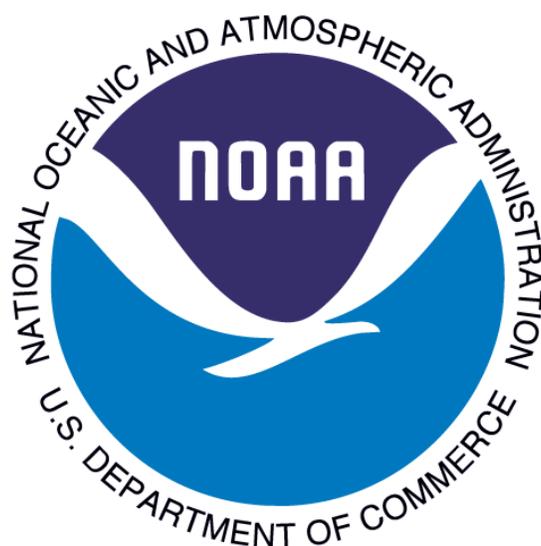


**U. S. Department of Commerce  
National Oceanic and Atmospheric Administration  
Information Systems Management Office  
Systems Support Division**



**OCIO TASB (Norfolk) NOAA1006**

**Information Technology Management (ITM)  
Policy Manual for the  
Norfolk Regional Center**

Updated: May 2007



# NRC Information Technology Management (ITM) Policy

## **TABLE OF CONTENTS**

- I. GENERAL INFORMATION
    - A. Purpose
    - B. Definition
    - C. Distribution
    - D. Scope
  - II. GENERAL MANAGEMENT POLICIES
    - A. Use of Technology
    - B. Management of Information Technology Activities
    - C. IT Project Priorities
    - D. Annual IT Planning and Development Strategy
    - E. IT Equipment Distribution
  - III. ROLES AND RESPONSIBILITIES
    - A. Director, NRC
    - B. TASB Chief
    - C. Other NRC Division Chiefs
    - D. All Employees
  - IV. SPECIFIC MANAGEMENT POLICIES
    - A. Local Application Development
    - B. Data Management
    - C. Hardware Management
    - D. Software Management
    - E. Telecommunications Management
    - F. IT Acquisition
    - G. LAN Resources
    - H. Documentation
    - I. Inventory
    - J. Systems and Telecommunications Use
    - K. Internet Use
    - L. Email Use
    - M. Use of Government Equipment (in NRC)
    - N. Use of Government Equipment (Offsite)
    - O. Copyrighted Software
    - P. Local Area Network Security
      - 1. LAN Account Management
      - 2. Password Management
      - 3. Patch Management
      - 4. Virus Protection
    - Q. Streaming Audio/Video Use
    - R. Policy Updates
- APPENDIX A NRC Authorized Commercial Software Packages

# NRC Information Technology Management (ITM) Policy

## **I. GENERAL INFORMATION**

### **A. Purpose:**

The purpose of this document is:

- To establish policy guidelines for NRC in managing information technology ("Information Technology" is defined below).
- To help ensure efficient use of limited automated information and telecommunications resources.
- To help prevent fraud, waste, and abuse in the use of such automated information and telecommunications resources.
- To establish the roles and responsibilities for managing NRC's automated information and telecommunications resources.
- To provide guidelines for managing current systems and applications.
- To provide instructions and guidance for all IT hardware, software, and telecommunications acquisitions.
- To provide instructions and guidance for all telecommunications equipment and line acquisitions.
- To provide instructions and guidance for developing and implementing all information technology (IT) and telecommunications applications in NRC.

Primary oversight for carrying out this policy is delegated to the Chief of the OCIO Technical and Administrative Support Branch (TASB). The policy provides management guidelines, in support of federal policies for the users of information technology within NRC. TASB will be cognizant of and adhere to all federal regulations pertaining to this policy and referenced in the Public law 100-235 COMPUTER SECURITY ACT OF 1987; 18 USC Sec. 1030 (1993): TITLE 18. CRIMES AND CRIMINAL PROCEDURE, CHAPTER 47. FRAUD AND FALSE STATEMENTS; 5 USC Sec. 552a: Privacy Act of 1974 and Amendments (as of Jan 2, 1991), TITLE 5, PART I, CHAPTER 5, SUBCHAPTER II; OMB CIRCULAR NO.A-130, February 8, 1996, Management of Federal Information Resources; Appendix III to OMB Circular No. A-130 - Security of Federal Automated Information Resources; Department of Commerce's Information Technology Security Handbook and Information Technology Management Handbook; NOAA's NAO 212-13, Information Technology Security Management and NOAA's Computer User's Guide for Protecting Information Resources.

### **B. Definition:**

"Information Technology" (IT) includes the related activities of data processing, and office automation and all associated hardware, software and services, as defined in the DOC "Information Technology Management Handbook".

For purposes of this document, the word "telecommunications" (TC) will be used to refer to all data and voice communications. This includes, but is not limited to, modems, telephones, private or public analog/digital telephone lines, switches, and all related equipment. Policies governing video and audio electronic conferencing are not included within this document.

## **NRC Information Technology Management (ITM) Policy**

### **C. Distribution:**

The Chief of TASB will distribute this policy to all Division chiefs and insure that a current copy is published on the NRC Intranet. This document is provided as a reference concerning IT management at NRC and as guidance for all systems users. NRC Division Chiefs will be responsible for ensuring their employees are aware of the policy and its' contents.

### **D. Scope:**

This policy applies to all current and proposed automated data systems and telecommunications operating at NRC regardless of funding source. This includes all requirements for IT processors, terminals, communication links (asynchronous, synchronous, TCP/IP), auxiliary equipment, software, all management information systems, Internet access, IP address management, Web site development and management, electronic commerce systems, data warehousing, document management and imaging systems, all related services - national and local, and all studies for the development and evaluation of such systems or requirements.

This policy also covers data communications as well as voice communications provided by NRC's telephone system and related dial tone services. It includes requirements for modems, data switches, hubs, multiplexers, voice mail, and all studies for the development and evaluation of such systems or requirements.

This policy applies to the preceding scope of activities regardless of their funding sources, organizational control and performance by government or contractor staff.

## **NRC Information Technology Management (ITM) Policy**

### **II. GENERAL MANAGEMENT POLICIES**

#### **A. Use of Technology:**

OCIO TASB Norfolk will strive to utilize the most advanced information technologies and telecommunication techniques to meet their needs of the clients they serve.

#### **B. Management of IT Activities:**

Central management and oversight of all information technology activities and resources will be provided through the OCIO TASB Norfolk in order to:

- Ensure adequate consideration of organizational objectives.
- Maximize efficient utilization of available resources.
- Provide a continuous evaluation of information technology management effectiveness at the NRC.

#### **C. IT Project Priorities:**

The highest priority for IT projects/activities will be assigned to the operation of the LAN Servers and the Wide Area Network. Second level priority will be given to the installation and support of national systems. Third level priority will be given to individual employee requests.

#### **D. Annual IT Planning and Development Strategy:**

At the beginning of each fiscal year the Chief of the TASB will contact the Business Line Division Chiefs to develop a plan and prioritize their IT requirements based on criticality to operations, technical merit, and anticipated improvement to productivity. TASB will consolidate these responses and develop their equipment/application strategic plan. The plan will be implemented as financial and operational restrictions allow. Any future needs that arise during the fiscal year will be evaluated and prioritized.

#### **E. IT Equipment Distribution:**

The NRC general IT equipment strategy is to upgrade all workstations at NRC to a faster, more advanced workstation with increased capabilities. The minimum standard platform by which NRC manages its upgrade strategy is transitory in nature and follows standards set by the NOAA OCIO as dictated by overall infrastructure requirements for operating systems, file sharing, systems deployment, E-mail, electronic commerce and telecommunications. In deciding which workstations have priority in upgrading, in consultation with the NRC management team, SD will consider the type of work being done, the type of software being used, and the demands of the applications used. To ensure these decisions are objective and based on expressed needs, NRC refers to the annual IT plan as the basis for establishing priorities.

## **NRC Information Technology Management (ITM) Policy**

### **III. ROLES AND RESPONSIBILITIES**

#### **A. TASB Chief**

Establishes the IT Policy and annual IT Plan, and delegates the oversight for carrying them out.

Resolves conflicts regarding IT or telecommunications issues.

Provides technical expertise and advice in strategic long-range planning, acquisitions, allocation and IT management to the NOAA Business Line offices for all decision making and planning associated with all ITM activities.

Develops, updates, and maintains long- and short-term goals, objectives, plans, and strategies, within the guidelines established by the ITM Policy including disaster recovery planning and implementation.

Monitors the design and conduct of operational tests and evaluations of information systems implemented at NRC in order to determine the effectiveness of these systems in meeting established requirements and design specifications.

Provides oversight and management of all NRC telecommunications equipment, services and support for both voice and data.

#### **B. Other NRC Division Chiefs**

Ensures employees are aware of the IT policy and policies, regulations and laws on use of IT resources, and in conjunction ensure employees are using resources appropriately.

On an annual basis, provides divisional ITM requirements to TASB for the inclusion into the NRC annual IT plan.

Send proposals for development and implementation of divisional applications to the TASB for action.

Approve the development of local applications within their division before they are submitted to TASB.

#### **C. All Employees**

Use IT and telecommunication resources in a responsible and productive manner as prescribed by policy, law and regulation.

Are cognizant of and practice all the security measures in this policy as well as NOAA's IT Rules of Behavior located on the NOAA Security Office web site:

[https://www.csp.noaa.gov/policies/NOAA\\_IT\\_System\\_Rules\\_of\\_Behavior\\_2006\\_updated.html](https://www.csp.noaa.gov/policies/NOAA_IT_System_Rules_of_Behavior_2006_updated.html)

## **NRC Information Technology Management (ITM) Policy**

Promptly report IT and telecommunications related problems to the TASB.

### **IV. SPECIFIC MANAGEMENT POLICIES**

#### **A. Local Application Development Policy**

A local application is defined as an application designed to enhance or improve operations within NRC. It is NOT designed for national implementation.

Development includes the entire process starting with problem definition and requirements specification through evaluation of alternatives, design, testing and finally, implementation.

A review with TASB of the proposed application is required BEFORE development begins.

The following information must be provided to TASB for analysis when reviewing a proposal for local application development:

- a. A description of the current work process.
- b. A definition of the problems to be resolved by the new application.
- c. A list of user requirements or specifications for the proposed system.

Due consideration must be given to safeguarding unauthorized access to any personnel data contained in the proposed system in accordance with the provisions and guidelines of the Privacy Act.

Development of new applications can be accommodated several different ways:

- a. The TASB may develop the application with its own staff.
- b. Upon project approval by TASB, a contractor may be hired to develop the application and SD staff will serve as COTR.
- c. Upon request approval by TASB, someone within the requesting Division may complete the development under guidance of the TASB staff.

The TASB will provide guidance and recommendation concerning the appropriate method of developing the requested application. Various needs have to be considered, including human resources, IT resources, time, and expertise. Regardless of the development method, ALL applications developed in NRC must be beta-tested and accepted by both TASB and the requesting Division.

Local database applications will be developed using NRC data base software standards and the techniques of structured analysis and design.

#### **B. Data Management Policy**

Data management involves controlling the processes of data collection, data entry, data editing, data retrieval and data security. Implementation of data control techniques is critical to successful management of information technology resources and includes the following elements:

## **NRC Information Technology Management (ITM) Policy**

- Data collection and quality control - will be the responsibility of those individuals directly involved with the work process being automated.
- Data entry - application design will enable data elements to be entered only once and as close to the data source as possible.
- Data editing - data verification, editing, error identification, correction, and updating will be performed by the application during entry.
- Data retrieval and security - data access and retrieval will be provided to those NRC employees who have a valid need for the data without regard to their divisional affiliation and with due regard to rights of individual privacy, data security, and NRC's policies.

### **C. Hardware Management Policy**

Equipment use - where possible, equipment dedicated to single applications will be avoided. Managers must seek opportunities to minimize cost and maximize efficiency through serving multiple applications, purposes, and programs through a single workstation.

Equipment maintenance – the TASB will provide technical operation, maintenance, and improvement of equipment.

Equipment moves or changes - all office changes or relocations that involve IT equipment must be coordinated with the TASB. The movement of any IT equipment must be handled or supervised by TASB. For all office relocations, IT equipment will first be removed by TASB and then replaced back into the office. IT equipment relocates with the user on internal division moves only.

### **D. Software Management Policy**

Use of existing software - existing software packages or applications that satisfy a user's requirements will be used instead of developing new application software. Before purchasing new software, an extensive search of available software or applications must be conducted by either an SD staff member or the user in conjunction with SD staff.

A list of authorized software can be found in Appendix A.

### **E. Telecommunications Management Policy**

All requests for telecommunications service or assistance should be submitted by service request to the TASB.

Trouble Reporting - In the event of telephone service outage, voice mail problems, or other failures the TASB will investigate local causes and if the problem is determined to reside external to the NRC facilities will coordinate with GSA to resolve the problem and notify the affected division(s) as to the action taken and the anticipated time before service will be restored. Service requests should include the nature of the problem, the name of the person experiencing the problem, and which telephone the problem was experienced on.

## **NRC Information Technology Management (ITM) Policy**

Station Design and Layout - TASB is responsible for coordinating all activities that require installing telephone lines, equipment, and voice mail within NRC, relocating existing service, adding additional equipment, or any other changes associated with the telephone physical infrastructure.

New/Changes to service - After receipt of a service request Systems Staff will consult with the user to determine features to be added to a new phone or any changes to existing phones.

### **F. IT Acquisition Policy**

IT procurement requests - all requests for IT equipment and software from commercial sources will be approved by TASB and forwarded to Acquisition Management Division.

Telecommunications procurement requests - TASB is responsible for ordering data communications and telephone equipment and services including video conferencing.

The purchase of ADP hardware, data communication equipment and services, and software will be researched exclusively by the TASB. Systems will coordinate with other NRC divisions, OFA and the other ASC's when applicable.

### **G. LAN Resources Policy**

LAN utilization - requests regarding LAN utilization must be initiated by an NRC Division Chief and/or Branch Chief and then forwarded to the TASB. This includes facilitating software access, evaluation and/or addition of new software, and implementing national or local applications.

Equipment movement - requests for any equipment movement and/or acquisition must be approved by the Division Chief and requested through TASB via the Helpdesk.

Adding/changing users - requests for adding or changing users shall be initiated by the appropriate Division Chief and submitted to TASB.

Deleting users - LAN accounts will be deleted for all employees terminating their employment within NRC automatically at close of business on the employees last day of employment (see Local Area Network Security). It is the responsibility of the employee's manager to insure that all data files and email that needs to be retained is transferred to another employee's folders.

New software - To request new software evaluation and/or installation on the network, justification documentation must be submitted. This documentation will include a description of the desired software/system, costs, training needs, and benefits of the software/system. TASB will provide assistance upon request.

### **H. Documentation Policy**

Complete documentation - user and maintenance documentation shall exist for all applications, and include source code and maintenance instructions for applications developed locally.

## **NRC Information Technology Management (ITM) Policy**

All documentation will be written using Microsoft Word and will be available in either Microsoft Word or Adobe Acrobat.

Timely development - Division Chiefs are responsible for providing appropriate system documentation of EXISTING systems developed external to NRC to TASB before the system is installed and implemented.

Programming code - internal programming code will be the primary method for system documentation for internally developed software.

Documenting special programming techniques - Any programming "tricks" or unusual programming techniques which cannot be documented within the source code will be documented separately and attached to the source code of the application. An example would be programming in a data base language where documentation regarding the Forms and/or Reports does not exist. Techniques manipulating those areas must be documented separately. In designing a spreadsheet for use by others, documentation regarding calculations and assumptions must be included.

Documentation review - All documentation and source code will be reviewed by TASB before the application is installed for use. Maintenance and/or modification of any local application must be documented and the TASB notified.

### **I. Inventory Policy**

Physical Inventory - TASB will maintain an equipment management system of all NOAA OCIO-owned IT and telecommunications related equipment for the purpose of tracking equipment distribution and status. All controlled/accountable equipment will be marked with a NOAA property number as required. TASB will maintain all serial numbered items in a database. This equipment management database will be updated as needed to reflect the current status.

Software and Applications Inventory - TASB will maintain an inventory of all systems implemented throughout NRC. The inventory will be updated as needed to reflect the current status.

Commercial Software Inventory - TASB will maintain an inventory of all commercial software purchased. The inventory will be updated as needed to reflect the current status.

### **J. Systems and Telecommunications Use Policy:**

Each NRC employee must comply with the following:

- Government IT and telecommunications equipment may not be used for activities other than approved Government business with the following exception: NAO 212-2 authorizes use of certain types of personal phone calls. For specific information refer to NAO 212-2.
- Confidential passwords that are issued to employees should not be shared or published and should be changed periodically. Each employee will be responsible for all use and any adverse impact stemming from the use of passwords they have been issued.

## **NRC Information Technology Management (ITM) Policy**

- Software that is copyrighted may not be copied or distributed to unauthorized users without vendor authorization.
- Authorization must be received from TASB before software can be loaded or placed onto Government equipment.
- Authorization must be received from System Division before moving, disconnecting, or altering IT or telecommunications equipment.
- Authorization must be received from TASB before adding, deleting, or changing standardized system program files used on the PC or LAN operating system, batch files or user profiles, etc. Included are the creation of hidden or password protected files.
- Personal IT and telecommunications equipment as well as personal ADP software programs may not be used at work.

### **K. Internet Use Policy:**

The Internet Use policies of the Department and NOAA allow moderate and occasional personal use of the Internet and email by employees provided that use does not include the following:

- The pursuit of private commercial business activities or profit-making ventures (i.e. employees may not operate a business with the use of the department's computers and internet resources).
- Matters directed toward the success or failure of a political party, candidate for partisan political office, or partisan political group.
- Prohibited direct or indirect lobbying.
- Use of Internet sites that result in an additional charge to the Government.
- Engaging in prohibited discriminatory conduct.
- The obtaining or viewing of sexually explicit material.
- Any activity that would bring discredit on the department.
- Any violation of statute or regulation.

The Department and NOAA expect employees to conduct themselves professionally while using Department resources. Employees must refrain from using Department resources for activities that are disruptive to the work place or in violation of public trust.

The Department and NOAA policies on the use of the Internet are available at <http://www.csp.noaa.gov/policies/index.html>

Where there is reasonable cause to believe employees may be misusing the Internet supervisors may request that official inquiries be conducted on their employees' Internet activities, including accessing computer file information. Employees found to be misusing Government Internet resources may be subject to disciplinary action up to and including removal from the Federal Service.

### **L. Email Use Policy:**

The Email policies of the department and NOAA allow moderate and occasional personal use of email by employees provided that use does not include the following:

## **NRC Information Technology Management (ITM) Policy**

- The pursuit of private commercial business activities or profit-making ventures (i.e. employees may not operate a business with the use of the department's computers and internet resources).
- Matters directed toward the success or failure of a political party, candidate for partisan political office, or partisan political group.
- Prohibited direct or indirect lobbying.
- Engaging in prohibited discriminatory conduct.
- Any activity that would bring discredit on the department.
- Any violation of statute or regulation.

Of course, the Department and NOAA expect employees to conduct themselves professionally while using Department resources. Employees must refrain from using Department resources for activities that are disruptive to the work place or in violation of public trust.

The Department and NOAA policies on the use of email are available at <http://www.csp.noaa.gov/policies/index.html>. Email, although property of the government, is still considered private. To insure this privacy no one, including managers, may be granted access to another employees email without the express written permission of the employee to whom the email account is assigned. This written consent will be cleared and filed by the IT Security Officer. Email accounts are disabled, by the LAN Administrator, within 24 hours after an employee terminates employment within NRC. It is the responsibility of the employee's manager to insure that all email that will be retained is forwarded to appropriate personnel.

Where there is reasonable cause to believe employees may be misusing the Internet or email supervisors may request that official inquiries be conducted on their employees' Email activities, including accessing computer file information. Employees found to be misusing Government Email resources may be subject to disciplinary action up to and including removal from the Federal Service.

### **M. Use of Government Equipment (in NRC):**

The following will provide a definition of what would constitute misuse of NRC computer equipment.

Regulations governing use of equipment prohibit employees from using computer equipment for any activity or purpose not directly associated with the performance of their duties, or not specifically authorized by their supervisors, however, both the department and NOAA provide authorization for employees to use the internet and email for occasional and moderate activities (refer to the Internet and Email Use Policies). This use is authorized to help personnel become proficient and maintain proficiency in using the Internet and Email.

Employees may not use government printers or supplies in conjunction with personal Internet or Email activities.

To help in determining what might be considered unauthorized use of government computer equipment the following are some of the types of activities considered to be misuse:

- Writing personal letters to friends, acquaintances and relatives.

## **NRC Information Technology Management (ITM) Policy**

- Writing resumes for employment, and completing Applications for Employment (SF-171).
- Using government systems to track, account for or report on personal finances.
- Using government systems to conduct affairs and activities associated with private business.
- Using government equipment or systems to develop or print course materials for seminars as a paid or voluntary trainer, teacher, or seminar leader for an organization which does not have a relationship with approved federal activities.
- Using government equipment or systems to produce documents, complete analysis work or products stemming from activities as a private consultant.
- Using government equipment or systems to support the activities of any private organization or church.
- Using government equipment or systems to keep any personal records not required by your employment or in conjunction with your duties. An example would be recipe files.
- Using government equipment or systems to access any bulletin board or network to communicate, access, retrieve and print to hard copy, disk or magnetic tape any information for personal use.

Please keep in mind that this list is neither exhaustive nor all-inclusive. These are only some of the activities and the nature of things that would be considered personal use and are prohibited. Please refer any question; you may have, concerning use of government computing equipment, peripheral equipment or software to the TASB staff at (757) 441-6870.

### **N. Use of Government Equipment (Offsite):**

Under certain circumstances, NOAA employees are permitted to borrow government equipment for home use for a specific period of time. This requires approval of the employee's first line supervisor and division chief and notification to the appropriate NRC Property Custodian (PC). The PC will be aware of regulations governing the borrowing of equipment. Below are restrictions that are to be followed when government-owned equipment is loaned to an NRC employee.

When may NRC property be used outside the office? With the approval of the appropriate division chief, the Chief of TASB, and the Property Custodian (PC) responsible for the property, NRC employees may take computer equipment home if they are required to regularly perform special tasks after hours or from home. The borrower is financially responsible for the property and may be required to pay for the equipment if it is lost, stolen, or damaged.

When laptop computers are taken on travel they should be carried on-board rather than being checked as baggage.

The procedures to be followed to borrow government-owned equipment is as follows:

1. The employee must obtain the approval of his/her supervisor and the Chief, TASB;
2. The PC responsible for the equipment completes NOAA Form 37-40, Personal Custody Property Record/Hand Receipt, furnishes a copy to the borrower and retains one copy for internal file/inventory record; and
3. Optional Form 7, Property Pass, is completed by the PC which allows the borrower to remove the property from a government facility and remains with security personnel.

## **NRC Information Technology Management (ITM) Policy**

Employees are reminded that government-owned computers, on-site or off-site, must be used in accordance with DOC/NOAA/NRC policy. Personally owned software or public domain software may be installed on government owned equipment provided that all licensing requirements are met, it is authorized by the TASB, and is used to accomplish the mission of NRC, NOAA, and the DOC. Software may be loaded by the TASB after it is virus scanned. The use of personally owned software must follow the procedures outline in the NRC Copyrighted Software Policy.

In accordance with the NRC Telecommuting Policy, government owned equipment will not be used by employees for the express purpose of telecommuting.

### **O. Copyrighted Software Policy:**

NRC will follow the DOC Copyrighted Software Policy without exception. This policy is as follows:

U. S. DEPARTMENT OF COMMERCE COPYRIGHTED SOFTWARE POLICY Title 17, United States Code, Section 106 gives copyright owners exclusive rights to reproduce and distribute their material, and Section 504 states that copyright infringers can be held liable for damages to the copyright owner. Title 18, United States Code provides felony penalties for software copyright infringement.

It is the responsibility of each DOC employee and supervisor to protect the government's interests as they perform their duties. This includes responsibility for assuring that commercial software, acquired by the government, is used only in accordance with licensing agreements. Likewise, it is also their responsibility to assure that any proprietary software is properly licensed before being installed on DOC equipment. This policy does not apply to software developed by or for a federal agency and no restrictions apply to its use or distribution within the federal government.

Supervisors will ensure that the following requirements are made known to all employees and will be held accountable for conducting periodic audits to ensure that these Policies are being followed:

- Install only commercial software, including shareware, which has been purchased through the government procurement process on DOC systems;
- Follow all provisions of the license agreements issued with the software and register organizational ownership;
- Do not make any illegal copies of copyrighted software. Normally the license will allow a single copy to be made for archival purposes. If the license is for multiple users, do not exceed the authorized number of copies;
- At least annually, an inventory of all software on each individual PC will be audited against the organization's license agreement records to ensure that no illegal copies of commercial software are installed on any equipment.
- Maintain written records of software installed on each machine and ensure that a license or other proof of ownership is on file for each piece of software;
- Store licenses, software manuals and procurement documentation in a secure location (i.e., closed file cabinet, etc.);
- When upgrades to software are purchased, the old version should be disposed of in accordance with the licensing agreement to avoid a potential violation. Upgraded software is considered a continuation of the original license, not an additional license;

## **NRC Information Technology Management (ITM) Policy**

- Some government owned software licenses do allow employees to take copies home for use on their personally owned computers under specific circumstances (e.g., for government work but not personal business). Unless the license specifically states that employees may take copies of software home for installation on home computers, doing so is a violation of the copyright law and the individual will be liable.
- All illegal copies of software will be deleted immediately.

All organizations must acquire special purpose software to inventory and document all software on all PCs belonging to the organization. This special purpose software may be a commercial product or the organization may acquire free software produced by the Software Publishers Association for this purpose from their operating unit ITSO.

Individual employees should be discouraged from installing their personally owned software on government equipment. If it is in the best interest of the DOC organization to allow personally owned software, authorization must be granted in writing by the immediate supervisor, showing the justification. Prior to authorization, the employee must provide the software license and give assurance that copyright infringement will not occur from installation on government equipment. Employees not following these procedures shall be held personally liable for any violations of the copyright laws and subject to the penalties contained in Title 17 and Title 18 of the United States Code.

### **P. Local Area Network Security Policy**

The NRC Local Area Network Security policy will be based on the DOC Local Area Network Security Policy, Section 10.15.1 of the DOC Information Technology Manual. This policy is available at <http://www.csp.noaa.gov/documents/lansec.txt>. The following specific policies will supplement or expand on the DOC policy for security on the NRC LAN:

#### **1. LAN Account Management**

**Windows NT Network:** Accounts for departing NRC employees will be immediately disabled at the end of the employees last day working in NRC. Within two days of the employees departure the user account of the NT network will be removed from the system entirely. It is the responsibility of the senior LAN Administrator to insure that all accounts are removed within the two day period.

**Email Accounts and NEMS:** Email accounts for departing employees will be disabled at the end of the employees last day working in NRC. All email messages in the departing employee's email folders must be forward to appropriate individuals prior to the employee's departure. In unique circumstances the employee's email folders may be retained for transfer to another individual; however, no email can be accessed or transferred without the express written consent of the departing employee. This written consent must be sent to the TASB LAN Administrator(s) and filed for reference. Within forty-eight hours of the employee's departure the email account will be deleted and the employee's information removed from the NEMS directory.

#### **2. Password Management:**

## **NRC Information Technology Management (ITM) Policy**

**Primary Administrator Account:** The Primary Administrator Password will be changed no less than once every thirty days, on or around the first day of the month. The Senior Network Administrator is responsible for changing the Primary Administrator password at the beginning of the month. If the Senior Network Administrator is not available the password can be changed by other SD staff who have the proper administrative rights on the network.

The password for the Primary Administrator account will be at least 8 characters in length and will consist of a combination of both letters and numbers. Once the password for the Primary Administrator account has been changed it is the responsibility of the person changing the password to ensure that the new password is disseminated to the other network administrator(s) within the TASB.

The Primary Administrator password is not to be shared with anyone outside of the TASB.

**Network Administrator Accounts:** Network Administrators, and anyone with a level of administrative rights on the network, will be required to change passwords on their personal accounts no less than every 30 days. The passwords will be at least 8 characters in length and will consist of a combination of both letters and numbers.

**Domain (End) Users:** Domain Users are required to change their passwords no less than once every 60 days. This requirement is to be set in the Windows NT policies. All passwords are to be at least 8 characters in length and will consist of a combination of both upper and lowercase letters, numbers, and special characters (!@#\$%^&\*+). New users will be instructed upon arrival of these requirements, as well as the need to secure the password at all times.

**Network Hardware (Switches, Printers, etc):** Telnet/HTTP password access for the switches, network printers, and other similar network devices will be changed no less than once every 90 days. The Senior Network Administrator is responsible for changing the Telnet/HTTP access passwords. The passwords for these devices are to be at least 8 characters in length and will consist of a combination of both upper and lowercase letters, numbers, and special characters (!@#\$%^&\*+).

### **3. Patch Management:**

The IT industry is constantly looking for, and finding, vulnerabilities in the Microsoft NT operating system. Keeping apprised of these vulnerabilities and insuring that the latest patches released by Microsoft to improve security are tested and implemented is an integral part of network security.

**Network Servers:** Patch management for the NT LAN servers is the responsibility of the Senior Network Administrator. No 'patches' or 'hot fixes' are to be applied to the LAN servers without an impact review with the TASB Chief and the LAN Administrator(s). Service patches will be downloaded only from the Microsoft web site or from available DOC/NOAA resources.

**Web Server:** Patch management for the NRC web server is the responsibility of the Primary Web Administrator. No 'patches' or 'hot fixes' are to be applied to the Web server without an

## **NRC Information Technology Management (ITM) Policy**

impact review with the TASB Chief and the Web Administrator. Service patches will be downloaded only from the Microsoft web site or from available DOC/NOAA resources.

### **4. Virus Protection**

The current numbers and sophistication of viruses being spread by the internet and email make viruses one of, if not the major, security threat to network, email, and web systems. To insure availability of the most current virus detection software NOAA has entered into an agreement with McAfee, Inc. to make the most current virus detection software engines and patches available to NOAA Network Administrators. The NRC Network Administrator(s) are responsible for insuring that the latest virus software is installed on all operational servers and desktops.

**Server Maintenance:** It is the responsibility of the LAN Administrator(s) to insure that the latest detection engine for the McAfee Virus Shield software is installed on all servers. The Administrators must manually download, install, and test the engines. All NRC servers will be programmed to automatically connect to the McAfee web site and download the latest patches at least once a week. In times of high activity for new viruses more frequent updating will be implemented. Note: Currently the latest patches are downloaded three times weekly.

**Desktop Maintenance:** All NRC workstations will have the latest version of the McAfee Virus Shield installed. All workstations will be configured to automatically download the latest patches from the LAN servers daily.

### **Q. Streaming Audio/Video Use Policy**

NRC's access to the NOAA network, as well as the Internet, is provided through a relatively slow network (WAN) connection between NRC, NOAA facilities in Silver Spring, Md. and Landover, Md. Access to numerous other processing locations such as the DOC Computer Center in Springfield, Va.; the National Finance Center; and the CAMS Implementation Center are routed through the OFA Information Technology Center (ITC) in Landover.

These two direct network connections handle all of the network traffic associated with Email as well as access to CAMS, Travel Manager, Payroll, Personnel, Personal Property, Real Property, CSPS, CPCS, NPS2000, and numerous other host based systems. In effect, almost all processing at NRC are dependent on these connections.

Use of any application running Live Streaming Audio or Video can tie up large amounts of bandwidth on the WAN. These applications directly compete with WAN resources and can degrade the performance of NRC's processing systems. Some examples of the Audio or Video applications that degrade our system are:

- Internet Radio
- Stock Market Ticker Tape
- News Broadcasts
- NOAA Web Casts
- Any application using continuous (streaming) audio or video

## **NRC Information Technology Management (ITM) Policy**

Some of the above applications, particularly NOAA Webcasts, are officially sponsored and approved. However, NRC's WAN capacity does not allow for multiple users to access these applications. Whenever a NOAA/DOC broadcast is relevant or important for NRC personnel the broadcast will be received and projected by a single computer in a space large enough for NRC personnel to view it as a group.

The TASB Chief may approve access to streaming applications by special request.

### **R. POLICY UPDATES**

This policy will be reviewed annually and revised as necessary.

# NRC Information Technology Management (ITM) Policy

## APPENDIX A

### AUTHORIZED DESKTOP SOFTWARE PACKAGES FOR USE AT NRC

**Operating Systems:**

MS DOS

Windows XP, Vista

**Internet Browser:**

Internet Explorer

**Word Processing:**

Microsoft Word

**Electronic Mail Client:**

Thunderbird

**Spreadsheet:**

Microsoft Excel

**Web Page Development:**

HTML Assistant Pro

Microsoft FrontPage 2000

DreamWeaver

Microsoft Word

**Virus Detection:**

McAfee Virus Scan

**Electronic Forms:**

Adobe Acrobat

Microsoft Word

**Database Languages:**

MS Access

**Project Management:**

MS Project

AutoDesk AutoCAD

PowerPoint

Paint Shop Pro

**Backup Software:**

Symantec Back-Up Exec