



**DEPARTMENT OF THE NAVY
(DON)**

**Application and Database Management System
(DADMS)**

System Rules of Behavior

May 20, 2004

Prepared for:

Department of the Navy Chief Information Officer (DON CIO)

Prepared by:

**AT&T Government Solutions Inc.
1900 Gallows Road
Vienna, Virginia 22182-3865**

TABLE OF CONTENTS

1. Introduction	1
2. User Agreement for System Rules of Behavior	4

TABLE

Table 1-1 DADMS Rules of Behavior	3
---	---

FIGURE

Figure 2-1 DADMS Login Screen	4
-------------------------------------	---

1. Introduction

Controls are needed for DADMS to ensure all users are accountable for their own actions and to protect mission-related data and equipment from both malicious and accidental loss or damage. The following rules of behavior have been developed to govern the behavior of all DADMS users to ensure they know and accept their responsibilities with respect to DADMS security. Individuals must agree to conform to these rules. This will be accomplished during DADMS login procedure as described later in this document. Consequences for violating DADMS Rules of Behavior vary according to the seriousness of the violation.

Minor infractions of the rules will result in management notification. More serious or continued infractions will result in the loss of system privileges. Major infractions that violate United States law, Department of Defense directives or regulations, will be referred to the office of the Inspector General for investigation and disciplinary action, which may include dismissal and/or criminal prosecution.

DADMS Rules of Behavior are listed in Table 1-1 below.

APPLICABLE TO	AREA	RULES
All Users	General Security	Users must ensure that the network resources and automated information systems (AISs) which they have been entrusted with are used properly, taking care that the laws and regulations governing the use of such resources are followed and that the value of all information assets are preserved.
		Each user is responsible for any and all activity performed under their assigned user ID.
		Users must be knowledgeable of DADMS security features and policies and seek additional information if it is not adequately provided during system training.
		Users must not circumvent any DADMS security control mechanism.
		Users must not read, alter, insert, copy, or delete any DADMS data except in accordance with their assigned job responsibilities. Ability to access data does not equate to authority. In particular, users must not browse or search DADMS data except in the performance of their authorized duties. It is a violation of federal law to access US Government data in excess of one's authorization (18 USC 1030).
		Users must not reveal information produced by DADMS except as required by their government job function and within established procedures.
		Users must notify supervisors when a particular access or authority is no longer required to perform their approved duties.
		If required, users must provide assistance with security audits and reviews.
		Users must report any known security breaches to their ISSO, the DADMS Help Desk and/or other DADMS management immediately after discovery of the occurrence.
		Users must report any attempts of bribery or extortion or any instances thereof to their management immediately.
	Environment	Users must protect DADMS data from loss, theft, damage, and unauthorized use or disclosure. The following rules listed in this "Environment" section defines how users can accomplish these objectives:
		Users must ensure that anyone seen using a DADMS workstation in the area is authorized to do so.

Appendix J – DADMS System Rules of Behavior

APPLICABLE TO	AREA	RULES	
		<p>Before accessing sensitive or Privacy Act information via DADMS, users must ensure that no unauthorized individuals can view their screen contents.</p> <p>Users must not leave an active workstation unattended. Active workstations may be locked (by using the authorized mechanisms) while unattended.</p> <p>Users must follow proper DADMS logon and logoff procedures.</p>	
	Passwords	<p>Users must protect user IDs and passwords from improper disclosure. Passwords provide DADMS access and are specifically assigned for accountability purposes. Users are responsible for any access made under their logon ID and password and must take the following precautions to protect their user ID and password from improper disclosure:</p> <p>Do not reveal passwords under any circumstances. If password disclosure occurs, immediately select a new one and report the disclosure to the ISSO.</p> <p>Do not share passwords with anyone else or use another person's password.</p> <p>Do not write passwords down.</p> <p>Change passwords at least every 90 days.</p> <p>Change passwords immediately if others know them.</p> <p>Choose "hard-to-guess" passwords by mixing upper and lower case letters, and at least one special and one numeric character.</p> <p>Do not use, in forward or backward sequence, whole or partial words, acronyms, or repetitive or commonly sequenced strings of three or more characters.</p> <p>Do not use strings of three or more characters from the previous five passwords, or a password based on intentional substitution of a part of any previous password.</p>	
	Media	<p>Ensure that paper copies of sensitive and private information is properly secured when not in use, and destroyed when no longer needed.</p> <p>User proper procedures to dispose of media that is no longer needed.</p> <p>Shred sensitive documents or place them in special collection bins where authorized personnel will collect them and ensure their proper destruction. Shred reports down the page instead of across.</p> <p>Ensure that floppy disks (and other storage media) are wiped before they are removed from a protected environment or reused for other purposes.</p> <p>Do not remove DADMS data from the workspace without written authority from DADMS management.</p>	
	System Administrators, Network Administrators, Application Developers, Troubleshooters, and DADMS Support Personnel	Misc. Admin Security	Support personnel will not read or alter any data except as required to complete the support duties assigned to them.
			Except for Network and System Administrators, and DADMS Help Desk staff, support personnel will not define new users to DADMS or alter user access privileges except on an emergency basis. After emergency procedures, control of user access will be returned to normal user administration as soon as possible.
			Support personnel will inform DADMS management of any special procedures or conditions, which may temporarily or permanently alter DADMS' security features.
			Support personnel will inform DADMS management of any maintenance performed on any DADMS system security mechanism.
			Support personnel will inform DADMS management of any diagnostic test result which indicates that a system security mechanism is not functioning properly.
			Support personnel will not change any information in any audit log under any circumstances.
			Support personnel will inform DADMS management in advance (except for emergencies) of any support procedure that involves disabling any audit log.

Appendix J – DADMS System Rules of Behavior

APPLICABLE TO	AREA	RULES
		Support personnel will ensure that any copies of sensitive information is properly secured and properly disposed of when no longer needed.
Configuration Managers	Config. Mgmt	Configuration managers will verify the authenticity and test status of any executable moved to the training or production environments. Configuration managers will not introduce any unapproved components into DADMS.
Information System Security Officers and Managers (ISSOs and ISSMs)	Access Control	<p>ISSOs will not grant access to DADMS resources except as directed by DADMS management and in accordance with established procedures.</p> <p>ISSOs will revoke the privileges of any user immediately when so directed by DADMS management.</p> <p>ISSOs will positively confirm the identity of the requestor before acceding to any password reset requests.</p> <p>ISSOs will grant excess privileges on an emergency basis only as directed by DON CIO management and only for the specified amount of time.</p> <p>ISSOs will be aware of the re-certification status of all users. Access will automatically be removed if user re-certification does not occur in a timely manner.</p> <p>ISSMs will investigate all suspected intrusion attempts, unauthorized access attempts, unauthorized alteration attempts, sabotage attempts and other misuse of the system without exception.</p> <p>ISSMs will not browse or scan the audit log except as part of their audit duties and within the bounds of established procedures.</p> <p>ISSMs will not reveal any information concerning user behavior except as required in the performance of their duties and within the bounds of established procedures.</p> <p>ISSMs will not reveal any audit log information outside of DADMS management or the investigating office.</p> <p>ISSMs will not alter any audit records under any circumstances.</p> <p>ISSMs will safeguard the privacy, integrity, and availability of the audit logs at all times.</p> <p>ISSMs will take care that information extracted from the audit log is properly secured when not in use and destroyed when no longer needed.</p> <p>ISSOs and ISSMs may delegate these responsibilities to the DADMS Help Desk.</p>

Table 1-1 DADMS Rules of Behavior

2. User Agreement for System Rules of Behavior

After logging into DADMS, the user sees the following screen:

The screenshot shows a web interface for DADMS. At the top, there is a horizontal bar with two buttons: 'AGREE' and 'DO NOT AGREE'. Below this, the text reads 'Login Accepted', 'Welcome to DADMSPROD LOY EBERSOLE', and 'Your last login was: 04/07/2004 3:21 PM'. A bolded statement follows: 'Logging into this website constitutes agreement to abide by the:'. Below this is a blue link labeled 'System Rules Of Behavior'. The next section is titled 'USER SESSION PROFILE' and contains several fields: 'Main Screen:' with a dropdown menu showing 'FAM Main Menu'; 'Echelon II UIC:' with a text box containing 'N00012'; 'User UIC:' with an empty text box; 'Component:' with a dropdown menu showing 'USN'; and 'Apply to:' with radio buttons for 'Session' (selected) and 'Always'. Below these fields is a red warning message: '*** You have Unread News ***'. At the bottom of the form is a 'Continue' button.

Figure 2-1 DADMS Login Screen

The System Rules Of Behavior link on this screen displays a copy of this document in a read only format. The first time a user logs into DADMS, or anytime the System Rules Of Behavior are updated, the user must select “AGREE” or “DO NOT AGREE”. On subsequent logins a “Continue” button is displayed. The user is logged off from DADMS if they select “DO NOT AGREE”, otherwise they are logged on with the agreement to abide by the System Rules Of Behavior.