Ordnance Information System (OIS)

Rules of Behavior (ROB)

Naval Supply Systems Command
Ammunition Logistics Center
OIS Program Management Office

ois-rob-2.1.2
July 2018

DOCUMENT ACCEPTANCE

Ordnance Information System
Rules of Behavior v2.1.2

Craig Murphy

OIS Program Manager

25 July 2018

Date

RECORD OF REVISIONS

Revision No.	Revision Date	Detailed Description of Change
1.0.0	05-Sep-2003	Baseline document
1.0.1	20-Sep 2006	Update to reflect NOLSC transition and new DIACAP requirements
2.0.0	22 May 2007	Review for out-of-date information
2.0.1	20 Jan 2010	Review for out-of-date information
2.0.2	15 Aug 2015	Update to reflect NAVSUP N65 transition and new DIACAP requirements
2.0.3	1 Jun 2016	Review and update out-of-date information
2.1.0	9 March 2018	Review and update out-of-date information, added compliance form as an Appendix
2.1.1	3 July 2018	Review and update information
2.1.2	13 July 2018	Removed For Official Use Only (FOUO) from the document header and footer.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF APPENDICES

1.0 INTRODUCTION

In the twenty-first century, information technology (IT) is an integral part of the physical weapon systems used by the Department of Defense (DoD) in providing for the defense of the United States. All Ordnance Information System (OIS) users have a vital responsibility and role in protecting this IT.

OIS users are trained in and held accountable for adherence to the Rules of Behavior (ROB) standard regarding security-related actions. This document contains systems security policy elements that are tailored for the users' specific roles. This set of standards will reduce the risk posed by non-adversarial internal threat agents. The content of this standard supports the NAVSUP Ammunition Logistics Center (NALC) Organizational Training and Security Awareness Program.

1.1 Scope

The OIS ROB applies to all military, contractor, and civilian personnel who have been granted access to OIS and who utilize its supporting IT resources; e.g., facilities, hardware, software, peripheral equipment, and data. OIS users include end users, developers, and anyone who has been granted access to OIS. OIS users shall follow the OIS ROB and protect the information, software, hardware, and all items that they work with daily. The following sections of this document detail the applicable rules for the following types of OIS users:

- All OIS users
- Configuration Managers
- Developers and Support Personnel
- Information System Security Managers (ISSM) and Information System Security Officers (ISSO)
- Operators, Network Administrators, and System Administrators

1.2 Purpose

This OIS ROB supplements the NALC Ammo Information Systems Security Manual and the NALC Ammo ROB. It is also a companion to the annual Security Awareness Indoctrination required of all OIS users.

2.0 RELATED DOCUMENTS

The rules contained in this document are in accordance with the following DoD and Department of the Navy (DON) directives, instructions, manuals, and guidance.

DODI 8500.01	Cybersecurity, March 14, 2014
DOD 8510.01	Risk Management Framework (RMF) for DoD Information Technology (IT), March 12, 2014
DODI 8520.02	Public Key Infrastructure (PKI) and Public Key (PK) Enabling, May 24, 2011
DODI 8520.03	Identity Authentication for Information Systems, May 13, 2011
SECNAV 5239.19	Department of the Navy Computer Network Incident Response and Reporting Requirements, March 18, 2008
SECNAV M-5239.1	Department of the Navy Information Assurance (IA) Program, November, 2005
OPNAV 5239.1C	Navy Information Assurance (IA) Program, August 20, 2008
OPNAVINST 5530.14E	Physical Security and Loss Prevention
SECNAVINST 5239.3C	Department of the Navy Cybersecurity Policy
SECNAVINST 5510.30B	Department of the Navy Personnel Security Program (PSP) Instruction
SECNAVINST 5510.36A	Department of the Navy Information Security Program (ISP) Instruction

3.0 ALL OIS USERS

The rules in this section apply to all military personnel, contractors, and civilian personnel who have been granted access to OIS and who utilize, support, and/or maintain its IT resources; e.g., facilities, hardware, software, peripheral equipment, and data.

3.1 General Security

1. Users shall be responsible for all activities performed under their assigned OIS usernames.
2. Users shall be knowledgeable of OIS security features and policies, and should seek additional information if it is not adequately provided during system training.
3. Users shall not circumvent any OIS security control mechanism.
4. Users shall not read, alter, insert, copy, or delete any OIS data, except as required by job function and established procedures. Access to data does not equate to authority. In particular, users must not browse or search OIS 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.
5. Users shall not reveal information produced by OIS to others, except as required by job function, and established procedures.
6. Users shall apply computer virus detection and eradication mechanisms in accordance with DoD, DON, OIS and local Command guidance.
7. Users shall notify supervisors when a particular access or authority is no longer required to perform their approved duties.
8. Users shall complete DON and DoD-mandated Security Training on an annual basis.
9. Users shall consent to monitoring and security testing to ensure that security procedures and rules for appropriate use are being followed.
10. Users shall follow local procedures for Non-secure Internet Protocol Router Network (NIPRNet) and Secret Internet Protocol Routing Network (SIPRNet) access and use.
11. Users shall report all observed compromises or security breaches involving OIS to their local Command ISSO and the responsible System Administrator. Examples of compromises or breaches include but are not limited to viruses, unauthorized access, theft, and inappropriate use. A reportable security incident is defined in Table 3-1.

TABLE 3-1: SECURITY INCIDENTS

Type of Security Incident	Description
Computer Intrusion	Unauthorized access to data or an information system
Attempted Intrusions	Unauthorized, unsuccessful attempts to access data or an information system
Denial of Service Attack	Actions that prevent any part of an automated information system from functioning properly, including actions that cause the unauthorized destruction or modification of data, or delay of service
Malicious Logic	Hardware, software, or firmware that is intentionally included in an information system for an unauthorized purpose, such as virus or Trojan horse
Probe	Any unauthorized attempt to gather information about an information system or its users online

3.2 Environmental Security

1. Users shall follow the rules for environmental, physical, and facility security as outlined by the local Command.
2. Users shall follow the proper OIS login and logoff procedures.
3. Individual sites shall be responsible for providing initial authentication to connect to the NIPRNet and SIPRNet.
4. Users shall ensure that any privately owned information technology resources used to access OIS meet DoD-security requirements, are validated by the Command ISSO or ISSM, and are authorized by the OIS Program Office prior to use.
5. Users shall abide by the rules for use of Portable Electronic Devices (PEDs) within DON spaces where collateral classified information is processed, transmitted, stored, or discussed. Users shall consult the local Command ISSO or ISSM prior to introducing any such devices into these areas.
6. Users shall abide by the local Command policy for software use on workstations.
7. Users shall handle Sensitive and Classified OIS materials in accordance with DoD, DON and local Command policies.

3.3 Media Security

1. Users shall properly secure and destroy paper copies of sensitive or private OIS information when not in use, in accordance with Department of the Navy (DON) policy.
2. Users shall properly secure and destroy sensitive or private OIS information stored on other media, such as CD ROM, diskette, etc., when not in use or no longer needed, in accordance with DON policy.
3. Individual sites shall be responsible for marking and labeling media and devices in accordance with DOD 5200.1-R vol. 2.

3.4 Account and Access Control Security

1. Users shall obtain and submit a fully executed, digitally signed OPNAV Form 5239/14 (REV 9/2011), System Authorization Access Request-Navy (SAAR-N), to confirm the user has authorized access to OIS. In addition, users shall obtain an Account Access Request Form (AARF) from the Customer Service Center (CSC) via the Unclassified OIS Portal at https://www.ois.disa.mil/ to request role permissions/access to specific sub-systems for OIS. The user shall submit the completed SAAR-N and AARF to the CSC for processing. A new AARF shall be submitted any time the user's roles or access requirements change. SAAR-N's and AARF's for all OIS employees are maintained onsite.
2. OIS employs Cryptographic Logon (CLO). All OIS user accounts shall require a Common Access Card (CAC) for Unclassified access (NIPRNet), or a PKI hardware token for SIPRNet access. With the DoD-mandated implementation of Public Key Enforcement, passwords are not permitted to log into OIS.
3. Users shall only use accounts for which they are authorized in accordance with their duties, clearance, and need-to-know. Account access privileges shall not be given to users until clearance and need to know is vetted by the Program Manager.
4. Users shall protect and maintain any information used or stored in their accounts on their local equipment. This includes but is not limited to ensuring that information and software are not lost, modified by, or released to unauthorized persons.

5. Users shall not attempt to access any data or programs for which access authorization or explicit consent been not granted by the Program Manager.
6. Account misuse by an authorized user may result in access privileges being revoked from the user.
7. Permitting the use of an account by an unauthorized person will result in access privileges being revoked from the account holder.
8. Remote access to OIS and system resources is limited to the approved privileged users, such as System, Portal, Network or Database Administrator. Whenever an administrative-type person leaves (quits/fired/etc.), that user's account shall be locked immediately. The account will be deleted after an approved SAAR-N/AARF is received, or directed by the OIS Program or Project Manager.
9. Remote access to OIS shall be through the approved method (NAVY VPN) via the NIPRNet and/or SIPRNet via a command-supported remote access server.
10. The user's manager shall submit a SAAR-N/AARF to delete a user's account and remove access when a user departs, voluntarily or involuntarily, a command or access to an OIS program or resource is no longer required. Users shall not attempt to access the program or resource after privileges have been removed.
11. Users should log into their account at least once every 30 days to keep their account active, as accounts will be locked after 30 days of inactivity. Should your account go 45 consecutive days without a login, it will be removed without warning and the user will have to go through the SAAR-N/AARF process again to reestablish the account.

3.5 Password Security

1. All OIS users shall initially access user accounts via an approved CAC or PKI token. Password use is not authorized except for limited situations that must be approved by the OIS Program Manager, and limited to privileged users for specific internal accounts and specific afloat users.
2. The following precautions shall be exercised in those limited instances where usernames and passwords are used for access to protect them from improper disclosure:
    a. Users should not reveal passwords or use another user's password under any circumstances. If a password is revealed or disclosed, the user shall immediately select a new password and report the disclosure to the ISSO.
    b. Users shall not write down passwords.
    c. Users shall not store passwords electronically in batch files or keyboard macros.
    d. Users shall select new passwords after 60 days. An elevated Information Operations Condition (INFOCON) level may require an immediate or more frequent change of passwords.
    e. Users shall change passwords after an account or OIS system becomes compromised, or if passwords are "cracked" during periodic password scanning.
    f. Users shall select passwords with a minimum of fifteen (15) alphanumeric characters, and should contain at least two each of upper case, lower case, numbers, and special characters (+, $, *, >, #, etc.). NOTE: The characters "&" and "@" should not be used when creating database passwords. When changing your password, it must differ from your previous password by at least 4 characters.
    g. Users shall not select passwords that are made up of words such as variations of user IDs, words in the dictionary, project names, or other work-related acronyms.

4.0 OIS DEVELOPERS, ADMINSTRATORS, AND SUPPORT PERSONNEL

The rules in this section pertain to OIS developers, application developers, and support personnel. Support personnel include:

- Functional Area Champions
- Network Administrators
- Portal Administrators
- System Administrators
- Database Administrators
- Project leads
- Testers
- Functionalists
- All other support personnel

4.1 General Administrative Security

1. Support personnel shall not read or alter any OIS data except as required to complete support duties assigned to them.
2. Support personnel shall inform the local ISSO or ISSM of any special procedures or conditions that may alter – temporarily or permanently – the security features of the OIS.
3. Support personnel shall inform the local ISSO or ISSM of any diagnostic test that indicates that a system security mechanism is not functioning properly.
4. Support personnel shall not change any information in any audit log under any circumstances.
5. Support personnel shall inform the local ISSO or ISSM in advance of any support procedure to be performed that involves the modification to or disabling of an audit log, or any action that adversely affects the confidentiality, integrity and availability of OIS, therefore weakening the OIS security posture.
6. Support personnel shall use OIS server resources, including computer equipment and networks, for authorized government use only.
7. Support personnel shall announce high-priority vulnerabilities, require callback reporting, require proper "fixes" to be immediately installed, and document task completion.
8. Support personnel shall distribute computer security announcements to all OIS development personnel in a timely manner.
9. Network Administrators, Portal Administrators, System Administrators, Database Administrators and CSC are the only support personnel who are authorized to add new users to OIS and modify user access privileges.
10. UNIX and Windows System Administrators, Portal Administrators and DBAs shall limit system privileges on all OIS servers or systems. User privileges to IT resources shall be granted based on each user's functional role and responsibilities. OIS supervisors, functional area champions, and project leads, in consultation with the ISSO, shall periodically review users' privileges and accesses to determine needed changes.

11. UNIX and Windows System Administrators, Portal Administrators and DBAs shall be the sole personnel with authority and ability to grant read/write access privileges for files, database objects, directories, and systems. This authority is given by the OIS PMO.
12. The UNIX and Windows System Administrators, Portal Administrators and DBAs shall install patches as quickly as possible, depending on the criticality of the vulnerability.
13. The UNIX and Windows System Administrators, Portal Administrators and DBAs shall apply Information Assurance Vulnerability Management notices (IAVM), including Information Assurance Vulnerability Alerts (IAVA), Information Assurance Vulnerability Bulletins (IAVB), and Information Assurance Vulnerability Technical Advisories (IAVTA) in a timely manner.
14. The IT Inventory Manager shall identify the procedures that the UNIX and Windows System Administrators shall follow when performing inventories of copyrighted software on OIS servers. Software that is not allocated shall be stored in the Enterprise Information System (EIS).
15. The ISSO, ISSM, and responsible Administrator shall take the appropriate action and ensure that all interested parties are contacted in the event of a security incident.
16. Physical access to the OIS computer areas is limited to those individuals who, by virtue of professional responsibilities and need-to-know, have reason to access these areas. Lists of such authorized personnel shall be posted within the OIS computer areas.
17. OIS servers shall undergo automated scans using anti-virus and compliance software.
18. UNIX and Windows System Administrators shall assist developers with requests to the hosting facility for anti-virus and compliance scans if additional scans of specific OIS servers are required.
19. UNIX and Windows System Administrators shall be the only personnel authorized to schedule scans or load and run anti-virus and compliance software on any OIS server.
20. UNIX and Windows System Administrator shall ensure that the current Virus Signature file and Host Based Security System (HBSS) files are installed on all OIS servers.
21. UNIX and Windows System Administrators, Portal Administrators and DBAs shall ensure that servers are regularly updated with software updates and patches, anti-virus and/or HBSS software.
22. If more than one person has system administration responsibilities, all of these personnel shall document their agreement to the guidelines and notify the primary System Administrator of changes made while using the root or administrator function. This shall be done to eliminate a single point of failure, and to provide primary and backup system administration support; i.e., check and balance.
23. For individual OIS servers, system privileges shall be limited to the UNIX and Windows System Administrators and specialized accounts; e.g., Portal and Database Administrator (DBA).
24. Users will ensure that devices that display or output classified or sensitive information in human-readable form are positioned to deter unauthorized individuals from reading the information.

4.2 Backup Procedures for Operators, System Administrators, and Network Administrators

The following rules pertain to OIS server backups. The Defense Information Systems Agency (DISA) Defense Enterprise Computing Centers (DECCs) are contractually responsible for performing backups of OIS servers hosted within the DECCs. Local (non-DECC) OIS server backup procedures are governed by the following rules.

1. The Operations Manager shall ensure that an effective policy for backup and restore is in place and properly implemented.
2. UNIX and Windows System Administrators shall be responsible to ensure that OIS server backups and recoveries are performed as defined in the OIS Contingency Plan.
3. Backup media for servers shall be kept long enough to ensure data integrity before reuse.
4. OIS backup materials maintained off-site shall be stored, handled, and disposed of appropriately based on their level of classification.

5.0 CONFIGURATION MANAGERS

The rules in this section apply to Configuration Managers who perform configuration management and related security measures.

1. Configuration Managers shall verify the authenticity and the test status of any executable moved to the OIS testing or production environments.
2. Configuration Managers shall not introduce any unapproved components into OIS.

6.0 ISSO AND ISSM

The rules in this section address access control issues. These rules apply to OIS ISSO(s), site ISSO(s), and the ISSM.

1. ISSO(s) shall only grant access to OIS resources in accordance with established procedures, and only when directed by the ISSM.
2. ISSO(s) shall revoke user privileges immediately when directed by the ISSM.
3. ISSO(s) shall positively confirm a requestor's identity before acceding to a request to reset a password.
4. ISSO(s) shall only grant additional privileges on an emergency basis, as directed in writing by the program manager, and only for the specified amount of time.
5. ISSO(s) shall be aware of the re-certification status of all OIS user facilities, networks, and hardware. ISSO(s) shall automatically remove access if user re-certification does not occur in a timely manner.
6. The ISSM shall investigate all suspected intrusion attempts, unauthorized access attempts, unauthorized alteration attempts, sabotage attempts, and other potential misuse of the system, without exception.
7. The ISSM shall not browse or scan the audit log except within the bounds of the established procedures for audit duties.
8. The ISSM shall not reveal any information concerning user behavior except as required in the performance of duties and within the bounds of established procedures.
9. The ISSM shall not reveal any audit log information outside of the investigating office.
10. The ISSM shall not alter any audit records under any circumstances.
11. The ISSM shall safeguard the privacy, integrity, and availability of the audit logs at all times.
12. The ISSM shall ensure that information extracted from the audit log is properly secured when not in use, and destroyed when no longer needed.

7.0 CONSEQUENCES OF NON-COMPLIANCE WITH THE OIS ROB

Failure to abide by the OIS ROB may constitute grounds for termination of access privileges, administrative action, and/or civil or criminal prosecution.

The ISSO, Network Administrator, or System Administrator shall handle local incidents as appropriate based on the severity of the non-compliance. The Command ISSM has final authority for determining or approving the consequence.

8.0 SUMMARY

All OIS users shall be responsible for the protection and security of OIS equipment, information, and material. By accepting, clicking the user acknowledgement checkbox on OIS splash screen, and complying with the OIS ROB, OIS users will meet this responsibility.

APPENDIX A: ACRONYMS

TABLE A-1: ACRONYMS	
Acronym	**Definition**
AARF	Access Action Request Form
AIS	Automated Information System
CSC	Customer Service Center
DBA	Database Administrator
DECC	Defense Enterprise Computing Center
DISA	Defense Information Systems Agency
DOD	Department of Defense
EIS	Enterprise Information System
IA	Information Assurance
IAVA	Information Assurance Vulnerability Alerts
IAVB	Information Assurance Vulnerability Bulletins
IAVM	Information Assurance Vulnerability Management
IAVTA	Information Assurance Vulnerability Technical Advisories
INFOCON	Information Operations Condition
ISSM	Information Systems Security Manager
ISSO	Information Systems Security Officer
IT	Information Technology
LAN	Local Area Network
NALC	NAVSUP Ammunition Logistics Center
NIPRNet	Non-secure Internet Protocol Routing Network
NOLSC	Naval Operational Logistics Support Center
OIS	Ordnance Information System
PC	Personal Computer
PED	Portable Electronic Device
ROB	Rules of Behavior
SIPRNet	Secure Internet Protocol Routing Network

APPENDIX B: ALTERNATE USER ACKNOWLEDGEMENT FORM

I acknowledge receipt of the OIS Rules of Behavior and have read and understanding said document. I further understand the consequences of not complying with the OIS Rules of Behavior as stated in said document.

User Last Name, First Name:

User Signature:

Please return to OIS Customer Service Center at Ord_Info_Sys_CSC@navy.mil and name the file in the following format: OIS_ROB_lastname_firstname_YYMMDD.