TRAFFIC FLOW MANAGEMENT SYSTEM (TFMS)

Thin Client User Account Request Form for:

National Traffic Management Log & Flight Schedule Monitor (NTML & FSM)

- **INTENDED FOR AND LIMITED TO FAA FACILITIES THAT MAY NOT REQUIRE A FULL TFMS REMOTE SITE; AND DO NOT HAVE OPERATIONAL CONNECTIVITY TO TFMS**
  Submit signed form to 9-AWA-TFMS-Accounts@faa.gov
- **If you have an account previously opened, please contact the TPC at (609) 485-9601 or email 9-ACT-TPC@faa.gov for further assistance.**

ACCOUNT ACTION: ☐ Create ☐ Remove

USER INFORMATION		
Last Name:	First:	M.I.:
Title:	Phone:	Email:
ORGANIZATION INFORMATION		
Organization/Company Name:		Location:
SUPERVISOR/POC INFORMATION		
Last Name:	First:	M.I.:
Title:	Phone:	Email:
SIGNATURE		Date:
ORGANIZATION INFORMATION		
Organization/Company Name:		Location:
----------GOVERNMENT ONLY----------		
☐ **NTML**	☐ **FSM**	
Justification:		
---------- FAA Use Only Below This Line ----------		
APPROVAL		
Account creations and deletions must be signed below before any system changes can be made.		
FAA Approver		Title
Signature		Date
Notes:		

RULES OF BEHAVIOR

The rules of behavior contained in this document are to be followed by all users of the TFMS. Users will be held accountable for their actions on any TFMS component. If an employee violates TFMS policy regarding the rules of the TFMS system, they may be subject to disciplinary action at the discretion of FAA management. Actions may range from a verbal or written warning, removal of system access for a specific period of time, reassignment to other duties, or termination, depending on the severity of the violation.

Work at home - It is against TFMS policy to conduct any official work at home, using any TFMS network access, such as remote access, Telnet, FTP, VPN, or dial-in access. Data also must not be copied from a TFMS resource using removable media (i.e., flash drives, CDs, DVDs, floppy disks, etc.) for transfer to a user's home computer system.

Dial-in/Remote Access - No dial-in or remote access is used to access TFMS, except in the case of authorized external sites, using secure VPN connections. However, if a justifiable need occurs, the TFMS Program Manager may authorize dial-in access to a TFMS system. It is understood that dial-in access would pose additional security risks, but may become necessary for certain job functions. If dial-in access is allowed, the TFMS ISSO will regularly review system audit logs and TFMS phone records, and conduct spot-checks to determine if TFMS business functions are complying with controls placed on the use of dial-in lines. All dial-in calls will use one-time passwords.

Connection to the Internet - Some TFMS personnel has access to the Internet. Access to the Internet should be closely controlled by the ISSO. TFMS divisions, staff managers, and technicians should know that only TFMS-authorized Internet connections will be allowed, and that all connections must conform to TFMS' security and communications architecture, and the TFMS Information System Security Plan (ISSP). All Internet activity is for official TFMS business only.

Protection of copyright licenses (software) – LAN and PC users are not to download LAN-resident software. Audit logs will be reviewed to determine whether employees attempt to access LAN servers on which valuable, off-the-shelf software resides, but to which users have not been granted access. Audit logs will also show users' use of a "copy" command; this may indicate attempts to illegally download software. Unauthorized copying of PC-based software is also prohibited.

Unofficial use of government equipment – Users should be aware that personal use of information resources – LAN and PC – is not authorized. This also includes connections to the Internet. Users may only access Websites and information from the Internet that is for official use only, related to users' authorized job functions. Users are prohibited from "surfing" the Web for personal reasons, including the sending and receiving of personal email.

Use of passwords – Users are to use passwords as specified by FAA Order 1370.92, which includes a mix of eight (8) alpha, numeric, upper/lowercase, and special characters. Users are to keep passwords confidential and are not to share passwords with anyone. Passwords are also to be changed every 90 days, and the same ones are not to be reused for a history of 5 password changes.

System privileges – Users are given access to TFMS based on a need to perform specific work. Users are to work within the confines of the access allowed and are not to attempt access to systems or applications to which access has not been authorized. Auditing will be conducted on a regular basis, and unauthorized access attempts will be addressed by the ISSO.

Individual accountability – Users will be held accountable for their actions on TFMS. This is stressed during computer security awareness training sessions.

Restoration of service – The availability of the LAN is a concern to all users. All users are responsible for ensuring the restoration of services in the event the LAN is not operational.

I acknowledge receipt of, understand my responsibilities, and will comply with the Rules of Behavior for TFMS.

Printed Name of TFMS User	Signature of User	Date