

Office of Marine and Aviation Operations ACCESS CONTROL POLICY

1. **REASON FOR ISSUE:** To establish policy for the implementation of information technology (IT) access control policy and procedures controls within the National Oceanic and Atmospheric Administration (NOAA), Office of Marine and Aviation Operations (OMAO).
2. **SUMMARY OF CONTENTS/MAJOR CHANGES:** This policy requires OMAO -wide compliance with access control policy and procedures in accordance with the National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 3 and related information security issuances pertaining to the security of NOAA information and information systems administered by OMAO, or otherwise under the authority, control, or on behalf of OMAO.
3. **RESPONSIBLE OFFICE:** NOAA / OMAO
4. **RELATED POLICY:** *NOAA IT Security Manual - Access Control*, and *Department of Commerce IT Security Program Policy, Section 4.1 - Access Control*
5. **RESCISSIONS:** None

CERTIFIED BY:

Douglas A. Perry
OMAO Chief Information Officer

Distribution: OMAO CIO, OMAO ITSO
Cc: System Owners, Subsystem Managers

Record of Changes/Revisions

This Access Control policy is a living document that is changed as required to reflect system, operational or organizational changes. This policy shall be reviewed at least annually to document changes and ensure that the policy continues to reflect the correct information about the system. Modifications made to this document are recorded in the Change/Revision Record below. This record shall be maintained throughout the life of the document.

Change / Revision Record				
Version No.	Date	DESCRIPTION OF CHANGE	Pages Affected/ Section	Change Made By
0.1	04/30/2008	Initial version of Policy developed for initial review.	All	T. Russell
0.1	05/15/2008	Modifications to initial version	All	T. Russell
0.1	05/30/2008	Added new terminology	20-21	T. Russell
1.0	06/12/2008	Policy approved and issued as version 1.0	All	D. Perry
1.1	07/20/2009	Annual review; minor edits except for Sections AC-18 and 20	AC-18 & 20	D. Perry
1.2	12/04/2009	Revised references, definitions and AC-2, AC-11, AC-17 & AC-20 for special use systems.	Sec 8, 9 & 10	D. Perry
1.3	01/30/2012	Revised to incorporate NIST800-53 Rev 3 changes and approved by OMAO CAB	Sec 8: AC-2, 5, 6, 9, 10, 12, 13, 14, 15, 16, 17, 18, 19, 20 22; Sec 9	S. Tadele, ISSO
1.3	06/24/2012	Revised to include HSPD-12 Compliance for access control and address exemptions for mission systems.	Sec 8: AC-2, AC-3, AC-7	S. Tadele, ISSO

ACCESS CONTROL POLICY

1 PURPOSE

The purpose of this document is to establish policies for the implementation of information technology (IT) access control within the National Oceanic and Atmospheric Administration (NOAA) Office of Marine and Aviation Operations (OMAO) in accordance with NIST SP-800-53 Revision 3, *Recommended Security Controls for Federal Information Systems*.

2 OBJECTIVE

This Access Control policy is primarily developed and used to detect and deter penetration of a computer system and to reveal misuse. The objective for access control is to ensure trusted computer systems provide authorized personnel with the ability to detect any action that can potentially cause access to, generation of, or affect the release of classified or sensitive information. Access control data will be selectively acquired based on the needs of a particular installation and/or application. The access control data must have sufficient details and granularity that support tracing auditable events to a specific individual or process.

3 SCOPE

The policy contained in this document is applicable to all OMAO IT users and all IT resources at all levels of sensitivity, whether owned and operated by OMAO or operated on behalf of OMAO by commercial contractors or other government agencies.

4 COMPLIANCE

This policy is based on Federal laws and regulations, including OMAO, NOAA, Dept of Commerce, and OMB Orders and Directives. As such, there are consequences for non-compliance. Depending on the severity of the violation, at the discretion of management and through due process of the law, consequences can include suspension of access privileges, reprimand, suspension from work, demotion, removal, and criminal and civil penalties.

5 POLICY REVIEW

Because of the dynamic nature of the OMAO information systems and infrastructure environments, this policy must be reviewed annually to ensure that it is current and updated as required. It is the responsibility of the OMAO Chief Information Officer (CIO) to facilitate the review of this policy on an annual basis. Senior management, system administrators, and system stakeholders should participate in the annual review.

6 DISSEMINATION

This access control policy is to be disseminated to all appropriate management, staff, users, vendors, third party processors, and support personnel. The OMAO CIO, or designated representative will establish a record to document that those involved have read, understand, and agree to abide this policy.

7 ROLES AND RESPONSIBILITIES

The major roles in access control activities are defined below:

7.1 OMAO CIO:

- A. Ensure key OMAO staff with system access control responsibility understands and follow this policy.
- B. Provide oversight for personnel with significant responsibility for information security and ensure that they are properly trained.
- C. Update this policy and related procedures as needed to ensure it meets OMAO mission requirements and complies with Federal and NOAA Laws, Policies, Procedures, and Guidelines.
- D. Ensure all Policies and Procedures herein are properly complied with and appropriate sanctions are implemented.

7.2 Management and Supervisors:

- A. Implement the requirements of this policy and related procedures within their assigned area of management control.
- B. Ensure key staff providing access control support are properly trained;

- C. Ensure that only software and/or procedures approved by OMAO and NOAA policy are used to ensure access control to OMAO data.
- D. Ensure that access control security violations/incidents occurring within their assigned area of management control are reported to the ITSO.
- E. Ensure coordination with the CIO and ITSO before authorizing the use of new access control systems.
- F. Ensure on a regular basis that all assigned employees, contractors and other individuals, who reside, or visit an OMAO facility operating unit, understand they are responsible for reporting actual or suspected access control security incidents to their immediate supervisor and the ITSO.

7.3 Information Technology Security Officer (ITSO) or Designee:

- A. Annually validating compliance with procedures contained in this policy to ensure access control is being configured and implemented properly in OMAO systems.
- B. Manage and regularly review physical and logical access given to OMAO employees, and ensure their access commensurate with their operational duties and level of clearance.
- C. Periodically review the process of providing access to OMAO systems and make recommendations on enhancing the process or tools.
- D. Periodically test access controls systems to ensure correct performance.
- E. Report incidents of noncompliance to the NCIRT.

7.4 OMAO Employees, Contractors, or Affiliated Support Staff:

- A. Follow the policies and procedures contained within this policy.
- B. Report access control security incidents or anomalies to their supervisors (COR for contractors) and the ITSO or designee.

8 POLICY

8.1 Access control Policy and Procedures (AC-1)

This document serves as the general access control policy for all OMAO IT users and resources in accordance with applicable laws, directives, policies, regulations, standards, and guidance. It addresses purpose, scope, roles, responsibilities, and management commitment, coordination among organizational entities, and compliance.

- A. As appropriate, each OMAO Operating unit will assign and document responsibility to specific parties, government or contractor, and define specific actions to ensure that the access control policy and procedures controls are implemented.
- B. Each OMAO Operating unit must consistently apply the access control policy and procedures on an ongoing basis.
- C. All OMAO personnel with access control responsibilities shall document anomalies or problems encountered in the implementation of the access control policy and procedures control and the resulting information shall be used to actively improve the control on a continuous basis.
- D. Access control is addressed for all areas identified in the access control policy and procedures. The techniques for implementing the access control requirements will vary from system to system depending upon the characteristics of the software, firmware, and hardware involved and any optional features that are to be available. OMAO will leverage industry proven and cost effective techniques to meet security and operational requirements.
- E. Special access control considerations are to be made for OMAO systems that process, store, or transmit Personally Identifiable Information (PII) and/or OMAO business sensitive information.

8.2 Account Management (AC- 2)

- A. All OMAO information systems must have written procedures, tailored to the OMAO system, for establishing, activating, modifying, reviewing, disabling, and removing accounts.
- B. All OMAO information system accounts must be reviewed every 90 days and configured to automatically lockout inactive users if accounts are inactive for a period of 90 days or more.
- C. All access requests to OMAO information systems must be authorized by the individual's manager or Contracting Officer Technical Representative (COR), and by the system owner or system manager. Access must be granted based on least privilege or on a need-to-know basis.

D. Establishing Accounts.

1. Access to OMAO resources is limited to authorized users, and account requests must specify the type of account requested (user, guest, group, administrator, etc.), the resource to be accessed (Domain, Application, VPN, etc.), the employee type (civilian, commissioned, contractor, associate, etc.), and unique requirements about the account (mission required anonymous logon, etc.).
2. OMAO users shall be granted a user ID and corresponding password for access to OMAO computing resources only upon receipt of an OMAO approved paper or digital access request form, and presentation of a Common Access Control (CAC) card.
3. Users must complete the online NOAA IT Security Awareness course and accept the NOAA Rules of Behavior within three days of being assigned use of IT equipment. If the training is not completed in the time allotted, the user ID will be suspended, and the user's manager or COR will be required to request an additional three-day temporary access period for the employee to complete the online course.
4. Accounts that enable remote access to OMAO networks require additional approval via a Remote Access Agreement signed by the individual and their manager or COTR.

E. Access for Individuals Who Are Not Government Employees.

Individuals who are not federal government employees (contractors, vendors, auditors, consultants, etc.), must not be granted a user ID or otherwise be given privileges to use OMAO information or information systems unless they have applied for a NOAA security clearance at the sensitivity designation level stated in the contract, completed initial security awareness and privacy training, and agreed to the NOAA Rules of Behavior.

F. Privileged Access.

1. Privileged Access (e.g. Admin or root accounts) to OMAO information systems shall be granted only to those users who have an operational requirement.
2. The account must be a separate account from their normal user account and must only be used while performing a function requiring privileged access. At no time should a privileged user account be used to access resources or information systems that a normal user account has been given rights to access (e.g., e-mail, home directories, etc.).
3. Access to servers and domain controllers is limited to authorized administrators; information systems must enforce HSPD-12, two factor

authentication, and requests for server certificates must be verified and approved by the OMAO Local Registration Authority (LRA). Note: mission information systems are required to comply with HSPD-12 two factor authentications NLT December 31, 2012 per NOAA policy.

G. Service Accounts.

1. Service accounts are accounts needed to run a program, routine, or process that performs a specific system function to support other programs, particularly at a low level. These accounts are typically non-individually identifiable accounts.
2. Service accounts shall only be created when there is a documented business need for such an account and the OMAO ITSO or ISSO has performed a formal security review.
3. Accounts shall be requested using the standard access request form for the applicable system.
4. When service accounts are created, the applicable Subsystem manager will be identified as the responsible person for the account and will ensure that the account password meets all NOAA password requirements.

H. Training Accounts.

1. Requests for temporary user accounts for training purposes must be submitted at least 2 weeks prior to the start date of a class for which temporary training accounts will be required. New account user IDs and passwords will be provided to the designated class coordinator.
2. Each password shall be set to immediately expire requiring the student to change the password upon its first use.
3. The accounts shall also be set to automatically suspend immediately following the end date of the class and deleted as part of the 90-day review process by system administrators.

I. Account Maintenance.

1. Subsystem Managers shall review the access privileges of all users within their area of responsibility at least annually to ensure that user accounts continue to adhere to the "least privilege" concept. User accounts shall have only the privileges required to perform the user's designated functions.
2. Administrators must only disclose passwords when: (i) a new user ID is being assigned; (ii) an authorized user has forgotten a password; or (iii) an authorized user account is locked due to a password-related problem. The password must be a new, one-time use password, revealed only as an

algorithm with information known by the user (i.e., part of a social security number plus part of a birth date) and only after the user's identity has been properly authenticated.

3. Account logon privileges may only be re-enabled after the user has requested it and properly identified themselves to the administrators resetting the account privileges.

J. Termination of Accounts.

1. Each information system user ID must be unique and connected solely with the user to whom it has been assigned. When a user separates from employment or whose contract is ended they are considered to be separated from the OMAO. After a user leaves the OMAO, there must be no re-use or reassignment of any existing user customer record and its affiliated user ID for at least 6 months.
2. Unless specifically requested by a user's manager, all user IDs will be disabled, but not deleted, the same day that the notice of departure is received, but not later than 6 pm on the next business day. The user ID shall be deleted within 4 to 6 weeks after the date of the separation notice from OMAO applications.
3. Upon receiving notice of a user's separation from OMAO, the applicable system administrator shall arrange for the user's manager to review the user's files and to transfer desired files to an alternate location. Within 4 to 6 weeks after a user has separated all remaining files in that user's directories will be purged.
4. OMAO management may revoke the privileges of any user at any time. Conduct that interferes with the normal and proper operation of OMAO information systems, which adversely affects the ability of others to use these information systems, or which is harmful or offensive to others will not be permitted.
5. Unless otherwise specifically requested otherwise by an OMAO manager, all user IDs will be disabled, but not deleted, at close of business on the day official notice of separation is sent by the local ITSO, and the user ID will be deleted 4-6 weeks later. If a manager officially requests that a user ID remain enabled after the user's clearance or non-use date, the manager must justify the delay in writing, and provide a specific date to disable.
6. Unless the OMAO ITSO has received instructions to the contrary, 4-6 weeks after a user has permanently left the OMAO, all files held in that user's directories will be purged.

8.3 Access Enforcement (AC- 3)

- A. All OMAO information systems will enforce assigned authorizations for controlling access to systems that process, store, or transmit PII and/or OMAO sensitive information. All systems that store, process, or transmit PII and/or OMAO sensitive information must utilize a properly maintained and configured version of an authentication-based access control system to ensure that the sensitive information is not improperly disclosed, modified, deleted, or rendered unavailable.
- B. All unsuccessful logins will be audited for all OMAO applications that process, store, or transmit PII and/or OMAO sensitive information. The system where the audit logs reside will be configured to ensure only authorized security and administrative staff is able to view or modify the logs.
- C. Access to OMAO information and information system resources will be granted only to individually identified and specifically authorized persons who have a demonstrated work related requirement for such access or a demonstrated “need to know.”
- D. The OMAO mission requires all systems to enforce access control to protect the confidentiality, integrity, and availability of the OMAO/NOAA information. In keeping with these objectives, management maintains the authority to:
 - 1. Restrict or revoke any user's privileges;
 - 2. Inspect, copy, remove, or otherwise alter any data, program, or other system resource that may undermine these objectives; and
 - 3. Take any other steps deemed necessary to manage and protect its information systems. This authority may be exercised with or without notice to the involved users.
 - 4. All systems and/or related devices connected to the OMAO network must be protected by an access control system approved by the OMAO Configuration Management process.
 - 5. All OMAO systems connected to third-party networks (dial-up lines, networks, Internet, etc.) will use the service contract agreement as the system interconnect agreement. All connections must be encrypted (FIPS 140-2 approved) along with the session credentials.
 - 6. Access controls will be established such that system users are not able to modify production data in an unrestricted manner. Users may only modify production data in predefined ways that preserve or enhance its integrity.

In other words, users must be permitted to modify production data ONLY when employing a controlled process approved by management.

7. System privileges must be defined so that non-production staff (i.e., internal auditors, information security administrators, programmers, computer operators) is not permitted to update "production" business information.
 8. Default to Denial of Access Control Privileges. If a computer or network access control system is not functioning properly, it must default to denial of privileges to end-users.
- E. OMAO information systems that require group and/or anonymous access can be exempt from HSPD-12 Implementation to perform mission/ business objectives of OMAO. In those cases, the access must be documented in an approved System Security Plan and supporting rationale for user actions not requiring two factor authentications must be provided.

8.4 Information Flow Enforcement (AC- 4)

- A. All OMAO information systems will enforce assigned authorizations for controlling the flow of information within the system and between interconnected systems and systems that contain PII and/or OMAO sensitive information. All OMAO facilities will at a minimum have a firewall and intrusion detection sensor at all external connections into the facilities LAN.
- B. PII and/or OMAO sensitive information must have written authorization before it is allowed to leave an OMAO facility C&A boundary (as defined in the system security plan). Approved flow of PII and/or OMAO sensitive information outside the OMAO facility must be encrypted using a FIPS 140-2 approved encryption.

8.5 Separation of Duties (AC- 5)

- A. All OMAO information systems must enforce separation of duties through assigned access authorizations.
- B. OMAO management must ensure the emplacement of controls involving separation of duties. These control measures must ensure that no one individual has exclusive control over OMAO information assets, auditing, system programming, quality assurance, configuration management, security, or benefits distribution / authorization.

8.6 Least Privilege (AC- 6)

- A. OMAO information systems must enforce the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of OMAO system tasks.
- B. OMAO information systems must enforce the use of non-privileged accounts by system administrators when accessing system functions that do not require elevated privileges and audit the use of privileged accounts to ensure compliance.
- C. All OMAO accounts will be reviewed at least annually to ensure that the accounts follow the security concept of “least privilege.” No administrator and user account should ever have more privileges than are required to do their job.
- D. The computer and communications system privileges of all users, systems, and programs must be restricted based on the need-to-know. Access to OMAO information, and information system resources will be granted only to individually identified and specifically authorized persons who have a demonstrated work-related requirement for such access or a demonstrated “need to know.”
- E. The “least privilege” concept will be enforced by the OMAO; this states that no administrator or user should have access to information system resources beyond those, which are required to perform their present job functions, and then only at the most restricted access level necessary.
- F. Restriction of Special System Privileges. Special system privileges, such as those whom have privileged accounts (E.g. System Administrators), will be restricted to those directly responsible for system management and/or security. In addition, access to Domain Controllers, network routers and firewalls, IT security servers, and enterprise services such as auditing, patching, and scanning tools will be further restricted to specific individuals in order to maintain separation of duties.
- G. Default User Privileges and Need for Explicit Approvals. Without specific written approval from management in the form of an authorized, completed access request document, administrators must not grant system privileges to any user.

8.7 Unsuccessful Login Attempts (AC- 7)

- A. To prevent password guessing attacks, the number of consecutive attempts to enter an incorrect password must be strictly limited. After three (3) unsuccessful attempts to enter a password, a system administrator will suspend the involved user ID until reset. However, unique mission/ business objectives and System administrator availability during flights or cruises, can be justification for enabling multiple login attempts on mission systems; in those cases supporting rationale must be provided in the approved System Security Plan.
- B. To prevent Denial of Service attacks perimeter network / defense devices will automatically release the suspension after 1 hour.

8.8 System Use Notification (AC- 8)

- A. All OMAO information systems will display an approved, standardized notification message prior to granting system access. The banner will inform potential users of the system of OMAO use policy and consent to monitoring. OMAO systems covered include but are not limited to all network devices (routers, switches, VPN, etc.), servers, workstations, services (secureFTP, PC Anywhere, etc.) and applications.
- B. For OMAO publicly accessible systems, the OMAO will provide a link on all Web pages that will give the user the ability to read the system use notification message.
- C. For systems that contain PII and/or OMAO sensitive information, the use notification message will be automatically generated and consented to by each OMAO user. This requires the user to acknowledge the system notification by either clicking “okay”, “yes” or typing a “Y” for yes in terminal situations. The banner is to re-appear each time the user re-logs into their OMAO account or after the account session expires.
- D. Potential users of OMAO information systems will see a banner notifying the user that the user is attempting to access a National Oceanic and Atmospheric Administration information system; that system usage may be monitored, recorded, and subject to audit; that unauthorized use of the system is prohibited and subject to criminal and civil penalties; and that use of the system indicates consent to monitoring and recording.
- E. The system use notification message provides appropriate privacy and security notices (based on associated privacy and security policies or summaries) and remains on the screen until the user takes explicit actions to log on to the information system. At a minimum the below banner will be posted to all OMAO information systems:

Notice to Users – WARNING!!

This is a United States Department of Commerce computer system, which may be accessed and used only for official Government business by authorized personnel. Unauthorized access or use of this computer system may subject violators to criminal, civil, and/or administrative action.

All information on this computer system may be intercepted, recorded, read, copied, and disclosed by and to authorized personnel for official purposes, including criminal investigations. Access or use of this computer system by any person whether authorized or unauthorized, constitutes consent to these terms.

Questions and comments should be directed to: omao.it.security@noaa.gov

8.9 Previous Login Notification (AC- 9)

This control is not applicable to Moderate information systems.

8.10 Concurrent Session Control (AC-10)

This control is not applicable to Moderate information systems.

8.11 Session Lock (AC-11)

- A. When there has been no local keyboard, mouse, or related activity on an OMAO information system for fifteen (15) minutes, session lock will be implemented to prevent further access to the system, unless continuous display of information is required to meet mission-specific objectives (in this case, a compensating control must be implemented and documented). The system will automatically activate a screen saver and lock the session. Session lock will remain in effect until the user reestablishes access using appropriate identification and authentication procedures.
- B. All OMAO information systems that contain PII and/or OMAO sensitive information will allow the user to initiate the manual session lock mechanisms.

8.12 Session Termination (AC-12)

Withdrawn and incorporated into SC-10.

8.13 Supervision and Review – Access Control (AC-13)

Withdrawn and incorporated into AC-2 and AU-6.

8.14 Permitted Actions Without Identification or Authentication (AC-14)

All OMAO information systems will allow anonymous access only to the extent necessary to perform the mission/ business objectives of the OMAO and only when the access is documented in an approved system security plan. The System Security Plan shall provide supporting rationale for user actions not requiring identification and authentication.

OMAO Systems that process, store, or transmit PII and/or OMAO sensitive information will not allow any type of system access without proper identification and authentication.

8.15 Automated Marking (AC-15)

Withdrawn and incorporated into MP-3.

8.16 Withdrawn and incorporated into MP-3. Security Attributes (AC-16)

This control does not apply to Moderate information systems.

8.17 Remote Access (AC-17)

- A. Allowed methods of remote access to OMAO systems must be documented, monitored, and controlled. Only designated OMAO managers and OMAO ITSO may authorize each remote connection for OMAO systems. Remote access to OMAO systems is to be strictly prohibited to the level of access necessary for the user to have to fulfill an operational need.
- B. Remote access to OMAO resources is permitted through the NOAA VPN system or via Secure Shell (SSH) Network Protocol.

It is the responsibility of users with NOAA VPN privileges to ensure that:

- 1. Unauthorized users are not allowed access to NOAA internal networks.
 - 2. Users possess a signed waiver to use personally owned information systems to connect to OMAO system resources. When using personally owned equipment, users must consent to having their personal equipment scanned and possibly reviewed for discovery of NOAA information should NOAA require such a review.
- C. Workstations used for remote access to the NOAA network must be Government-approved equipment and meet the following requirements:

1. Be hardened in accordance with NOAA/OMAO-approved configuration guides.
 2. Workstations will not be used to host a server that is accessed by the Internet.
 3. Workstations will have the NOAA standard virus protection installed, active, and maintained with current updates (e.g., McAfee).
 4. Workstations will have a software firewall installed and activated.
 5. Workstations will periodically use anti-spyware software to ensure their computer is free of spyware.
- D. Software used to access the NOAA networks or to process NOAA information will be acquired, installed, configured, and maintained at current releases and security patches; in accordance with direction and support provided by OMAO and NOAA security and support organizations.
1. Users will not share their account information (including their NOAA VPN ISP dial-up account) or NOAA VPN media with others.
 2. All OMAO information communicated, processed, or stored will be protected according to its classification as directed by OMAO security guidance.
 3. Users will prevent others from accessing OMAO information that is under their control and from using OMAO-supplied equipment for reasons not related to OMAO. Users will also use a password-protected screensaver (set to fifteen minutes or less) and always lock or log off of their computer when leaving it unattended. Users will log off their computer when leaving at the end of each workday, but will not power off their computer.
 4. E-mail and file transfer services will be used with caution to make sure that OMAO information does not become available to third parties as a result of its transmission across service support servers.
 5. Bluetooth, peer-to-peer networking, remote control software, and other unapproved software will not be used while connected to the NOAA network.
 6. Automatic password-saving features will not be used.
 7. Users will report any security exposure as quickly as possible and fully cooperate in order to mitigate associated risks.

- E. OMAO managers and CORs are responsible for approving remote access for each of their employees or contractor staff that require remote access to OMAO shares in order to perform their duties. Manager/CORs and employees/contractors must sign a Remote Access Agreement and forward the signed copy (digitally scanned or hardcopy) to the OMAO CIO or ITS0 for approval. The ITS0 (or designee) then requests that a VPN account be established by contacting the NOAA NOC.
- F. Modems can present a significant security risk to the NOAA network; as such require a written waiver signed by the OMAO CIO and ITS0 to request the use of a modem.
 - 1. Requests for modems must contain the name, location, and phone number of the person using the modem, the name of the users' manager, the type of modem to be installed, and the reason a connection is needed. Requests that can be satisfied by Internet access or a site-to-site VPN will be denied.
 - 2. The OMAO ITS0 (or designee) will maintain a database or spreadsheet that contains the user's name, location, manager, division, voice phone numbers, and modem phone number if a separate phone line is required, and the reason that the connection is needed. The modem will be clearly identified in the appropriate network topology diagram in the System Security Plan.
 - 3. Managers are responsible for notifying the ITS0 (or designee) when an individual no longer requires modem access due to either transferring to another division or leaving the OMAO.
 - 4. Users are prohibited from connecting dial-up modems to workstations that are simultaneously connected to the NOAA Trusted Campus Network.
 - 5. OMAO users must not establish any communications systems that accept incoming dial-up calls unless these systems have first been approved by the appropriate System Owner and the OMAO ITS0.
 - 6. The maximum permissible password attempts for a user accessing dial-up connections is three. If a computer user has not provided a correct password after three consecutive attempts, the connection must be immediately terminated.
 - 7. Restriction of Third-Party Dial-Up Privileges. Third-party vendors must only be given inbound dial-up maintenance privileges when a Subsystem Manager or System Owner determines that they have a

legitimate need for such a connection. These privileges must be enabled only for the time period required to accomplish the approved tasks and all activity monitored by OMAO staff. The modem line must be physically disconnected when not in use.

8.18 Wireless Access (AC-18)

- A. Computers containing wireless access devices (such as laptop computers with built-in wireless access devices) must have their wireless access device disabled while in an OMAO facility, unless the wireless network has been registered and approved by the OMAO CIO in accordance with NOAA IT Security policy. Registered wireless networks must enforce access restrictions that require WPA-2 encryption, invoke strong passwords, register MAC addresses, and connect only via the Outside Campus Network. Sponsors of visitors (including vendors) are responsible for ensuring their visitors have disabled such wireless devices.
- B. Connecting wireless access points or computers containing active wireless devices to an OMAO network is strictly prohibited without the prior approval of the OMAO CIO.

8.19 Access Control for Mobile Devices (AC-19)

- A. The ITSO (or designee) must approve all portable and mobile devices before allowing them access to OMAO computing resources. Personally owned mobile devices are not authorized to connect to NOAA networks.
- B. Government issued portable and mobile devices (e.g., notebook computers, personal digital assistants, cellular telephones, and other computing and communications devices with network connectivity and the capability of periodically operating in different physical locations) must be configured in accordance with the NOAA/OMAO hardening guides before OMAO network access with the device can be authorized.
- C. All portable and mobile devices are to be stored in an access controlled area when not being used.

8.20 Use of External Information Systems (AC-20)

- A. The use of a non-Government external information system to access OMAO computing resources that stores, processes, or transmits Personally Identifiable Information (PII) and/or OMAO sensitive information is strictly prohibited without the written permission of the OMAO CIO.

- B. Contractor or other approved OMAO users that wish to process, store, or transmit Personally Identifiable Information (PII) and/or OMAO sensitive information offsite, must be approved by the OMAO CIO and first undergo the formal Certification and Accreditation (C&A) process.
- C. Non-Government owned computer equipment shall not be connected directly to OMAO networks. Visitors and contractors at OMAO facilities must utilize wireless or ISP OCN connections for internet access.

8.21 User-Based Collaboration and Information Sharing

This control is not applicable to a moderate information system

8.22 Publicly Accessible Content (AC-22)

- A. The OMAO CIO will designate individuals that are authorized to post information onto Publicly Accessible systems and access OMAO web servers.
- B. The OMAO CIO will ensure that authorized individuals have reviewed DOC, NOAA and OMAO web management policies and procedures, and are aware that publicly accessible information must not contain nonpublic information.
- C. OMAO System Owners and/or web content managers must review proposed content of publicly accessible information for nonpublic information prior to posting onto OMAO information systems.
- D. OMAO System Owners and/or web content managers must review the content on publicly accessible OMAO information systems for nonpublic information at least quarterly, and remove any nonpublic information that is discovered.

9 REFERENCES

- A. Computer Act of 1987
- B. Office of Management and Budget (OMB) Circular A-130, Appendix III, Management of Federal Information Resources, November 2000
- C. National Institute of Standards and Technology, Special Publication (SP) 800-12, *An Introduction to Computer Security: The NIST Handbook, Chapter 17 – Logical Access Control*, October 1995
- D. National Institute of Standards and Technology, Special Publication (SP) 800-64, *Security Considerations in the Information System Development Life Cycle*, October 2003
- E. National Institute of Standards and Technology, Special Publication (SP) 800-30, *Risk Management Guide for Information Technology Systems*, July 2002
- F. National Institute of Standards and Technology, Special Publication (SP) 800-53 Revision 3, *Recommended Security Controls for Federal Information System*, August 2009
- G. Department of Commerce IT Security Program Policy, January 2009
- H. National Oceanic and Atmospheric Administration IT Security Manual, 212-1302, version 4.2, March 11th, 2008

10 DEFINITIONS

- (1) Access. The *ability* to do something with a computer resource, such as a technical ability (read, create, modify, or delete a file, execute a program, or use an external connection).
- (2) Authorization. The *permission* to use a computer resource; permission is granted directly or indirectly by the application or system owner.
- (3) Authentication. The process of *proving* to some reasonable degree that the user is who they claim to be.
- (4) Classification. The assignment of information or an information asset to categories on the basis of the information's need for confidentiality, integrity, and availability.
- (5) Personally Identifiable Information (PII). Personally Identifiable Information or Personally Identifying Information (PII) is any piece of information which can potentially be used to uniquely identify, contact, or locate a single person.
- (6) OMAO Sensitive Information. OMAO sensitive information is all OMAO data, on any storage media or in any form or format, which requires protection due to the risk of harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information. The term includes information whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, proprietary

information, records about individuals requiring protection under various confidentiality provisions such as the Privacy Act and the HIPAA Privacy Rule, and information that can be withheld under the Freedom of Information Act. Examples of OMAO sensitive information include the following: individually-identifiable medical, OMAO track data that deals with the movement of chemicals, spent fuel rods, or hazardous waste, and personnel information; financial, budgetary, research, quality assurance, confidential commercial, critical infrastructure, investigatory, and law enforcement information; information that is confidential and privileged in litigation such as information protected by the deliberative process privilege, attorney work-product privilege, and the attorney-client privilege; and other information which, if released, could result in violation of law or harm or unfairness to any individual or group, or could adversely affect the national interest or the conduct of federal programs.

(7) Virtual Private Network. A **virtual private network (VPN)** is a computer network that is implemented in an additional software layer (overlay) on top of an existing larger network for the purpose of creating a private scope of computer communications or providing a secure extension of a private network into an insecure network such as the Internet.

(8) Secure Shell Network Protocol. **Secure Shell**, or **SSH**, is a network protocol that allows data to be exchanged using a secure channel between two networked devices. Used primarily on Linux and Unix based systems to access shell accounts, SSH was designed as a replacement for Telnet and other insecure remote shells, which send information, notably passwords, in plaintext, leaving them open for interception. The encryption used by SSH provides confidentiality and integrity of data over an insecure network, such as the Internet.