

Procedure Guide for the Multifunction Arc Jet Instrumentation and Computation (MAJIC) System TSF-06-018

National Aeronautics & Space Administration

Ames Research Center

Moffett Field, CA

Issue Date: 7-16-2012
Effective Date: 7-16-2012



National Aeronautics and
Space Administration

THIS PAGE LEFT INTENTIONALLY BLANK

Document Change History

Date	Author	Description
7-16-06	S. Eddlemon	Initial Baseline
2-18-09	S. Eddlemon	Updated to incorporate IT Security requirements for Moderate Systems.
7-13-12	M. Cohen	Added Rules of Behavior

TABLE OF CONTENTS

1	Introduction.....	1
2	Consequences for Violation of Rules	1
3	User Accounts & Access	1
3.1	Account Philosophy	1
3.2	Prerequisites Required to Obtain Accounts	1
3.3	Process for Obtaining Access to Lab Systems.....	1
3.3.1	Requests	1
3.3.2	Issue	1
3.3.3	Review Process	2
3.3.4	Checkout	2
3.4	Process for Accessing the System Remotely	2
3.5	Physical Access.....	2
3.5.1	External Entities.....	2
4	Data and Information Management	2
4.1	Types of Information Allowed on the System.....	2
4.2	Authorized Uses for Information	2
4.3	Distribution Restrictions	3
4.3.1	Media Access Control.....	3
4.4	Data/Media Labeling	3
4.4.1	Data/Media Disposal.....	3
4.5	Information Sharing.....	3
5	Authentication & Access Control	3
5.1	Password Requirements.....	3
5.1.1	Procedures for Changing.....	4
5.1.2	Lost Password	4
5.1.3	Procedures for Compromise	4
5.1.4	Administrative Default Passwords.....	4
5.2	Invalid Access Attempts	4
5.3	Access Scripts	4
6	Logging & Auditing.....	4
6.1	Logging Philosophy	4
6.2	Accountability.....	4
6.2.1	Forensics	4
6.2.2	Support for Accountability & Audit Trails.....	5
6.3	Audit Timing.....	5
6.4	Log Retention.....	5
7	System Maintenance & Configuration.....	5
7.1	Flaw Remediation	5
7.2	Remote Maintenance	5
7.3	Configuration Settings	5
7.3.1	System Services	5
7.3.2	Software Restrictions	6
7.4	Virus Mitigations	6
7.5	Non Government owned systems	6
8	Incident Handling & Reporting	6

1 Introduction

This document describes the policies and procedures that govern Multifunction Arc Jet Instrumentation and Computation (MAJIC) system.

2 Consequences for Violation of Rules

Violations of rules of system or NASA policy will result in sanctions for failure to comply. For any type of violation, the first violation will result in verbal warning. The second violation of a similar type may result in written warning. The third violation of a similar type may result in loss of access privileges and potential personnel actions. Sufficiently egregious violations may result directly in loss of access, personnel action and/or criminal prosecution without requiring prior verbal or written warning. Consequences are at the discretion of NASA or contractor management.

3 User Accounts & Access

3.1 Account Philosophy

All users and system administrators will be granted the least access necessary to fulfill project goals. Each user shall have a unique user ID. Temporary and emergency accounts are not permitted.

3.2 Prerequisites Required to Obtain Accounts

- The requestor must have a project requirement or related deliverable before access will be considered.
- All individuals with access to lab systems will complete SATERN training prior to account creation.
- All individuals with access to lab must be US Citizens
- All individuals with access to lab systems will be members of the Thermophysics Facility Branch, either Civil Servant or Support Service Contract.

3.3 Process for Obtaining Access to Lab Systems

3.3.1 Requests

- Requests for access to the MAJIC system must be submitted and approved through the NASA Account Management System (NAMS). In NAMS, the application name is "ARC ArcJet Data Acquisition System" and its resource ID is 10454.

3.3.2 Issue

- Accounts will be provisioned only after the NAMS request has been fully approved. Accounts will be created by the MAJIC Domain Administrator and

users will be granted the minimum level of access necessary to achieve the goals of the user's task or project.

3.3.3 Review Process

- All accounts will be reviewed at least annually by system owner or designee

3.3.4 Checkout

- Upon completion of a project or task, all accounts granted to a user will be disabled for 3 months, after which they will be removed. All data related to the account or user may be retained indefinitely.
- Upon notification from ARC checkout system of termination or transfer, user accounts will be immediately disabled

3.4 Process for Accessing the System Remotely

- Remote access is disallowed.

3.5 Physical Access

- Physical access to the Arc Jet Complex is restricted to US citizens.
- Visitors must be escorted
- Visitors entering restricted areas must sign in. Upon exit, visitors must record time of departure.
- Unsupervised access requires authorization of the system owner.

3.5.1 External Entities

External Entities are not allowed access to the network or systems. Systems and network is contained within the Arc Jet Complex of Facilities (buildings N234 and N238).

4 Data and Information Management

4.1 Types of Information Allowed on the System

Information on the MAJIC Systems shall be limited to that data collected during the course of the Arc Jet Test and any programs necessary to reduce that data. All of which is necessary for completion of tests.

4.2 Authorized Uses for Information

Information will be used only for the purpose for which it was gathered or collected.

4.3 Distribution Restrictions

Data collected during tests conducted in the Arc Jet Complex shall be reduced to engineering units. Written permission from the system owner or designee is required prior to distribution or disclosure of output from data systems in any form (printed, cd-rom, USB Key, etc.) to individuals outside the project.

4.3.1 Media Access Control

- Printed or electronic information is given to the Test Engineer for their particular test only.
- Archived data shall be kept on the System for future possible data reduction if needed by the Test Engineer or test program which owns the data. This data is only accessible by Authorized System personnel.
- Media containing data from the Arc Jet Complex will not be transported outside of NASA facilities without written authorization from the particular Test Engineer or test program which owns the data.

4.4 Data/Media Labeling

Data will be labeled and handled according to the classification of the data and NASA policy

4.4.1 Data/Media Disposal

- When computers are excessed, all media must be degaussed, wiped, or damaged beyond recovery before removal from the Test Facility in accordance with NASA & ARC Policies.
- Hard copies of any data related in any way to the Test Facility will be shredded before disposal.
- CD's are to be shredded and hard drives are to be drill pressed or similarly destroyed.

4.5 Information Sharing

The procedures and policies for the sharing of information gathered and reduced, shall follow all procedures specified in the Test Planning Guide, (Document Number A029-9701-XM3), and any additional requirements specified in the Test Plan.

5 Authentication & Access Control

5.1 Password Requirements

Passwords to Facility systems will not, under any circumstances, be saved in an unencrypted format on any computer system, at any time. Passwords are transmitted and stored with one- way encryption to prevent anyone (including the System Administrator) from reading the clear-text passwords, passwords are encrypted while in transmission, and must follow password requirements of NASA policy.

5.1.1 Procedures for Changing

Passwords shall be changed on a 60 day period by the Authorized User.

5.1.2 Lost Password

Lost or forgotten passwords require a verbal request for change to the Domain Administrator.

5.1.3 Procedures for Compromise

Any possible password compromise must be communicated to the Facility ISSO immediately upon discovery or suspicion.

5.1.4 Administrative Default Passwords

Before adding an IT component to the MAJIC Domain, the administrator must demonstrate to the ISSO that factory configured passwords have been changed. This is usually accomplished by demonstrating failed logins for the factory installed users.

5.2 Invalid Access Attempts

After 3 unsuccessful access attempts, the user account is disabled. Re-enabling normally requires Domain Administrator action.

5.3 Access Scripts

Any type of program, script, or other automation that facilitates authentication by way of storing credentials on a computer system and presenting them automatically without user intervention is prohibited.

6 Logging & Auditing

6.1 Logging Philosophy

All user actions will be logged and auditable when possible.

6.2 Accountability

The audit trail provides accountability by providing a trace of user actions associated with a unique user identifier, a system node identifier, and a unique password known only to the user.

6.2.1 Forensics

- The audit trail supports after-the-fact investigations of how, when, and why events occur.
- The audit trail includes sufficient information to establish what events occurred and who (or what) caused them. In general, an event record specifies:
 - Type of event

- o When the event occurred
 - o User ID associated with the event
 - o Program or command used to initiate the event
 - o Hostname or other system identifier
- In the event of any suspected security problem, refer to the MAJIC Incident Response Plan for directions. That plan ensures compliance with the NASA guidance and appropriate coordination with the NASA Security Operations Center.

6.2.2 Support for Accountability & Audit Trails

Users utilize unique userIDs.

6.3 Audit Timing

- On a regular basis a system administrator will audit logs of the entire MAJIC Domain.
- Security configurations of physical and logical access control will be evaluated following any personnel changes within the Test Facility Personnel.

6.4 Log Retention

Audit data and system logs will be retained for a minimum of one year.

7 System Maintenance & Configuration

System maintenance will be performed regularly and in accordance with vendor recommendations.

7.1 Flaw Remediation

- When flaws, bugs, misconfigurations, or other inaccuracies are identified in the MAJIC system components, the individual identifying the issue will correct or report the issue in a timely fashion. If the issue poses a significant security risk, a temporary workaround to eliminate the vulnerability will be employed (i.e. disabling the affected services until a software patch is available).
- System administrators will subscribe to security related email distribution lists relevant to the technologies being evaluated or utilized.
-

7.2 Remote Maintenance

Remote maintenance is not permitted.

7.3 Configuration Settings

7.3.1 System Services

- All systems will have anonymous services disabled whenever possible.

- All services not required to fulfill project goals will be disabled and/or blocked.

7.3.2 Software Restrictions

- MAJIC system users shall not install software that is not properly licensed or not related to project goals and completion of duties.
- Software shall only be installed and used in accordance with the license agreement that covers it.

7.4 Virus Mitigations

- Virus protection software shall be installed before USB Thumb drives or similar are connected to the system for data down transmittal.
- Virus signatures will be updated weekly

7.5 Non Government owned systems

Non-government owned devices are not allowed to connect to or interact with the MAJIC system.

8 Incident Handling & Reporting

In the event of any suspected security problem, refer to the MAJIC Incident Response Plan for directions. That plan ensures compliance with the NASA guidance and appropriate coordination with the NASA Security Operations Center.