administrator, Information Systems Security Officer or the helpdesk immediately. If you are unable to contact any of the above, report the situation to the [Cyber Security Management Center \(CSMC\)](#) or 866-580-1852, option 1.
- For NAS systems contact the appropriate person in your incident management chain, who should in turn contact the Security Information Group (SIG). If you are unable to contact anyone in your incident management chain, report the incident directly to the SIG at 9-ATOW-HQ-SIG/AWA/FAA or 202-385-4427.
- No matter how unsure you are, report your suspicions, because what you know may fit with other pieces of information to help resolve an issue or avoid one. When in doubt, report it! Be prepared to describe the circumstances under which the incident occurred, including the date and time, any people involved, and any other information that could help mitigate the potential damage to the system.

## **4.5 Protecting ERAM Security Controls**

An ERAM user may not divulge to non-ERAM users specific information concerning ERAM security equipment, software, or procedures in effect or proposed for adoption.

## **5. Role-Based Access Controls**

To limit damage in the event that the ERAM security procedures fail, the SA and the SM control user access to any given object (e.g., a data file) and the actions each user is permitted to perform on that object. The SA and the SM will determine the permissions granted to each user, based on the roles that the user is required to perform. Each ERAM user will perform only those tasks he/she is authorized to perform. A user will not attempt to perform tasks the user is not specifically authorized to perform. If a user believes a particular separation of duties hinders mission accomplishment, the user will bring the matter promptly to the attention of their supervisor.

Security is an important consideration for ERAM architecture and design. The ERAM security service is a logical grouping of related functions that provide identification, authentication, access control, security- relevant event logging, audit, integrity checking, encryption/decryption, and network security. These functions are grouped into Platform Security and Perimeter Security.

ERAM utilizes a role-based, access- control system to ensure that data and information are available to users who meet established criteria. The implementation of role-based access control assigns users to groups, and each group is allowed designated privileges. Users responsible for a specific region only have access to resources covered in that specific region. Users responsible for the entire region have access to all resources in all regions. All logged-on users have a profile associated with him/her. The user profiles associate each user ID with the appropriate control commands he/she is authorized to execute. The user has access only to those commands that he/she is authorized to execute.

The identity and contact information regarding the ISSO, SA, and SM is located at the local site where the individual is assigned.

The local site policy and procedures document addresses the duties and actions required to ensure security is enforced and maintained,

## **6. Employee Termination**

ERAM Security Management and Administration are required to review and reauthorize all accounts on an annual basis. Accounts inactive for more than one month are identified on a monthly basis and are disabled or deleted following coordination with the account owners and managers.

As a standard practice and as part of his/her account management and security administration duties, the ERAM SA ensures that procedures for both friendly and unfriendly termination of employees are followed.

## ERAM Rules of Behavior

Friendly termination of an ERAM employee is expected regularly and follows normal in-processing/out-processing. The in-processing/out-processing checklist requires the individual to be cleared by the SA.

Unfriendly termination requires immediate removal of an employee under involuntary or adverse conditions. As soon as removal of an individual under unfriendly termination is determined, the Site Manager (SM) notifies the System Security Administrator (SA). The SA is responsible for removing or deactivating the user account.

## 7. Noncompliance

Users who do not comply with the prescribed ERAM Rules of Behavior are subject to actions in accordance with existing policy and regulations, applicable union contracts or applicable Table of Penalties (contained in [FAPM 2635, Conduct and Discipline](#) or [Standards of Conduct ER-4.1](#)). These penalties include official, written reprimands, suspension of system privileges, temporary suspension from duty, removal from current position, and termination of employment. FAA will enforce the use of penalties against any user who willfully violates any [FAA/ATO or Federal system security policy or order](#) as appropriate.

## 8. Information Technology Professionals and Users with Elevated (Administrator) Rights:

In addition to the above rules, you must ensure that any elevated privileges granted to you for the purpose of performing your work assignments are not misapplied in order to gain access to information systems or to install unauthorized hardware or software. You occupy a position of trust and shall not erode the confidence placed in you by the FAA. Any evidence of such abuse will result in appropriate disciplinary action.

For disciplinary action, refer to Section 7 of this document “Noncompliance”

### ACKNOWLEDGEMENT:

I acknowledge receipt of and understand my responsibilities and obligation to comply with these ERAM Rules of Behavior.

---

Signature of User

---

Date

**APPENDIX A      Acronyms**

<b>ACRONYM</b>	<b>DEFINITION</b>
ARTCC	Air Route Traffic Control Center
ASHSAVI	Annual Security and hazardous Materials Security Awareness Virtual Initiative
AT	Air Traffic
ATC	Air Traffic Control
ATM	Air Traffic Management
COOP	Continuity of Operations Planning
COTS	Commercial off-the-shelf
CSMC	Cyber Security Management Center
DOT	Department of Transportation
E-Mail	Electronic Mail
ERAM	En Route Automation Modernization
FAA	Federal Aviation Administration
FIPS	Federal Information Processing Standards Publication
FISMA	Federal Information Security Management Act
FRAC	FTI Remote Access Capability
FTI	FAA Telecommunications Infrastructure
I&A	Identification and Authentication
IAW	In Accordance With
ISSO	Information Systems Security Officer
M&C	Monitor and Control
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
NAS	National Airspace System
NIST	National Institutes of Standards and Technology
OMB	Office of Management and Budget
SIG	Security Information Group
SM	Site Manager
RA	Remote Access
SA	Site System Security Administrator
SSH	Secure Shell
WJHTC	William J. Hughes Technical Center