SECTION 16

INFORMATION TECHNOLOGY RULES OF BEHAVIOR

16.1 Background

The MARAD Chief Information Officer is committed to providing a robust, reliable and secure information technology (IT) environment that supports the MARAD mission objectives and your help in this effort is essential to MARAD's success. These Rules of Behavior (ROBs) have been developed to ensure you are aware of your personal responsibilities for protecting MARAD's IT resources. Rules of Behavior (ROBs) establish guidelines for the use of MARAD's IT assets. The ROBs also explain some of the consequences for using MARAD IT assets inappropriately.

16. 2 Purpose, Scope, & Applicability

16.2.1 Purpose

ROBs help ensure you are aware of your responsibilities when accessing and operating MARAD IT assets. These ROBs summarize the most common laws and guidelines from various DOT and other Federal documents, most specifically OMB Circular A-130. By reading and signing these ROBs, you acknowledge that you understand your responsibilities when using MARAD's IT assets and agree to abide by the ROBs. You have personal responsibility for the security of your computers and the data they contain.

16.2.2 Scope

The ROBs extend to all MARAD personnel and any other persons using MARAD IT assets or accessing MARAD systems under formally established agreements. This includes contractors and other federally funded users.

16.2.3 Applicability

ROBs are applicable to all MARAD personnel, government or contractors, for the period of time assigned to MARAD.

16.3 Roles and Responsibilities

16.3.1 MARAD CIO

The MARAD CIO is responsible to ensure that the ROBs are updated, as required to cover changes in DOT/MARAD policy and procedures. The MARAD CIO is responsible to ensure that all MARAD personnel have read and signed the ROBs. For those who are not willing to sign the ROBs, the supervisor or COTR must document via a Memo for the Record (MFR) that this employee has read the ROBs and has agreed to abide by their requirements.

16.3.1.1. The MARAD CIO reserves the right to enforce the use of penalties against you if you willfully violate any MARAD, DOT or federal system security (and related) policy. The ROBs are based on the principles described in the DOT Employee Awareness Guide to Information Technology Security and other regulatory documents such as the Code of Ethics for Government Employees, Office of Personnel Management regulations, Office of Management and Budget regulations, and Standard of Conduct for Federal Employees. Therefore, the Rules of Behavior carry the same responsibility for compliance as other official documents.

16.3.1. 2 The MARAD CIO office will maintain a repository of all signed ROBs and Memos for the Record

16.3.2 MARAD Information Systems Security Officer (ISSO)

The MARAD Information Systems Security Officer (ISSO) is responsible for maintaining the ROBs and ensuring all MARAD users comply with MARAD IT security policies. To find out who the MARAD ISSO is, please contact the MARAD Help Desk.

16.3.3 MARAD Human Resources

Provide a copy of the ROBs to all new MARAD employees.

16.3.4 MARAD Help Desk

Prior to granting access to the new personnel (Government and Contractors), the help desk will ensure that a signed ROB or MFR is on file. If signed ROB or MFR is not on file for Contractor personnel, the appropriate MARAD government Contracting Officer Representative must be contacted.

16.3.5 User Responsibilities

16.3.5.1 General

Users must adhere to the DOT Standards of Conduct and MARAD's ROBs by behaving in an ethical, proficient, informed, and trustworthy manner. Users should complete the DOT or MARAD Computer Security Awareness Training prior to obtaining access to DOT or MARAD systems. Users should access and use only systems, software and data for which Users have authorization and use them for authorized purposes only. Users should notify appropriate personnel when access to MARAD IT resources is no longer required and should make no further attempt to access these resources. Users should not alter the configuration of government equipment unless authorized, including installing software or peripherals. Behavior consistent with these rules is required to gain and continue access to MARAD IT systems.

16.3.5.2 Access Control

Do not grant access to systems and data to those who do not have an official need to know. Do not attempt to override technical management and/or security controls. Do not use your trusted position and access privileges to exploit system controls or access data for any reason other than in the performance of official duties. Never share or compromise your password.

16.3.5.3 Passwords

16.3.5.3.1 Passwords should be unique to each user. The objective when choosing a password is to make it as difficult as possible for someone else to guess what you've chosen. Based on system requirements and limitations, passwords should be a minimum of eight characters, and be a combination of letters, numbers and special characters (such as #$%^). If the system will allow case-sensitive passwords, use a password with both upper- and lower-case letters. Dictionary words should not be used. Passwords should be changed at least every 90 days and should never be repeated. Compromised passwords should be changed immediately.

16.3.5.3.2 Don't use your login name in any form (as-is, reversed, doubled, with a number or other letter or symbol, etc.). Don't use first or last name in any form, or any names of children, mother, spouse, etc. Don't use any information easily obtained about you or your family members, including birth dates, addresses, telephone numbers, etc.

16.3.5.4 Internet Use

16.3.5.4.1 Connection to the Internet must be coordinated with the MARAD Help Desk. Except for limited personal use, the downloading of files, programs, templates, images, and messages is prohibited, unless explicitly authorized and approved by the MARAD ISSO. Because they pose a potential security risk, the use of external Web-based instant messaging services, or communications software or devices, is prohibited. Except for limited personal use, do not use the Internet to make non-work related purchases or acquisitions. Using the Internet to manage, run, supervise, or conduct personal business is prohibited.

16.3.5.4.2 Deliberately, or knowingly, viewing or downloading material from web sites that promote, display, present, share or distribute pornography is a violation of MAO 770-713-3, "Prevention and Elimination of Harassment in the Workplace". Users may be subject to penalties or administrative action outlined in MAO 770-751, "Disciplinary and Adverse Actions". Possession of or involvement in child pornography is a felony offense subject to civil and criminal liability. Possession of such material will be reported to investigative authorities.

16.3.5.5 Peer-to-Peer File Sharing

The use of peer-to-peer file sharing services is prohibited, unless expressly approved by the ISSO. Software that uses the Internet to exchange files (i.e., music, games, etc.) between users by either directly connecting the users to the files or connecting them through a mediating server is strictly prohibited. Because these software applications are used primarily to illegally share copyrighted material, the use of such applications subjects MARAD to the possibility of civil prosecution. Additionally, the use of these applications can result in the loss of sensitive data and damage to MARAD systems.

16.3.5.6 Email

Except for limited personal use, non-work-related e-mail is prohibited. The dissemination of e-mail chain letters, e-mail invitations, or e-mail cards is prohibited. E-mail addresses and e-mail list-servers constitute sensitive information and should not be sold, shared, disseminated, or used in any unofficial manner. Using an official e-mail address to subscribe to electronically-distributed, non-work related newsletters or magazines is prohibited.

16.3.5.7 Working from Home

Users who work from home must ensure a safe and secure working environment free from unauthorized visitors. Home users connected to the Internet via a broadband connection (e.g. DSL or a cable modem) should install a hardware or software firewall. No official material should be stored on the user's personal computer. All data should be stored on removable media and then secured to prevent inadvertent access.

16.3.5.8 Remote Dial-up Access/Off-site Access of IT Resources

Authorized personnel may connect to the MARAD network remotely only if pre-approved by the OCIO. Users must log-off and secure all connections/ports upon completion of each work session. At no time should an active connection be left unattended.

16.3.5.9 Virus Prevention

Personally owned computers using MARAD's IT facilities (such as MARAD's LAN) shall regularly run anti-virus software. It is the user's responsibility to acquire and keep the software up-to-date. Do not open files attached to an email from an unknown, suspicious or untrustworthy source. If Users suspect the file may contain a virus, immediately contact the MARAD Help Desk or the ISSO. Delete chain emails and junk email. Do not forward or reply to them. These types of email are considered spam, which is unsolicited, intrusive mail that reduces the performance of the network. Exercise caution when downloading files from the Internet. Ensure that the source is a legitimate and reputable one. If users are uncertain about any email or file, contact the MARAD Help Desk or the ISSO for assistance.

16.3.5.10 Scanning

All MARAD computers are subject to monitoring and periodic scanning for viruses and inappropriate materials. You are required to cooperate with these efforts.

16.3.5.11 Sensitive Information

Sensitive information may include, but is not limited to, personal information and proprietary data. Removable media with sensitive information should be properly marked, protected, and erased when no longer needed.

16.3.5.12 Classified Information

Classified information shall not be received on, sent from, or stored on MARAD's LAN. If a user has access to classified information, refer to Executive Order 12958 and DOT 1640.4D, Classified Information Management Manual, for guidelines governing the handling and control of classified information and materials.

16.3.5.13 Copyrighted Material

Use unauthorized copyrighted software only as permitted by law or by the copyright owner. Protect copyrighted software and information in accordance with the conditions under which it is provided.

16.3.5.14 Faxing Sensitive Information

Include the following disclaimer on the fax cover sheet when sending faxes containing sensitive information:

> ******WARNING******
> *The attached information may be sensitive. It is intended only for the addressee(s) identified above. If you are not the addressee(s), or an employee or agent of the addressee(s), please note that any dissemination, distribution, or copying of this communication is strictly prohibited. If you have received this fax in error, please destroy the document and notify the sender of the error. Thank you.*

16.3.5.15 Physical Security

Protect personal and government property from theft, destruction, or misuse. Do not remove computers from MARAD premises unless authorized. Contact the MARAD Help Desk when computer equipment needs to be moved.

16.3.5.16 Reporting of IT Security Incidents

Users are required to report all observed compromises of IT security (viruses, unauthorized access, theft, inappropriate use, etc.) to the MARAD Help Desk or ISSO. Immediately notify the MARAD Help Desk of any unusual events or problems that appear to be affecting the operational characteristics of your IT equipment.

16.4 Documentation

16.4.1 The ROB information sheet in Appendix 16-1 must be signed by all MARAD government and contractor personnel prior to granting access to the MARAD LAN. Personnel who do not sign are not relieved from the requirements of the ROB. Appendix 16-2 contains a sample Memo for the Record that must be completed for personnel who choose not to sign.

16.4.2 Acknowledgement

The following acknowledgement must be completed on all MARAD ROB signature sheets.

I have read and understand the ROBs governing the use of MARAD networks and agree to abide by them. I understand failure to do so may result in disciplinary action.

Printed User Name		**Date**	
User Signature			

Appendix 16-1
Maritime Administration
Information Technology Rules of Behavior

Maritime Administration
Information Technology Rules of Behavior

The MARAD Chief Information Officer is committed to providing a robust, reliable and secure information technology (IT) environment that supports the MARAD mission objectives and your help in this effort is essential to MARAD's success. These Rules of Behavior (ROBs) have been developed to ensure you are aware of your personal responsibilities for protecting MARAD's IT resources. Please read and sign these ROBs in order to obtain and retain access to MARAD's IT resources. If you choose not to sign these ROBs you are NOT relieved of these requirements.

//signed//
Donna K. Seymour
Chief Information Officer

1. Frequently Asked Questions

What are Rules of Behavior?

Rules of Behavior (ROBs) establish guidelines for the use of MARAD's information technology (IT) assets. The ROBs also explain some of the consequences for using MARAD IT assets inappropriately.

Why are Rules of Behavior Needed?

ROBs help ensure you are aware of your responsibilities when accessing and operating MARAD IT assets. These ROBs summarize the most common laws and guidelines from various DOT and other Federal documents, most specifically OMB Circular A-130. By reading and signing these ROBs, you acknowledge that you understand your responsibilities when using MARAD's IT assets and agree to abide by the ROBs. You have personal responsibility for the security of your computers and the data they contain.

Who is covered by the Rules of Behavior?

The ROBs extend to all MARAD personnel and any other persons using MARAD IT assets or accessing MARAD systems under formally established agreements. This includes contractors and other federally funded users.

What are the consequences for behavior inconsistent with the Rules?

Failure to abide by the ROBs may constitute grounds for administrative action (such as reprimand, termination of employment, suspension from duty, temporary or permanent loss of system privileges), civil prosecution and/or criminal prosecution.

Who can you contact if you have questions about the Rules of Behavior?

The MARAD Information Systems Security Officer (ISSO) is responsible for maintaining the ROBs and ensuring all MARAD users comply with MARAD IT security policies. To find out who the MARAD ISSO is, please contact the MARAD Help Desk.

2. Compliance

MARAD reserves the right to enforce the use of penalties against you if you willfully violate any MARAD, DOT or federal system security (and related) policy. The ROBs are based on the principles described in the DOT Employee Awareness Guide to Information Technology Security and other regulatory documents such as the Code of Ethics for Government Employees, Office of Personnel Management regulations, Office of Management and Budget regulations, and Standard of Conduct for Federal Employees. Therefore, the Rules of Behavior carry the same responsibility for compliance as other official documents.

3. User Responsibilities

General

You should adhere to the DOT Standards of Conduct and MARAD's ROBs by behaving in an ethical, proficient, informed, and trustworthy manner. You should complete the DOT or MARAD Computer Security Awareness Training prior to obtaining access to DOT or MARAD systems. You should access and use only systems, software and data for which you have authorization and use them for authorized purposes only. You should notify appropriate personnel when access to MARAD IT resources is no longer required and should make no further attempt to access these resources. You should not alter the configuration of government equipment unless authorized, including installing software or peripherals. Behavior consistent with these rules is required to gain and continue access to MARAD IT systems.

Access Control

Do not grant access to systems and data to those who do not have an official need to know. Do not attempt to override technical management and/or security controls. Do not use your trusted position and access privileges to exploit system controls or access data for any reason other than in the performance of official duties. Never share or compromise your password.

Passwords

Passwords should be unique to each user. Your objective when choosing a password is to make it as difficult as possible for someone else to guess what you've chosen. Based on system requirements and limitations, passwords should be a minimum of eight characters, and be a combination of letters, numbers and special characters (such as #$%^). If the system will allow case-sensitive passwords, use a password with both upper- and lower-case letters. Dictionary words should not be used. Passwords should be changed at least every 90 days and should never be repeated. Compromised passwords should be changed immediately.

Don't use your login name in any form (as-is, reversed, doubled, with a number or other letter or symbol, etc.). Don't use your first or last name in any form, or any names for your children, mother, spouse, etc. Don't use any information easily obtained about you or your family members, including birth dates, addresses, telephone numbers, etc.

Internet Use

Connection to the Internet must be coordinated with the MARAD Help Desk. Except for limited personal use, the downloading of files, programs, templates, images, and messages is prohibited, unless explicitly authorized and approved by the MARAD ISSO. Because they pose a potential security risk, the use of external Web-based instant messaging services, or communications software or devices, is prohibited. Except for limited personal use, do not use the Internet to make non-work related purchases or acquisitions. Using the Internet to manage, run, supervise, or conduct personal business is prohibited.

Deliberately, or knowingly, viewing or downloading material from web sites that promote, display, present, share or distribute pornography is a violation of MAO 770-713-3, "Prevention and Elimination of Harassment in the Workplace". You may be subject to penalties or administrative action outlined in MAO 770-751, "Disciplinary and Adverse Actions". Possession of or involvement in child pornography is a felony offense subject to civil and criminal liability. Possession of such material will be reported to investigative authorities.

Peer-to-Peer File Sharing

The use of peer-to-peer file sharing services is prohibited, unless expressly approved by the ISSO. Software that uses the Internet to exchange files (i.e. music, games, etc.) between users by either directly connecting the users to the files or connecting them through a mediating server is strictly prohibited. Because these software applications are used primarily to illegally share copyrighted material, the use of such applications subjects MARAD to the possibility of civil prosecution. Additionally, the use of these applications can result in the loss of sensitive data and damage to MARAD systems.

Email

Except for limited personal use, non-work-related e-mail is prohibited. The dissemination of e-mail chain letters, e-mail invitations, or e-mail cards is prohibited. E-mail addresses and e-mail list-servers constitute sensitive information and should not be not be sold, shared, disseminated, or used in any unofficial manner. Using an official e-mail address to subscribe to electronically-distributed, non-work related newsletters or magazines is prohibited.

Working from Home

Users who work from home must ensure a safe and secure working environment free from unauthorized visitors. Home users connected to the Internet via a broadband connection (e.g. DSL or a cable modem) should install a hardware or software firewall. No official material should be stored on the user's personal computer. All data should be stored on removable media and then secured to prevent inadvertent access.

Remote Dial-up Access/Off-site Access of IT Resources

You may connect to the MARAD network remotely only if pre-approved by the OCIO. You must log-off and secure all connections/ports upon completion of each work session. At no time should an active connection be left unattended.

Virus Prevention

Personally owned computers using MARAD's IT facilities (such as MARAD's LAN) shall regularly run anti-virus software. It is your responsibility to acquire and keep the software up-to-date. Do not open files attached to an email from an unknown, suspicious or untrustworthy source. If you suspect the file may contain a virus, immediately contact the MARAD Help Desk or the ISSO. Delete chain emails and junk email. Do not forward or reply to them. These types of email are considered spam, which is unsolicited, intrusive mail that reduces the performance of the network. Exercise caution when downloading files from the Internet. Ensure that the source is a legitimate and reputable one. If you are uncertain about any email or file, contact the MARAD Help Desk or the ISSO for assistance.

Scanning

All MARAD computers are subject to monitoring and periodic scanning for viruses and inappropriate materials. You are required to cooperate with these efforts.

Sensitive Information

Sensitive information may include, but is not limited to, personal information and proprietary data. Removable media with sensitive information should be properly marked, protected, and erased when no longer needed.

Classified Information

Classified information shall not be received on, sent from, or stored on MARAD's LAN. If you have access to classified information, refer to Executive Order 12958 and DOT 1640.4D, Classified Information Management Manual, for guidelines governing the handling and control of classified information and materials.

Copyrighted Material

Use unauthorized copyrighted software only as permitted by law or by the copyright owner. Protect copyrighted software and information in accordance with the conditions under which it is provided.

Faxing Sensitive Information

Include the following disclaimer on the fax cover sheet when sending faxes containing sensitive information:

> ******WARNING******
> *The attached information may be sensitive. It is intended only for the addressee(s) identified above. If you are not the addressee(s), or an employee or agent of the addressee(s), please note that any dissemination, distribution, or copying of this communication is strictly prohibited. If you have received this fax in error, please destroy the document and notify the sender of the error. Thank you.*

Physical Security

Protect personal and government property from theft, destruction, or misuse. Do not remove computers from MARAD premises unless authorized. Contact the MARAD Help Desk when computer equipment needs to be moved.

Reporting of IT Security Incidents

You are required to report all observed compromises of IT security (viruses, unauthorized access, theft, inappropriate use, etc.) to the MARAD Help Desk or ISSO. Immediately notify the MARAD Help Desk of any unusual events or problems that appear to be affecting the operational characteristics of your IT equipment.

4. Acknowledgement

I have read and understand the ROBs governing the use of MARAD networks and agree to abide by them. I understand failure to do so may result in disciplinary action.

Printed User Name		**Date**	
User Signature			

APPENDIX 16 -2
MEMO FOR THE RECORD

The following information has been read on this day to the individual whose name appears in the acknowledgement block. This individual understands that their choice not to sign the MARAD Rules of Behavior (ROBs) does not alleviate their responsibility to adhere to these requirements.

Maritime Administration
Information Technology Rules of Behavior

The MARAD Chief Information Officer is committed to providing a robust, reliable and secure information technology (IT) environment that supports the MARAD mission objectives and your help in this effort is essential to MARAD's success. These Rules of Behavior (ROBs) have been developed to ensure you are aware of your personal responsibilities for protecting MARAD's IT resources. Please read and sign these ROBs in order to obtain and retain access to MARAD's IT resources. If you choose not to sign these ROBs you are NOT relieved of these requirements.

//signed//
Donna K. Seymour
Chief Information Officer

2. Frequently Asked Questions

What are Rules of Behavior?

Rules of Behavior (ROBs) establish guidelines for the use of MARAD's information technology (IT) assets. The ROBs also explain some of the consequences for using MARAD IT assets inappropriately.

Why are Rules of Behavior Needed?

ROBs help ensure you are aware of your responsibilities when accessing and operating MARAD IT assets. These ROBs summarize the most common laws and guidelines from various DOT and other Federal documents, most specifically OMB Circular A-130. By reading and signing these ROBs, you acknowledge that you understand your responsibilities when using MARAD's IT assets and agree to abide by the ROBs. You have personal responsibility for the security of your computers and the data they contain.

Who is covered by the Rules of Behavior?

The ROBs extend to all MARAD personnel and any other persons using MARAD IT assets or accessing MARAD systems under formally established agreements. This includes contractors and other federally funded users.

What are the consequences for behavior inconsistent with the Rules?

Failure to abide by the ROBs may constitute grounds for administrative action (such as reprimand, termination of employment, suspension from duty, temporary or permanent loss of system privileges), civil prosecution and/or criminal prosecution.

Who can you contact if you have questions about the Rules of Behavior?

The MARAD Information Systems Security Officer (ISSO) is responsible for maintaining the ROBs and ensuring all MARAD users comply with MARAD IT security policies. To find out who the MARAD ISSO is, please contact the MARAD Help Desk.

2. Compliance

MARAD reserves the right to enforce the use of penalties against you if you willfully violate any MARAD, DOT or federal system security (and related) policy. The ROBs are based on the principles described in the DOT Employee Awareness Guide to Information Technology Security and other regulatory documents such as the Code of Ethics for Government Employees, Office of Personnel Management regulations, Office of Management and Budget regulations, and Standard of Conduct for Federal Employees. Therefore, the Rules of Behavior carry the same responsibility for compliance as other official documents.

5. User Responsibilities

General

You should adhere to the DOT Standards of Conduct and MARAD's ROBs by behaving in an ethical, proficient, informed, and trustworthy manner. You should complete the DOT or MARAD Computer Security Awareness Training prior to obtaining access to DOT or MARAD systems. You should access and use only systems, software and data for which you have authorization and use them for authorized purposes only. You should notify appropriate personnel when access to MARAD IT resources is no longer required and should make no further attempt to access these resources. You should not alter the configuration of government equipment unless authorized, including installing software or peripherals. Behavior consistent with these rules is required to gain and continue access to MARAD IT systems.

Access Control

Do not grant access to systems and data to those who do not have an official need to know. Do not attempt to override technical management and/or security controls. Do not use your trusted position and access privileges to exploit system controls or access data for any reason other than in the performance of official duties. Never share or compromise your password.

Passwords

Passwords should be unique to each user. Your objective when choosing a password is to make it as difficult as possible for someone else to guess what you've chosen. Based on system requirements and limitations, passwords should be a minimum of eight characters, and be a combination of letters, numbers and special characters (such as #$%^). If the system will allow case-sensitive passwords, use a password with both upper- and lower-case letters. Dictionary words should not be used. Passwords should be changed at least every 90 days and should never be repeated. Compromised passwords should be changed immediately.

Don't use your login name in any form (as-is, reversed, doubled, with a number or other letter or symbol, etc.). Don't use your first or last name in any form, or any names for your children, mother, spouse, etc. Don't use any information easily obtained about you or your family members, including birth dates, addresses, telephone numbers, etc.

Internet Use

Connection to the Internet must be coordinated with the MARAD Help Desk. Except for limited personal use, the downloading of files, programs, templates, images, and messages is prohibited, unless explicitly authorized and approved by the MARAD ISSO. Because they pose a potential security risk, the use of external Web-based instant messaging services, or communications software or devices, is prohibited. Except for limited personal use, do not use the Internet to make non-work related purchases or acquisitions. Using the Internet to manage, run, supervise, or conduct personal business is prohibited.

Deliberately, or knowingly, viewing or downloading material from web sites that promote, display, present, share or distribute pornography is a violation of MAO 770-713-3, "Prevention and Elimination of Harassment in the Workplace". You may be subject to penalties or administrative action outlined in MAO 770-751, "Disciplinary and Adverse Actions". Possession of or involvement in child pornography is a felony offense subject to civil and criminal liability. Possession of such material will be reported to investigative authorities.

Peer-to-Peer File Sharing

The use of peer-to-peer file sharing services is prohibited, unless expressly approved by the ISSO. Software that uses the Internet to exchange files (i.e. music, games, etc.) between users by either directly connecting the users to the files or connecting them through a mediating server is strictly prohibited. Because these software applications are used primarily to illegally share copyrighted material, the use of such applications subjects MARAD to the possibility of civil prosecution. Additionally, the use of these applications can result in the loss of sensitive data and damage to MARAD systems.

Email

Except for limited personal use, non-work-related e-mail is prohibited. The dissemination of e-mail chain letters, e-mail invitations, or e-mail cards is prohibited. E-mail addresses and e-mail list-servers constitute sensitive information and should not be not be sold, shared, disseminated, or used in any unofficial manner. Using an official e-mail address to subscribe to electronically-distributed, non-work related newsletters or magazines is prohibited.

Working from Home

Users who work from home must ensure a safe and secure working environment free from unauthorized visitors. Home users connected to the Internet via a broadband connection (e.g. DSL or a cable modem) should install a hardware or software firewall. No official material should be stored on the user's personal computer. All data should be stored on removable media and then secured to prevent inadvertent access.

Remote Dial-up Access/Off-site Access of IT Resources

You may connect to the MARAD network remotely only if pre-approved by the OCIO. You must log-off and secure all connections/ports upon completion of each work session. At no time should an active connection be left unattended.

Virus Prevention

Personally owned computers using MARAD's IT facilities (such as MARAD's LAN) shall regularly run anti-virus software. It is your responsibility to acquire and keep the software up-to-date. Do not open files attached to an email from an unknown, suspicious or untrustworthy source. If you suspect the file may contain a virus, immediately contact the MARAD Help Desk or the ISSO. Delete chain emails and junk email. Do not forward or reply to them. These types of email are considered spam, which is unsolicited, intrusive mail that reduces the performance of the network. Exercise caution when downloading files from the Internet. Ensure that the source is a legitimate and reputable one. If you are uncertain about any email or file, contact the MARAD Help Desk or the ISSO for assistance.

Scanning

All MARAD computers are subject to monitoring and periodic scanning for viruses and inappropriate materials. You are required to cooperate with these efforts.

Sensitive Information

Sensitive information may include, but is not limited to, personal information and proprietary data. Removable media with sensitive information should be properly marked, protected, and erased when no longer needed.

Classified Information

Classified information shall not be received on, sent from, or stored on MARAD's LAN. If you have access to classified information, refer to Executive Order 12958 and DOT 1640.4D, Classified Information Management Manual, for guidelines governing the handling and control of classified information and materials.

Copyrighted Material

Use unauthorized copyrighted software only as permitted by law or by the copyright owner. Protect copyrighted software and information in accordance with the conditions under which it is provided.

Faxing Sensitive Information

Include the following disclaimer on the fax cover sheet when sending faxes containing sensitive information:

> ******WARNING******
> *The attached information may be sensitive. It is intended only for the addressee(s) identified above. If you are not the addressee(s), or an employee or agent of the addressee(s), please note that any dissemination, distribution, or copying of this communication is strictly prohibited. If you have received this fax in error, please destroy the document and notify the sender of the error. Thank you.*

Physical Security

Protect personal and government property from theft, destruction, or misuse. Do not remove computers from MARAD premises unless authorized. Contact the MARAD Help Desk when computer equipment needs to be moved.

Reporting of IT Security Incidents

You are required to report all observed compromises of IT security (viruses, unauthorized access, theft, inappropriate use, etc.) to the MARAD Help Desk or ISSO. Immediately notify the MARAD Help Desk of any unusual events or problems that appear to be affecting the operational characteristics of your IT equipment.

6. Acknowledgement

The ROBs governing the use of MARAD networks have been read to the named individual and who has agreed to abide by them. This individual agrees that failure to do so may result in disciplinary action.

Printed User Name		**Date**	
Supervisor/COTR Name			
Supervisor/COTR Signature			